CYBER SECURITY
Governance & Management

CYBERLAW: TECNOLOGIA, INOVAÇÃO E SEGURANÇA

RICARDO AZEVEDO

PROFESSOR

- Advogado em Direito Digital, Gerente Jurídico e Consultor Legal de diversas empresas do setor de Tecnologia da Informação.
- Especialista em Direito Tributário pela GVLAW/EDESP e Pós-Especialização em Tributação dos Negócios de Tecnologia e Propriedade Intelectual pela GVLAW/EDESP.
- Professor na Faculdade de informática e Administração Paulista – FIAP há mais de 6 anos.
- Mais de 25 anos de experiência com atuação nas esferas Consultiva e Contenciosa em Direito Tributário, Trabalhista, Contratos e questões relacionadas a Inovação e Tecnologia.
- Experiência em projetos de relevância para empresas envolvendo Digital Law, planejamento tributário, implantação de novos negócios e reestruturações societárias e redução de contingências fiscais e trabalhistas,.
- Presidente do Comitê Jurídico da ABINC – Associação Brasileira de Internet das Coisas – 2020-2022

dr.ricardoazevedo@icloud.com

OBJETIVO

- O Programa deste curso tem como objetivo a resolução de problemas reais das empresas por meio da aplicação das melhores estratégias, práticas, regulamentações, normas e leis sobre Direito Digital.

- Assim, para entender o negócio como um todo, necessário conhecer o arcabouço jurídico e sua aplicabilidade para a proteção de sistemas, informações e pessoas.

CONTEÚDO DESTE CURSO:

DIREITO DIGITAL: TECNOLOGIA, INOVAÇÃO E LEGISLAÇÃO

- Marcos Regulatórios da Era Digital no Brasil e no Mundo
- Responsabilidades Civil, Criminal e Questões Trabalhistas.
- Investigação dos Ilícitos Eletrônicos no Ambiente Corporativo.
- Regulamentos Internos em Cibersegurança.
- Privacidade e Proteção Dados (LGPD)
- Direito em Inteligência Artificial e IoT
- Regulamentação das Moedas Eletrônicas

AVALIAÇÃO:
DIREITO DIGITAL: TECNOLOGIA, INOVAÇÃO E LEGISLAÇÃO

- Trabalho final, valendo nota de 01 a 10.
- Prazo de entrega: 10 dias após o fim do curso.

CYBER DIREITO

- Marcos Regulatórios da Era Digital no Brasil e no Mundo

CONCEITOS INICIAIS: DIREITO DIGITAL

O Direito Digital é o conjunto de normas, aplicações, conhecimentos e regulação das relações jurídicas realizadas no meio digital.

Esse ramo do Direito cria parâmetros e regras para que as interações que ocorrem no meio online aconteçam de forma harmônica. Não é um ramo autônomo do direito mas um conglomerado de vários campos do direito.

Matéria obrigatória nos cursos de Direito a partir de 2021: Res. MEC 5/2018.

Responsabilidade Civil – Reparação de danos materiais (dano emergente e lucro cessante) e danos morais. (Arts. 186 e 927 do Código Civil.

Responsabilidade Penal – Lei Carolina Dieckmann – arts. 154-A, 266 e 298 do Código Penal

Questões Trabalhistas

Legislação específica

LGPD
Marco Civil da Internet
Código de Defesa do Consumidor
Lei do Cadastro Positivo
Lei de Direitos Autorais
Lei do Software
Lei de Propriedade Industrial (concorrência desleal)
Lei Geral das Telecomunicações
*Futura Legislação sobre Inteligência Artificial

IMPORTÂNCIA DO DIREITO DIGITAL

Regulação da atividade online

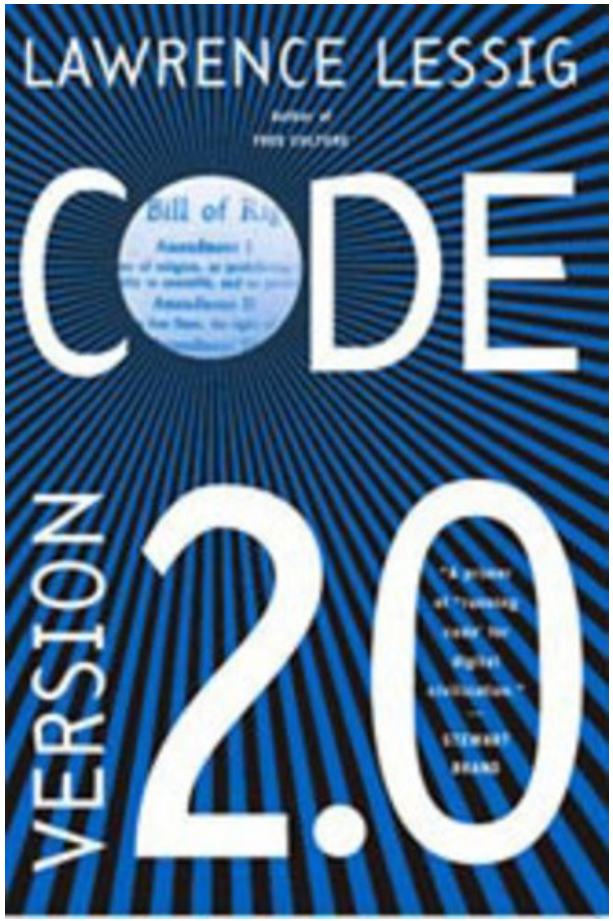
- O Direito estabelece regras para a atividade online, incluindo questões relacionadas à privacidade, segurança da informação, proteção de dados pessoais, uso de conteúdo protegido por direitos autorais, etc.

Proteção dos direitos fundamentais

- O Direito Digital é importante para proteger os direitos fundamentais, tais como liberdade de expressão, privacidade e propriedade intelectual no contexto da era digital.

Desenvolvimento da economia digital

- O direito digital é fundamental para o desenvolvimento da economia digital, regulamentando questões como a prestação de serviços online, a realização de negociações eletrônicas, gestão de contratos, organização da estrutura jurídica de uma empresa digital e a proteção de consumidores na compra de produtos e serviços na internet.



Lawrence Lessig é um escritor norte americano e professor na faculdade de direito de Harvard, sendo um dos fundadores do Creative Commons e um dos maiores defensores da internet livre, do direito à distribuição de bens culturais, à produção de trabalhos derivados (criminalizadas pelas leis atuais), e do fair use.

Cyberlaw:

Para **Lessig**, a crença comum de que ciberespaço não pode ser regulado, que em sua essência é imune ao controle governamental e **de qualquer outro órgão, está errada. Ele defende que o ciberespaço não possui uma "natureza", apenas o código e a arquitetura que o define, e que por isso ele pode ser um espaço tanto livre quanto altamente regulado, até mais do que nosso espaço real. Lessig defende que a legislação deve observar as questões técnicas.**

https://upload.wikimedia.org/wikipedia/commons/f/fd/Code_v2.pdf

Four Puzzles From Cyberspace

Regulabilidade: é a capacidade que um governo possui de regular (controlar) os comportamentos (ou condutas sociais) de seus cidadãos de maneira autônoma. Como exemplo de instrumento de regulação para um ordenamento jurídico comum, pode-se citar a sanção penal e a coerção estatal (poder de polícia, por exemplo).

Regulação através do Código: Lessig indaga se a regulação do comportamento no ciberespaço, pode utilizar a legislação existente para questões offline..
Neste caso, Lessig orienta que as legislações devem observar a relevância da questão técnica**,** pois o **Código** pode forçar certas condutas, tornando-as obrigatórias. ou limitar essas condutas, proibi-la. Os legisladores poderiam então, **regulamentar o próprio código**, e não mais as situações dele decorrentes.

Ambiguidades Resultantes: Esse tema expressa a preocupação de Lessig com a problemática das consistências jurídicas na tentativa de tornar o ciberespaço, enquanto ordenamento jurídico, mais coerente, em particular os impactos que essas alterações irão trazer para três áreas da vida social e política:

- Propriedade intelectual.
- Privacidade e intimidade.
- Liberdade de expressão.

Relações entre os ordenamentos jurídicos: Nesse tema, Lessig está preocupado com as **relações entre os ordenamentos jurídicos coexistentes**, mais particularmente na questão da **soberania** e na forma como a arquitetura da Internet é pressionada pelos ***conflitos de soberania entre os vários ordenamentos jurídicos existentes***.

PRINCIPAIS MARCOS LEGAIS DO DIREITO DIGITAL

Constituição Federal de 1988

- *O art. 5º, Inciso X, "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação."*
- *art. 5º, Inciso LXXIX "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".*
- *Art. 22, Inc.XXX, estabelece que compete privativamente à União legislar sobre proteção e tratamento de dados.*

1993

- **Código de Defesa do Consumidor:** Art. 43, estabelece que na abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele, bem como objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.

1995

- **Diretiva 95/46/CE da União Europeia –** Primeira legislação unificada da CE sobre tratamento de dados pessoais e privacidade.
- **Grupo de Trabalho do Artigo 29. -** É o grupo de trabalho europeu independente que lidou com as questões relacionadas com a proteção de dados pessoais e da privacidade até 25 de maio de 2018 (data de aplicação do GDPR). https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_pt

PRINCIPAIS MARCOS LEGAIS DO DIREITO DIGITAL

1997

- **Lei Geral das Telecomunicações –** Lei nº 9.472, de 16 de junho de 1997 - Define os conceitos do que são serviços de telecomunicações.

2001

- **MP 2.200-2, de 24 de agosto de 2001.** Institui a Infraestrutura de Chaves Públicas Brasileira ICP-Brasil, garante ao documento eletrônico o mesmo status legal de documento público ou particular.

PRINCIPAIS MARCOS LEGAIS DO DIREITO DIGITAL

2011

- **Lei do Cadastro Positivo (Lei 12.214/2011) -** Dispõe sobre o regime de tratamento das informações positivas dos consumidores junto aos cadastros positivos.
- **Lei de Acesso à Informação (Lei 12.527/2011)** – Promove a transparência das informações em posse do poder publico, disciplinando o direito de acesso à informação previsto na CF/88.

2012

- Lei Carolina Dieckman (Lei 12.737/2012) - Criminaliza a invasão de aparelhos eletrônicos com a intenção de obtenção de dados pessoais. **Foi alterada recentemente pela Lei 14.155/2021**.

2013

- Decreto nº 7.962/2013 - Regulamentou o Código de Defesa do Consumidor, para dispor sobre a contratação no comércio eletrônico.

PRINCIPAIS MARCOS LEGAIS DO DIREITO DIGITAL

2014

- Marco Civil da Internet (Lei 12.965/2014) - Foram introduzidos conceitos como (a) neutralidade de rede (impede que provedores conexão de rede cobrem valores diferentes dos usuários em função do que acessam, ou seja, os provedores só podem cobrar pela velocidade de conexão), (b) liberdade de expressão (garante que todas as pessoas tenham igual direito de difundir informações e opiniões na rede); (c) privacidade (determina que provedores e sites não podem usar dados dos usuários com fins comerciais, mas têm que guardar esses dados pelos prazos definidos na lei), além de estabelecer quais são as obrigações dos órgãos públicos no fornecimento de internet.

PRINCIPAIS MARCOS LEGAIS DO DIREITO DIGITAL

2016

- **GDPR (2016)** – O Regulamento (UE) 2016/679 é o novo Regulamento Geral sobre a Proteção de Dados da União Europeia e estabelece as regras relativas ao tratamento, por uma pessoa, uma empresa ou uma organização, de dados pessoais relativos a pessoas na UE.

2017

- Reforma Trabalhista – Lei 13476/2017 – Regula o trabalho fora das dependências do empregador com a utilização de tecnologias de informação e comunicação (teletrabalho e Home Office)

2018

- Lei nº 13. 640, de 26 de março de 2018 – Regulamenta o transporte remunerado privado individual de passageiros.
- Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGDP).
- **Resoluções n° 4.656 de 26/4/2018 e 4.657 de 26/4/2018** – Regulamentam as Fintechs que poderão oferecer crédito digital e atuar como Sociedades de Crédito Direto (SCD) ou Sociedades de Empréstimo entre Pessoas (SEP), sem a necessidade de intermediação direta com bancos.
- **Resolução n° 4.658 de 26/04/2018 e Circular n°3.909 de 16/08/2018**, que estabelecem a obrigação de uma política de segurança cibernética e os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem para as instituições financeiras e os arranjos de pagamento. Atualizada pela Resolução nº 4893, de 26/02/2021.

PRINCIPAIS MARCOS LEGAIS DO DIREITO DIGITAL

FIAP MBA+

2019

- **Lei Complementar nº 167, de 24/04/2019** – altera a legislação do Simples Nacional (LC 123/06) e introduz o INOVA SIMPLES, simplificando as regras de abertura de empresas e acesso ao INPI para registro das inovações.
- **Comunicado n° 33.455 de 24/4/2019** - aprovou a divulgação dos requisitos fundamentais para a implementação, no Brasil, do Sistema Financeiro Aberto (Open Banking), que abrangem o objetivo, a definição, o escopo do modelo, a estratégia de regulação e as ações para sua implementação.
- **Decreto nº 9.854. de 25 de junho de 2019** - instituiu o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas.
- **Decreto 10.046 de 09 de outubro de 2019. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.**

2020

- **Circular nº 3.985 de 18 de fevereiro de 2020** - novo arranjo instituído para disciplinar a prestação de serviços de pagamento relacionados a transações de pagamentos instantâneos (PIX) e estabelece o Sistema de Pagamentos Instantâneos – SPI.
- Lei **nº 14.108, de 16 de dezembro de 2020,** isenta os equipamentos M2M da Taxa de Fiscalização de Instalação, da Taxa de Fiscalização de Funcionamento, do Condecine, e isenta de licença prévia de funcionamento estas estações de IoT, de 01/01/2021 a 31/12/2025.
- **Decreto 10.222, de 05 de fevereiro de 2020**, que aprova a Estratégia Nacional de Segurança Cibernética (E-Ciber), entre outras definições, é seu objetivo aprimorar o arcabouço legal através de **um anteprojeto de lei sobre segurança cibernética**, com diretrizes que irão proporcionar alinhamento macroestratégico ao setor e contribuir de forma decisiva para elevar a segurança das organizações e dos cidadãos.

2021

- **Marco Legal das Startups (Lei Complementar nº 182, de 1º de julho de 2021).** Institui o marco legal das **startups** e do empreendedorismo inovador; e altera a Lei nº 6.404, de 15 de dezembro de 1976, e a Lei Complementar nº 123, de 14 de dezembro de 2006 (Simples Nacional).

  São enquadradas como startups as organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados (Pela LC 167 define-se **startup** como a empresa de caráter inovador que visa a aperfeiçoar sistemas, métodos ou modelos de negócio, de produção, de serviços ou de produtos, os quais, quando já existentes, caracterizam **startups** de natureza incremental, ou, quando relacionados à criação de algo totalmente novo, caracterizam **startups** de natureza disruptiva.

***Faturamento até R$ 16 milhões.**

***Até 10 anos de inscrição no CNPJ.**

***Declaração em seu ato constitutivo ou alterador e utilização de modelos de negócios inovadores para a geração de produtos ou serviços ou constituída de acordo com as regras do Inova Simples.**

PRINCIPAIS MARCOS LEGAIS DO DIREITO DIGITAL

Digital Markets Act (Regulamento EU 2022/1925) (Outubro 2022)

– A"Lei dos Mercados Digitais" é uma proposta de regulamento que objetiva limitar o poder de mercado das grandes plataformas on-line, principalmente, em relação aos "**Business Users**" destas, adotando-se práticas equitativas. Aplicável a partir do início de maio de 2023.

- **Existem 3 critérios cumulativos que colocam uma empresa ao alcance da DMA: (a) dimensão a empresa (volume de negócios no Espaço Econômico Europeu (EEE) igual ou superior a € 7,5 bi ou capitalização de mercado equivaler a pelo menos € 75 bi); (b) Número de usuários (empresa operar uma plataforma central equivalente a 45 mi de usuários finais ou 10 mil clientes corporativos na EEE) e; c) Posição consolidada (a empresa alcança um dos dois critérios "a" ou "b", nos 3 últimos exercícios financeiros).**
- **Âmbito de aplicação**: (i) serviços de intermediação em linha (e.g. mercados em linha, app stores ou serviços de intermediação em setores como a mobilidade ou energia); (ii) motores de pesquisa em linha; (iii) serviços de redes sociais em linha; (iv) serviços de plataforma de partilha de vídeos; (v) serviços de comunicações interpessoais independentes do número; (vi) sistemas operativos; (vii) navegadores web; (viii) assistentes virtuais; (ix) serviços de computação em nuvem; e (x) serviços de publicidade em linha (ad networks, ad exchanges e outros serviços de intermediação publicitária).
- Ex. **(i) Proibições de combinar dados coletados de dois serviços diferentes pertencentes à mesma empresa (por exemplo , Facebook e WhatsApp); (ii) disposições para a proteção dos usuários de negócios das plataformas (incluindo anunciantes e editores);(iii) instrumentos legais contra os métodos de auto preferência usados pelas plataformas para promover seus próprios produtos (resultados preferenciais para produtos do Google ao usar a Pesquisa Google); (iv) Obrigação de pré-instalação de alguns serviços (Google Android); entre outro**.
- **- Multas:** multas até 10% do faturamento global anual de uma empresa (20% em caso de reincidência). No caso de infrações sistemáticas, a *autoridade europeia* também poderá impor medidas comportamentais ou estruturais necessárias para garantir eficácia das obrigações previstas no regulamento, incluindo proibição de novas aquisições ou imposição de alienação de determinados negócios. O DMA ainda confere à *Autoridade Europeia* o poder de realizar investigações de mercado para garantir que as obrigações estabelecidas no regulamento se mantenham atualizadas diante da constante evolução dos mercados digitais. (https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en).

PRINCIPAIS MARCOS LEGAIS DO DIREITO DIGITAL

Digital Services Act (Regulamento UE 2022/2065) (Outubro/2022)

– A Lei de Serviços Digitais entrou em vigor em 16/11/2022 com aplicabilidade a partir de 17/02/2024 -

Reforça, padroniza e esclarece em toda a UE as condições para isenções de responsabilidade: **Plataformas e outros intermediários não são responsáveis pelo comportamento ilícito dos usuários, a menos que estejam cientes de atos ilegais e não os removam**.

Melhora significativamente os mecanismos para a remoção de conteúdo ilegal e para a proteção efetiva dos direitos fundamentais dos usuários online, incluindo a liberdade de expressão. Também cria uma supervisão pública mais forte das plataformas online.

Ambito de Aplicação: (i) Aplicação: Serviços intermediários que oferecem infraestrutura de rede; (ii) **Serviços de hospedagem**; (iii) **Plataformas online** (mercados online, lojas de aplicativos, plataformas de economia colaborativa e plataformas de mídia social) e; **Plataformas online muito grandes** que atingem mais de 10% dos 450 milhões de consumidores na Europa

Todos os intermediários online que oferecem os seus serviços na UE, ainda que estabelecidos fora dela, terão de cumprir as novas obrigações **proporcionais à sua capacidade e tamanho**: (i) **medidas para combatede bens, serviços ou conteúdos ilegais online** , como um mecanismo para os usuários sinalizarem tal conteúdo e para as plataformas cooperarem com "sinalizadores confiáveis", (ii) **novas obrigações de rastreabilidade de usuários comerciais** em mercados on-line, para ajudar a identificar vendedores de mercadorias ilegais ou esforços razoáveis de mercados on-line para verificar aleatoriamente se produtos ou serviços foram identificados como ilegais em qualquer banco de dados oficial; (iii) **salvaguardas eficazes para os usuários**, incluindo a possibilidade de contestar as decisões de moderação de conteúdo das plataformas; (iv) **proibição de certos tipos de anúncios direcionados em plataformas online** (quando visam crianças ou quando usam categorias especiais de dados pessoais, como etnia, opiniões políticas, orientação sexual); (v) **medidas de transparência para plataformas online** em uma variedade de questões, inclusive sobre os algoritmos usados para recomendações; (vi) **obrigações para plataformas muito grandes** para evitar o uso indevido de seus sistemas ou mecanismos de pesquisa, adotando ações baseadas em riscos e por auditorias independentes de seus sistemas de gerenciamento de riscos; (vii) **acesso de pesquisadores a dados-chave** das maiores plataformas e mecanismos de busca, a fim de entender como os riscos online evoluem e; (viii) **estrutura de supervisão para lidar com a complexidade do espaço online:** os países da UE terão o papel principal, apoiados por um novo Conselho Europeu de Serviços Digitais; para plataformas muito grandes, para supervisão e execução das legislações nacionais.

Penalidades: Multas de até 6% do volume anual de negócios mundiais do prestador de serviços, bem como multa diária de 5% do volume de negócios ou rendimento médio diário mundial do prestador de serviços de intermediação referentes ao exercício financeiro anterior, calculado a partir da data especificada de uma decisão do Conselho Europeu de Serviços Digitais que determinar a retirada de conteúdo indesejado.

PRINCIPAIS MARCOS LEGAIS DE COMBATE A DISSEMINAÇÃO DE CONTEÚDO ILEGAL

FIAP MBA+

França

- A França adotou uma lei em 2018 para combater a disseminação de notícias falsas na internet e que permite aos tribunais retirar conteúdo de redes sociais se considerarem que é “manipulador” ou ”enganoso”. A França tem uma autoridade administrativa independente chamada Conselho Superior do Audiovisual (Conseil Supérieur de l’Audiovisuel – CSA), que é responsável por regular as emissoras de rádio e televisão e pode tomar medidas para garantir o respeito à legislação de mídia, incluindo a remoção de conteúdo ilegal.

Alemanha

- A Alemanha aprovou a Lei de Execução da Rede de Informação em 2017. Esta lei exige que as empresas de redes sociais removam conteúdo ilegal, incluindo discurso de ódio e notícias falsas, dentro de um prazo específico. As empresas que não cumprem a lei estão sujeitas a multas elevadas.

Reino Unido

- O Reino Unido aprovou a Lei de Segurança Online em 2021, que exige que as empresas de redes sociais removam conteúdo prejudicial, como discurso de ódio e conteúdo extremista, também sob pena de multas pesadas. Órgãos independentes do Governo como o Ofcom e o ICO, supervisionados pelo Parlamento, podem fiscalizar os agentes de Telecom e Internet, depois de cumprirem um rigoroso processo e assegurar o direito de defesa, do contraditório e de privacidade.

Austrália

- Lei de Notícias e Código de Barganha em 2021, que inclui disposições para o controle do conteúdo em plataformas de redes sociais, permitindo que o governo australiano retire conteúdo se considerar que é prejudicial.

Estados Unidos

- Os EUA não tem legislação específica para o controle de conteúdo de mensagens na internet ou redes sociais, as empresas de tecnologia são regulamentadas pela Seção 230 da Lei de Decência das Comunicações, que protege as empresas de responsabilidade pelo conteúdo publicado em suas plataformas pelos usuários. (https://www.estadao.com.br/internacional/como-duas-batalhas-na-suprema-corte-dos-eua-podem-remodelar-as-regras-da-internet/).

OCDE

- As leis de diversos países, especialmente no âmbito da OCDE, tipicamente exigem que o regulador siga um processo claro antes de remover o conteúdo. As empresas de tecnologia têm o direito de contestar a decisão do regulador, e há procedimentos claros para recursos e revisões. A lei também estabelece salvaguardas para proteger a liberdade de expressão, garantindo que as opiniões legítimas e as críticas construtivas não sejam censuradas.

PL 2630/2020 – PONTOS PRINCIPAIS DO PROJETO

- **Proibição da criação de contas falsas** nas mídias sociais para simular a identidade de uma pessoa ou entidade;
- **Proibição de uso de 'bots'**, ou seja, contas automatizadas geridas por robôs;
- **Limitação do alcance de mensagens muito compartilhadas;**
- **Determina que empresas mantenham o registro de mensagens encaminhadas em massa** durante três meses;
- Exige a **identificação de usuários que patrocinam conteúdos** publicados, essa seria uma forma de evitar anúncios falsos de golpes financeiros, por exemplo;
- **Proíbe que contas oficiais** de organizações governamentais ou de pessoas de interesse público (como políticos) **bloqueiem contas de cidadãos comuns**;
- **Criação do Conselho de Transparência e Responsabilidade na Internet**, entidade autônoma de supervisão para regulamentar e fiscalizar os provedores;
- Determina que provedoras de redes sociais estabeleçam **sedes no Brasil**;
- Imposição de **sanções ou punições**, como advertências ou multas, **às empresas que descumprirem as medidas** previstas em lei.
- Criação do **Conselho de Transparência e Responsabilidade na Internet**: A lei propõe que seja criada uma entidade autônoma para fiscalizar os provedores de internet, que será responsável por instaurar processos administrativos contra os provedores de conteúdo e aplicar sanções em caso de descumprimento da lei. Portanto, em caso de decisão judicial que exija a remoção imediata de conteúdo, os provedores têm o prazo de 24 horas para cumprir o determinado. Caso contrário, a multa é de R$ 50 mil a R$ 1 milhão por hora de descumprimento.

PL 2630/2020 – PONTOS PRINCIPAIS DO PROJETO

- De acordo com o projeto de lei, **os provedores devem atuar rapidamente para prevenir e combater práticas ilícitas em suas plataformas, ou seja, assim que forem notificadas sobre conteúdos potencialmente criminosos, além de evitar a disseminação em massa dessas publicações**, tais como:

  - Crimes contra o Estado Democrático de Direito;
  - Atos de terrorismo e planejamento de terrorismo;
  - Estímulos ao suicídio e à automutilação;
  - Crimes contra crianças e adolescentes;
  - Práticas de crimes de racismo;
  - Violência contra a mulher;
  - Dificultar ou contrariar medidas sanitárias em caso de decreto de situação de emergência em saúde pública, sendo considerado uma infração sanitária.

- Outra ação prevista no texto do PL 2630/2020, determina que as plataformas avaliem riscos sistêmicos de seus serviços que podem estar facilitando a propagação de conteúdo ilegal ou até mesmo ameaçando a liberdade de expressão. Isso significa que a análise deve incluir:

  - Sistemas de recomendação e outros algoritmos;
  - Sistemas de moderação de conteúdos;
  - Termos de uso e sua aplicação;
  - Sistemas de exibição de anúncios publicitários;
  - Aberturas no sistema que possibilitem a manipulação de forma intencional, como é o exemplo da criação de contas falsas

PL 2630/2020 – PONTOS PRINCIPAIS DO PROJETO

- **Publicação das Análises de Risco Sistêmicos**: Os documentos que registrem tais análises devem ser publicadas uma vez ao ano ou sempre que as plataformas foram alteradas de forma significativa.
- **Controle parental**: Deverá ser criado mecanismos para impedir o uso dos serviços por crianças e adolescentes sempre que o conteúdo não for direcionado para a faixa etária. As mídias sociais acessíveis às crianças devem ter um nível elevado de privacidade, proteção de dados e segurança

- **Punições:** As punições cabíveis ao descumprimento da lei serão:
  - Advertência, oferecendo um prazo para que a plataforma possa agir sobre o conteúdo;
  - Multas, podendo chegar a R$ 50 milhões de reais por infração;
  - Suspensão ou proibição das atividades no país.

Para aqueles que promoverem ou financiarem a divulgação em massa de notícias falsas, poderá ser aplicada pena de **um a três anos de prisão e pagamento de multa**.

PL 2120 de 25/04/2023 – Marco Legal das Plataformas Digitais

Contraponto ao PL 2630/2020

- Art. 5º As plataformas digitais deverão criar mecanismos que permitam a qualquer usuário notificá-los, de forma justificada, da presença, em seus serviços, de práticas contrárias aos termos de uso do serviço.
- Art. 6º As plataformas digitais deverão nomear representante no Brasil.
- Art. 10º - As plataformas digitais devem restringir o funcionamento de contas automatizadas não identificadas publicamente como tal. Disponibilizar meios para permitir que o usuário da conta automatizada a identifique publicamente como tal. E, as plataformas devem adotar medidas técnicas que viabilizem a identificação de contas que apresentem movimentação incompatível com a capacidade humana, devendo informá-las em seus termos de uso.
- Art. 12. As plataformas têm o dever de garantir a proteção prioritária de crianças e adolescentes no uso de seus serviços, devendo atuar em face de conteúdos potencialmente ilegais gerados por terceiros no âmbito de seus serviços, tendo o dever geral de atuação, em prazo hábil a ser definido pela entidade de autorregulação, quando notificadas por qualquer usuário.
- Art. 17. Observada a devida proteção aos segredos comerciais e industriais, as plataformas digitais devem produzir relatórios anuais de transparência no âmbito e nos limites técnicos de seus serviços, disponibilizados em seus sítios eletrônicos, de fácil acesso, legíveis por máquina, em português, de modo a informar procedimentos gerais relativos à moderação de contas e conteúdos gerados por terceiros.

Punições:

- As decisões judiciais que determinarem a remoção imediata de conteúdo ilícito que tenha causado dano a que se refere esta Lei, deverão ser cumpridas pelas plataformas no prazo de até 24 (vinte e quatro) horas, sob pena de multa de R$ 50.000,00 (cinquenta mil reais) até R$ 250.000,00 (duzentos e cinquenta mil reais), por hora de descumprimento, a contar do término da vigésima quarta, após o recebimento da notificação.
- multa simples, de até 6% (seis por cento) do faturamento do grupo econômico no Brasil no seu último exercício ou, ausente o faturamento, multa de R$ 10,00 (dez reais) até R$ 1.000 (mil reais) por usuário cadastrado da plataforma digital sancionado, limitada, no total, a R$ 100.000.000,00 (cem milhões de reais), por infração.
- **Autorregulação:** As plataformas digitais deverão instituir, na forma de pessoa jurídica de direito privado, entidade de supervisão e autorregulação, com representação igualitárias pelas plataformas digitais associadas que se enquadrem nos requisitos desta Lei. Deverá ainda elaborar um código de conduta.

CRIPTOMOEDA: BRASIL

Lei 14.478, de 21/12/2022 – Dispõe sobre a prestadora de serviços de ativos virtuais; e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e as Leis nºs 7.492, de 16 de junho de 1986, e 9.613, de 3 de março de 1998, para incluir a prestadora de serviços de ativos virtuais no rol de instituições sujeitas às suas disposições..

- Define o ativo virtual como sendo a representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para realização de pagamentos ou com propósito de investimento;

- Atribui a aplicabilidade do Código de Defesa do Consumidor às operações conduzidas no mercado de ativos virtuais;

- Define as atividades que as prestadoras de serviços do setor poderão realizar e as diretrizes que deverão seguir. Exemplificando, troca entre ativos virtuais e moeda nacional ou estrangeira e troca entre um ou mais ativos virtuais.

- Acrescenta ao Código Penal (decreto-lei 2.848, de 1940) um novo tipo de estelionato, com pena de reclusão de quatro a oito anos e multa. Será enquadrado no crime de fraude com a utilização de ativos virtuais quem organizar, gerir, ofertar ou distribuir carteiras ou intermediar operações envolvendo criptomoedas para obter vantagem ilícita em prejuízo alheio, induzindo ou mantendo alguém em erro;

Art. 171-A. Organizar, gerir, ofertar ou distribuir carteiras ou intermediar operações que envolvam ativos virtuais, valores mobiliários ou quaisquer ativos financeiros com o fim de obter vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento. Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.

O Governo Federal ainda precisa definir qual(ais) órgão(s) será(ão) responsável(eis) pela fiscalização do setor.

Obs. **O texto estabelece que serão aplicadas, no que couber, as regras do Código de Defesa do Consumidor para as operações do mercado de ativos pessoais.**
Obs. **O Texto não autoriza o lançamento de criptoativos através de ICO.**

CRIPTOMOEDA: BRASIL

BANCO CENTRAL: BACEN/COMUNICADO N° 31.379, DE 16 DE NOVEMBRO DE 2017

- Alerta sobre os riscos decorrentes de operações de guarda e negociação das denominadas moedas virtuais e que no momento não há qualquer regulação relacionada com o Sistema Financeiro Nacional. Ressalta , ainda, que as operações com moedas virtuais e com outros instrumentos conexos que impliquem transferências internacionais referenciadas em moedas estrangeiras não afastam a obrigatoriedade de se observar as normas cambiais

COMISSÃO DE VALORES MOBILIÁRIOS (CVM) : Ofício Circular n° 11/2018

- Autoriza o investimento indireto em criptoativos por meio da aquisição de cotas de fundos e derivativos, entre outros ativos, negociados em terceiras jurisdições, desde que admitidos e regulamentados naqueles mercados. No entanto, no cumprimento dos deveres que lhe são impostos pela regulamentação, cabe aos administradores, gestores e auditores independentes observar determinadas diligências na aquisição desses ativos. A CVM ainda alertou que ICO (*Initial Coin Offering*) não estão autorizadas no Brasil.

RECEITA FEDERAL DO BRASIL: INSTRUÇÃO NORMATIVA RFB Nº 1888, 03 DE MAIO DE 2019

- As corretoras precisarão informar à Receita Federal do Brasil informações de todas as transações de seus clientes, como nome dos envolvidos, valores, data e taxas. A obrigatoriedade também vale para pessoas físicas que investem neste mercado de forma independente, sem as corretoras, e cujas transações com as moedas ultrapassarem 30.000 reais em um determinado mês.

JUNTA COMERCIAL DE SÃO PAULO: HARMONIZAÇÃO DE ENTENDIMENTO DE 20 DE OUTUBRO DE 2020

- Autoriza as empresas integralizar o capital social com bitcoins/criptomoeda (Código Civil - Art. 997, III - Lei das Sociedades Anônimas -Art. 7º), mediante avaliação pecuniária (laudo técnico que garanta que os valores declarados correspondem à realidade.

PRINCIPAIS MARCOS LEGAIS DO DIREITO DIGITAL

Futuro (?)

- Projeto de Lei n° 2630, de 2020 (Lei das Fake News)/ou PL 2120/2023.
- Inteligência Artificial
- Lançamento de Criptomoedas / NFTs
- Blockchain
- Metaverso

- Responsabilidades Civil, Criminal e Questões Trabalhistas.

- Responsabilidade Civil.

RESPONSABILIDADE **CIVIL**

Responsabilidade Civil: toda ação ou omissão que gera violação de uma norma jurídica legal ou contratual, resultando em uma obrigação de reparar o ato danoso.

Responsabilidade Civil Subjetiva	Responsabilidade Civil Objetiva
Diz-se subjetiva a responsabilidade quando se baseia na culpa do agente, que deve ser comprovada para gerar a obrigação indenizatória.	É aquela em que a obrigação de indenizar independe de dolo ou culpa, bastando o nexo causal entre a conduta e o dano experimentado pela vítima. "Haverá obrigação de reparar o dano, independente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem" (artigo 927, parágrafo único, do Código Civil). **Dano moral presumido (In Re Ipsa)**: **O constrangimento causado à pessoa, independe de prova**, ou seja, incita na própria coisa, logo, para constituir tal dano moral basta a violação de um direito, independente do sentimento negativo de mágoa, angustia, tristeza, humilhação, vexame, vergonha, etc, os quais só terão relevância para a qualificação do dano. **O Dano Material precisa ser comprovado**.
Ex. Danos Cíveis.	Ex. Danos Causados pelo Estado; Código de Defesa do Consumidor; **Danos na Prestação de Serviços Regulados**;.

Ato Ilícito	Dolo ou Culpa do Agente	Nexo de Causalidade	Dano	Ato Ilícito	Nexo de Causalidade	Dano

Responsabilidade Civil: Relação de Consumo (Art. 14 do Código de Defesa do Consumidor)

Art. 14. O fornecedor de serviços responde, **independentemente da existência de culpa**, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.

§ 1º O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais:

I - o modo de seu fornecimento;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - a época em que foi fornecido.

§ 2º O serviço não é considerado defeituoso pela adoção de novas técnicas.

§ 3º O fornecedor de serviços **só não será responsabilizado** quando provar:

I - **que, tendo prestado o serviço, o defeito inexiste;**

II - a culpa exclusiva do consumidor ou de terceiro.

§ 4º A responsabilidade pessoal dos profissionais liberais será apurada mediante a verificação de culpa.

Responsabilidade Civil: Outros Casos

TRANSAÇÃO COMERCIAL. SITE ESPECIALIZADO DA INTERNET. PRESTAÇÃO DE SERVIÇO. FRAUDE. CAPTURA DE INFORMAÇÕES PESSOAIS DO CADASTRO. (...) Nos casos de realização de transação comercial através de site especializado, responde a respectiva empresa pelas fraudes sofridas pelos seus clientes (...). Havendo o cadastramento do endereço eletrônico do cliente em seu banco de dados, através do qual se daria o contato com os possíveis compradores, configura defeito do serviço, se essa informação (...) ao conhecimento de estelionatário, que dela se utilizou para ludibriar a consumidora e obter o recebimento indevido da mercadoria anunciada. (...) Mas no caso presente, ela também estaria presente por força da violação do dever de preservação de informação restrita ou sigilosa.‖ (TJ/DF, Relator Luis G. B. de Oliveira, Recurso Inominado nº. 20060110966598, Julgado em 18/03/2008).

Tipo de Dano

Dano material é o prejuízo financeiro efetivamente sofrido pela vítima, causando diminuição do seu patrimônio.

- Dano Emergente
  - o que efetivamente o lesado perdeu
- Lucros Cessantes
  - o que razoavelmente deixou de ganhar

Dano Moral (Conceito):

O dano moral decorre de uma violação de direitos da personalidade, atingindo, em última análise, o sentimento de dignidade da vítima. Pode ser definido como a privação ou lesão de direito da personalidade, independentemente de repercussão patrimonial direta, desconsiderando-se o mero mal-estar, dissabor ou vicissitude do cotidiano, sendo que a sanção consiste na imposição de uma indenização, cujo valor é fixado judicialmente, com a finalidade de compensar a vítima, punir o infrator e prevenir fatos semelhantes que provocam insegurança jurídica.

LGPD: Danos Morais ocasionados por incidentes de segurança X natureza in re ipsa da Responsabilidade Civil.

PROCESSUAL CIVIL E ADMINISTRATIVO. INDENIZAÇÃO POR DANO MORAL. VAZAMENTO DE DADOS PESSOAIS. DADOS COMUNS E SENSÍVEIS. DANO MORAL PRESUMIDO. IMPOSSIBILIDADE. NECESSIDADE DE COMPROVAÇÃO DO DANO.

I - Trata-se, na origem, de ação de indenização ajuizada por particular contra concessionária de energia elétrica pleiteando indenização por danos morais decorrentes do vazamento e acesso, por terceiros, de dados pessoais.

II - A sentença julgou os pedidos improcedentes, tendo a Corte Estadual reformulada para condenar a concessionária ao pagamento da indenização, ao fundamento de que se trata de dados pessoais de pessoa idosa.

III - A tese de culpa exclusiva de terceiro não foi, em nenhum momento, abordada pelo Tribunal Estadual, mesmo após a oposição de embargos de declaração apontando a suposta omissão. Nesse contexto, incide, na hipótese, a Súmula n. 211/STJ. In casu, não há falar em prequestionamento ficto, previsão do art. 1.025 do CPC/2015, isso porque, em conformidade com a jurisprudência do STJ, para sua incidência deve a parte ter alegado devidamente em suas razões recursais ofensa ao art. 1022 do CPC/2015, de modo a permitir sanar eventual omissão através de novo julgamento dos embargos de declaração, ou a análise da matéria tida por omissa diretamente por esta Corte. Tal não se verificou no presente feito. Precedente: AgInt no REsp 1737467/SC, Rel. Ministro Napoleão Nunes Maia Filho, Primeira Turma, julgado em 8/6/2020, DJe 17/6/2020.

IV - O art. 5º, II, da LGPD, dispõe de forma expressa quais dados podem ser considerados sensíveis e, devido a essa condição, exigir tratamento diferenciado, previsto em artigos específicos. Os dados de natureza comum, pessoais mas não íntimos, passíveis apenas de identificação da pessoa natural não podem ser classificados como sensíveis.

V - O **vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações.**

VI - Agravo conhecido e recurso especial parcialmente conhecido e, nessa parte, provido.

(STJ - AREsp: 2130619 SP 2022/0152262-2, Data de Julgamento: 07/03/2023, T2 - SEGUNDA TURMA, Data de Publicação: DJe 10/03/2023)

Responsabilidade Civil: Tipo do Dado Pessoal para Análise da Criticidade para Apuração de Danos.

Contexto	Incidente de segurança. Reconhecimento da ocorrência do vazamento, porém, ausência de prova de culpa da Ré, tampouco de dano moral ocorrido.
Citação	"Nenhuma fraude foi praticada em seu desfavor tendo por objeto os dados vazados, os quais, aliás, não dizem respeito à sua intimidade e, portanto, seu conhecimento por terceiros não causa, por si só, qualquer violação a direito de personalidade. De se reiterar que os dados pessoais da Parte Autora, eventualmente vazados, são aqueles que se fornece em qualquer cadastro, inclusive nos sites consultados no dia a dia. **A maioria dos dados envolve qualificação do consumidor que não é acobertada por sigilo e o conhecimento por terceiro não viola direito da personalidade**. Os demais dados também são fornecidos comumente em aplicativos e sites de compras ou transações diárias. Já as informações sobre o consumo de eletricidade ou número de instalação mostram-se de pouca relevância para terceiros. **Ora, é certo que, para se caracterizar dano moral a ensejar reparação, o fato deve gerar grave ofensa à honra, à dignidade ou a atributo da personalidade da pessoa. Ademais, para que haja responsabilidade civil, seja ela subjetiva ou objetiva, é necessária a efetiva ocorrência de dano, devendo este ser presumido somente em hipóteses excepcionais**. "(TJSP 1007620-63.2021.8.26.0405

Dano Moral x Mero Aborrecimento

O mero aborrecimento pode ser classificado como uma situação, que mesmo sendo lesiva, é comum na vida cotidiana, ou seja, algo visto como normal, compreensível e suportável na sociedade, é um mero dissabor.

Apesar de caracterizar falha no fornecimento do produto ou na prestação do serviço, bem como desrespeito à lei, o mero aborrecimento é entendido como um acontecimento trivial e por isso não enseja indenização, pois mesmo que configure desgaste ao consumidor e de alguma forma prejudique sua rotina, não há agressão exacerbada.

Dano Moral x Mero Aborrecimento

Em razão da pandemia do Covid-19, Síndico de condomínio comunica através do grupo de whatsapp dos moradores que o uso da piscina, quadra de futebol e academia estão suspensos até segundo momento.

Alguns moradores inconformados iniciam discussão no grupo. O Síndico informa que está apenas seguindo a legislação e um destes moradores, comentando ser um juiz de direito, profere impropérios e palavrões contra o Síndico, informando que o mesmo será removido do cargo se o uso da piscina, quadra de futebol e academia não forem imediatamente liberado.

Você entende que o Síndico tem direito a pleitear indenização por danos morais daquele morador?

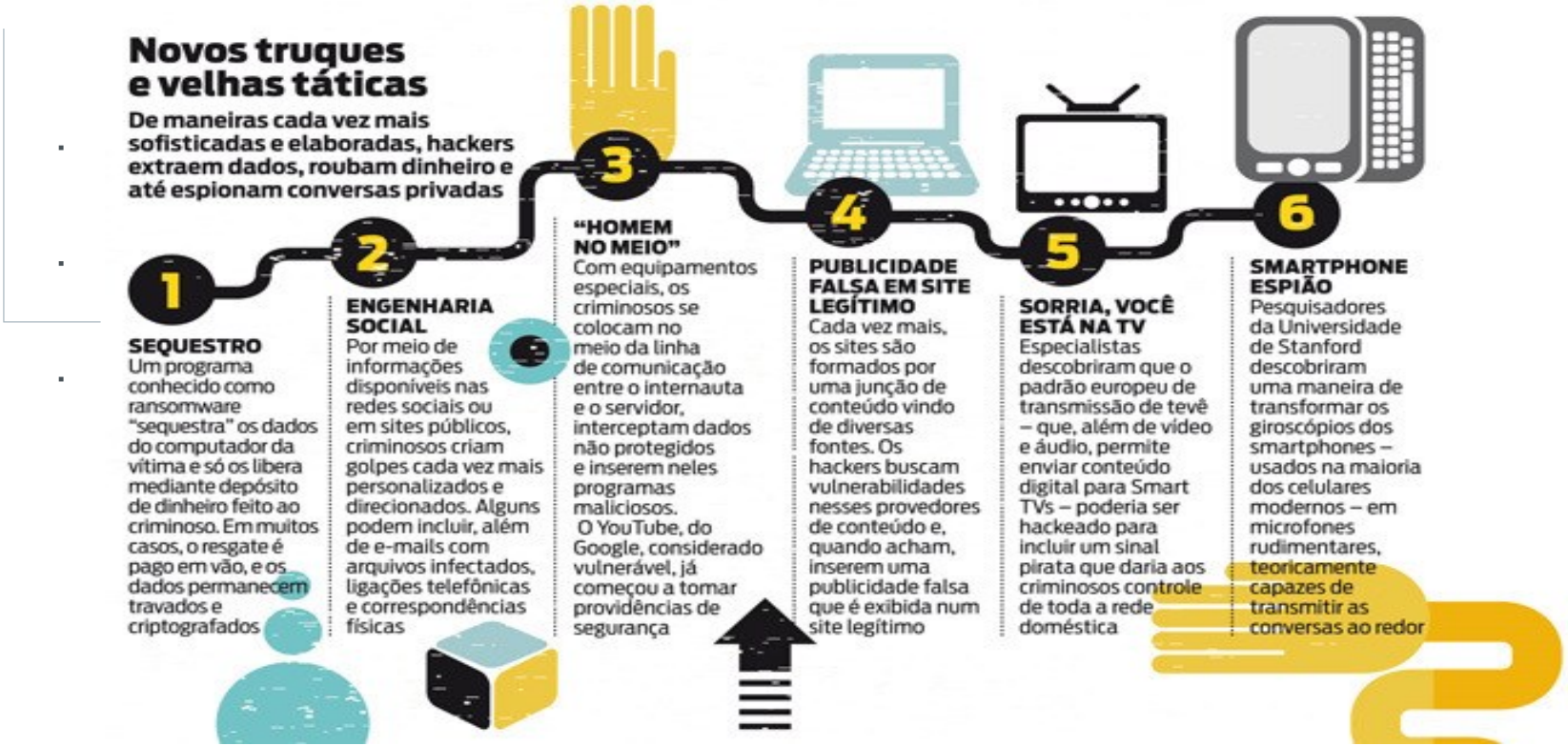
Dano Moral x Mero Aborrecimento

INDENIZAÇÃO POR **DANOS MORAIS**. VEICULAÇÃO DE CRÍTICAS À **SÍNDICA** POR MEIO DE MENSAGENS POSTADAS NO GRUPO DE CONDÔMINOS DO "**WHATSAPP**". TRANSTORNOS DECORRENTES DE DESCONTENTAMENTO COM ADMINISTRAÇÃO DE CONDOMÍNIO. PROIBIÇÃO DE USO DE ÁREAS COMUNS. AUSÊNCIA DE PROVAS. ÔNUS DA AUTORA. EXEGESE DO ART. 373, INC. I, DO CPC. **DANO MORAL**. INOCORRÊNCIA. Mensagens postadas pelos corréus via "**WhatsApp**" em grupo de condôminos criticando a atuação da **síndica**, em que pese causar-lhe aborrecimentos e transtornos, não atingiu sua honra de modo a provocar **dano moral**, pois referem-se ao descontentamento com o trabalho por ela desempenhado. Em que pese não se exigir a prova do **dano moral**, é imprescindível a demonstração do fato que o gerou pela parte que alega o abalo psíquico. Recurso desprovido.

Ação de indenização por danos morais. Ofensa dirigida por condômino a síndico, em grupo de moradores no aplicativo "WhatsApp". Atribuição de conduta criminosa, sem fundamento em provas. Ofensa à honra subjetiva do autor. Palavreado injurioso dirigido ao autor com nítida intenção de ofendê-lo. Conduta que extrapola o direito de crítica à gestão do síndico. Danos morais caracterizados. Quantum indenizatório bem fixado. Sentença mantida. Recurso não provido.

Legislação Brasileira Aplicável aos Crimes Eletrônicos

Responsabilidade Penal



Responsabilidade Penal - Legislação Brasileira Aplicada aos Crimes Eletrônicos

Lei Carolina Dieckmann (Alterada em 2021 pela Lei 14.155, de 27/05/2021) :

Art. 154-A. Invadir dispositivo informático de uso alheio, **conectado ou não à rede de computadores**, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:

Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

§ 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

§ 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços). se da invasão resulta prejuízo econômico.

§3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

§ 4º Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Ação penal

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Responsabilidade Penal - Legislação Brasileira Aplicada aos Crimes Eletrônicos – Lei 9.279/96

A concorrência desleal se divide em duas espécies:

- **Concorrência desleal específica** (art. 195), onde a lei enumera várias condutas que são consideradas crime de concorrência desleal. **Concorrência desleal genérica** (art. 209), que institui o direito à indenização a todos os lesados, por algum ato de concorrência desleal não previsto na lei.

Exemplos de concorrência desleal:

- **Difamação do concorrente:**

É uma forma de concorrência desleal que consiste em difamar a empresa concorrente, depreciando produtos, bens ou serviços com o objetivo de prejudicá-la em termos financeiros ou de imagem. Esse exemplo de concorrência desleal é muito comum na internet, através de compartilhamento de conteúdos que depreciam a imagem de outros negócios, como boatos difamatórios, por exemplo.

Mas não confunda a difamação do concorrente com a simples publicidade comparativa. Neste último caso, uma empresa compara os seus produtos ou serviços com outros que já existem no mercado, apenas como parâmetro ao consumidor. Aqui então não se configura como um ato ilícito.

- **Concorrência parasitária**:

Neste exemplo de concorrência desleal, uma empresa se aproveita do sucesso do concorrente e consegue novos clientes, sem investimento ou esforço. Isso acontece quando a empresa espera o concorrente lançar um produto , por exemplo, para copiá-lo sem investimento em pesquisa ou publicidade.

- **Violação de marcas:**

É considerada um ato de concorrência desleal e se caracteriza pela confusão do consumidor entre duas marcas, levando a um desvio de clientela. Uma forma de evitar que sua empresa seja vítima ou condenada por violação de marca é fazendo o registro no Instituto Nacional da Propriedade Industrial (INPI).

A LPI (Lei nº 9.279/96) assegura que é direito do prejudicado o ressarcimento de perdas e danos por prejuízos causados em função dos atos de concorrência desleal. Se você é vítima mas tem dúvidas quanto a quem efetivamente praticou o ato desleal, convém dar entrada em uma investigação policial, em até 6 meses da data do conhecimento da autoria do crime de concorrência desleal.

Responsabilidade Penal - Legislação Brasileira Aplicada aos Crimes Eletrônicos – Lei 9.279/96

Art. 195. Comete crime de concorrência desleal quem:

I - publica, por qualquer meio, falsa afirmação, em detrimento de concorrente, com o fim de obter vantagem;

II - presta ou divulga, acerca de concorrente, falsa informação, com o fim de obter vantagem;

III - emprega meio fraudulento, para desviar, em proveito próprio ou alheio, clientela de outrem;

IV - usa expressão ou sinal de propaganda alheios, ou os imita, de modo a criar confusão entre os produtos ou estabelecimentos;

V - usa, indevidamente, nome comercial, título de estabelecimento ou insígnia alheios ou vende, expõe ou oferece à venda ou tem em estoque produto com essas referências;

VI - substitui, pelo seu próprio nome ou razão social, em produto de outrem, o nome ou razão social deste, sem o seu consentimento;

VII - atribui-se, como meio de propaganda, recompensa ou distinção que não obteve;

VIII - vende ou expõe ou oferece à venda, em recipiente ou invólucro de outrem, produto adulterado ou falsificado, ou dele se utiliza para negociar com produto da mesma espécie, embora não adulterado ou falsificado, se o fato não constitui crime mais grave;

IX - dá ou promete dinheiro ou outra utilidade a empregado de concorrente, para que o empregado, faltando ao dever do emprego, lhe proporcione vantagem;

X - recebe dinheiro ou outra utilidade, ou aceita promessa de paga ou recompensa, para, faltando ao dever de empregado, proporcionar vantagem a concorrente do empregador;

XI - divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato;

XII - divulga, explora ou utiliza-se, sem autorização, de conhecimentos ou informações a que se refere o inciso anterior, obtidos por meios ilícitos ou a que teve acesso mediante fraude; ou

XIII - vende, expõe ou oferece à venda produto, declarando ser objeto de patente depositada, ou concedida, ou de desenho industrial registrado, que não o seja, ou menciona-o, em anúncio ou papel comercial, como depositado ou patenteado, ou registrado, sem o ser;

XIV - divulga, explora ou utiliza-se, sem autorização, de resultados de testes ou outros dados não divulgados, cuja elaboração envolva esforço considerável e que tenham sido apresentados a entidades governamentais como condição para aprovar a comercialização de produtos.

Pena - detenção, de 3 (três) meses a 1 (um) ano, ou multa.

Responsabilidade Penal - Legislação Brasileira Aplicada aos Crimes Eletrônicos – Lei 9.279/96

- Questões Trabalhistas.

Questões Trabalhistas – Vínculo Empregatício.

Justiça do Trabalho de São Paulo reconhece vínculo empregatício entre motorista e aplicativo de transporte.

A 14ª Turma do TRT da 2ª Região declarou, por maioria, vínculo empregatício entre um motorista e a empresa de transporte por aplicativo Uber Brasil e reconheceu que a dissolução do contrato realizada de forma unilateral pela organização, sem justificativa, equivale a uma dispensa sem justa causa.

Para fundamentar o julgado, a Corte ressaltou a existência de pessoalidade, uma vez que o motorista não poderia se fazer substituir em suas atividades, e de onerosidade, uma vez que a existência de remuneração é incontroversa na relação. O magistrado observou ainda a não-eventualidade, justificando que o homem prestou serviços ao longo de cinco anos para a companhia de forma contínua. Nesse aspecto, considerou também outras formas de controle de habitualidade, como a estipulação de metas a serem cumpridas sob pena de desvinculamento da plataforma. O relatório reconheceu, por fim, a presença de subordinação, levando em conta que a recusa de chamadas por corridas resulta em sanções ao profissional, assim como a estruturação do algoritmo da Uber, que impõe ao condutor a forma de execução do trabalho (**Pub. ww2.trt2.jus.br em 08/11/22 - Proc. nº 1001543-75.2021.5.02.0043)**.

Em 2018, o Poder Judiciário do Estado da Califórnia teve a oportunidade de julgar o caso Dynamex Operations West, Inc. versus. Superior Court, onde restou estabelecidos certos requisitos para determinar se um determinado empregado pode ser considerado um "independente Contractor", ou seja, um autônomo (https://law.justia.com/cases/california/supreme-court/2018/s222732.html):

A - O trabalhador está livre do controle e direção da entidade contratante na execução do serviço, tanto no âmbito do contrato de prestação de serviços como no próprio fato, ou seja, durante a realização do serviço?

B - O trabalhador que executa o serviço está fora do curso normal dos negócios da entidade contratante (ou seja, da atividade fim da empresa contratante)?

O trabalhador está habitualmente envolvido em um comércio, ocupação ou negócio estabelecido de forma independente da mesma natureza do trabalho executado para a entidade contratante?

Em outro famoso caso, a Suprema Corte do Reino Unido também reconheceu em 2020, uma decisão da Tribunal do Trabalho inglês, que decidiu que a empresa de transporte por aplicativos de transporte Uber deve reconhecer os seus motoristas como "workers", categoria que inclui trabalhadores ocasionais, temporários ou alguns trabalhadores autônomos, devendo oferecer aos mesmos salário-mínimo, férias e contribuições para a aposentadoria daqueles. (https://www.supremecourt.uk/cases/uksc-2019-0029.html).

No Reino Unido existem as classificações de workers e employees, sendo que estes se referem àquela pessoa que trabalha em tempo integral para uma determinada pessoa, mediante um contrato de trabalho, tendo mais direitos do que os workers, como por exemplo, o pagamento de auxílio-doença, licença maternidade, aviso prévio, proteções contra demissões injustas, além dos benefícios que pagos aos "workers".

Questões Trabalhistas – Questões Práticas.

Propriedade / Exploração do Software.

O Art. 4º da Lei do Software estabelece que "**Salvo estipulação em contrário, pertencerão exclusivamente ao empregador, contratante de serviços ou órgão público, os direitos relativos ao programa de computador, desenvolvido e elaborado durante a vigência de contrato ou de vínculo estatutário, expressamente destinado à pesquisa e desenvolvimento, ou em que a atividade do empregado, contratado de serviço ou servidor seja prevista, ou ainda, que decorra da própria natureza dos encargos concernentes a esses vínculos.**"

O tratamento previsto neste artigo será aplicado nos casos em que o programa de computador for desenvolvido por bolsistas, estagiários e assemelhados.

Questões Trabalhistas – Questões Práticas.

Home Office

A prestação de serviços preponderantemente fora das dependências do empregador, com a utilização de tecnologias de informação e de comunicação que, por sua natureza, não se constituam como trabalho externo – Arts. 75-A a Arts. 75-E da CLT.

*Observação das Regras da Segurança e Medicina do Trabalho;

* Pagamento do aumento de despesas do funcionário na sua residencia, como energia e internet;

*manutenção do Vale Refeição/Vale Alimentação quando já estiver integrado à remuneração ou previsto de acordo coletivo de Trabalho;

*possibilidade de suspensão do VT.

Lei nº 14.442, 2022 – Passa a considerar as expressões "teletrabalho" e "trabalho remoto" como sinônimos.

a) o teletrabalho poderá ser realizado por jornada ou por produção ou tarefa (somente nestes casos não há marcação de ponto);

b) o comparecimento, mesmo o habitual, às dependências do empregador para a realização de atividades específicas que exijam a presença não descaracteriza o regime de teletrabalho ou trabalho remoto;

c) teletrabalho não se confunde com o telemarketing ou teleatendimento;

d) o tempo de uso de equipamentos tecnológicos e semelhantes fora da jornada de trabalho não constitui tempo à disposição, regime de prontidão ou sobreaviso, salvo previsão em acordo individual ou norma coletiva de trabalho;

e) aprendizes e estagiários também podem ser teletrabalhadores;

f) aos teletrabalhadores aplicam-se as disposições previstas na legislação local e nas normas coletivas relativas à base territorial de seu estabelecimento de lotação, de modo a dirimir a controvérsia existente em relação a qual norma coletiva será aplicada;

g) ao teletrabalhador que realiza seu trabalho fora do território nacional aplica-se a legislação brasileira, exceto disposição em contrário estipulada pelas partes e ou enquadrados na Lei nº 7.064 (expatriados);

h) acordo individual poderá dispor sobre horários e meios de comunicação entre empregado e empregador, desde que assegurados os repousos legais;

i) a prestação de serviços na modalidade de teletrabalho deverá constar expressamente do instrumento de contrato individual de trabalho e;

j) o empregador não será responsável pelas despesas resultantes do retorno ao trabalho presencial, na hipótese de o empregado optar pela realização do teletrabalho ou trabalho remoto fora da localidade prevista no contrato, salvo disposição em contrário estipulada entre as partes.

Questões Trabalhistas – Questões Práticas.

Monitoramento de Funcionários

Não se vislumbra ilegalidade na decisão recorrida que admitiu a utilização do vídeo de monitoramento realizado dentro do veículo de propriedade da empresa, pois demonstrada a indispensabilidade da medida para fins de prova da falta grave praticada pelos recorrentes (TST - RR: 449001920125170012, Relator: Delaíde Miranda Arantes, Data de Julgamento: 14/08/2019, 2ª Turma, Data de Publicação: DEJT 23/08/2019).

AGRAVO DE INSTRUMENTO DA RECLAMADA. RECURSO DE REVISTA. AÇÃO CIVIL PÚBLICA AJUIZADA PELO MINISTÉRIO PÚBLICO DO TRABALHO. TUTELA RESSARCITÓRIA. MONITORAMENTO DAS ATIVIDADES DOS EMPREGADOS POR MEIO DE CÂMERA. PRETENSÃO DE PAGAMENTO DE INDENIZAÇÃO POR DANO MORAL COLETIVO. PODER FISCALIZATÓRIO DO EMPREGADOR. AUSÊNCIA DE ILICITUDE DA CONDUTA. Decisão Regional em que adotado o entendimento de que o monitoramento dos trabalhadores por meio de câmera acarreta dano moral coletivo. Aparente violação do art. 5º, X, da CF, nos moldes do art. 896 da CLT, a ensejar o provimento do agravo de instrumento, nos termos do artigo 3º da Resolução Administrativa nº 928/2003. Agravo de instrumento conhecido e provido. RECURSO DE REVISTA DA RECLAMADA. AÇÃO CIVIL PÚBLICA AJUIZADA PELO MINISTÉRIO PÚBLICO DO TRABALHO. TUTELA INIBITÓRIA. MONITORAMENTO DAS ATIVIDADES DOS EMPREGADOS POR MEIO DE CÂMERA. PODER FISCALIZATÓRIO DO EMPREGADOR. AUSÊNCIA DE ILICITUDE DA CONDUTA. 1. Trata-se de Ação Civil Pública em que o Ministério Público do Trabalho denuncia irregularidades praticadas pela reclamada, relativas à vigilância constante de seus empregados por meio de câmeras instaladas em suas dependências, com exceção dos banheiros. 2. **Constata-se do acórdão do Tribunal Regional o seguinte: resta incontroverso, na hipótese vertente, que a demandada mantém câmeras de monitoramento nos locais em que seus empregados executam suas tarefas laborais; é incontroverso que não havia câmeras em vestiários e banheiros**, conforme, inclusive, deixou claro a inicial. 3. Em primeira instância, a reclamada foi condenada a desativar e retirar as câmeras de filmagem instaladas no interior de suas dependências onde houvesse execução de atividades por empregados e onde não existisse a possibilidade de acesso por terceiros invasores, sob pena de multa diária. O Tribunal Regional manteve a condenação sob o fundamento de que "O monitoramento permanente das atividades dos empregados gera indiscutível desconforto a estes, incita a desconfiança mútua, bem como desrespeita o critério da confiança recíproca que deve informar as relações contratuais entre empregados e empregadores, disso resultando grave ofensa à dignidade dos trabalhadores, inclusive porque parte do princípio de que o empregado pode ser desonesto". 4. Contudo, o monitoramento dos empregados no ambiente de trabalho por meio de câmera, sem qualquer notícia no acórdão do Tribunal Regional a respeito de excessos pelo empregador, tais como a utilização de câmeras espiãs ou a instalação de câmeras em recintos que fossem destinados ao repouso dos funcionários ou que pudessem expor partes íntimas dos empregados, como banheiros ou vestiários, não configura ato ilícito, inserindo-se dentro do poder fiscalizatório do empregador. 5 . Nessa medida, não é possível exigir que a empregadora desative as câmeras de vigilância. 6. Configurada a ofensa ao art. 2º da CLT. (...) 5 . Nessa medida, não é possível impor indenização por dano moral coletivo, pois ausente à ilicitude da conduta e o dano. 6. Configurada a ofensa ao art. 5º, X, da CF. Recurso de revista conhecido e provido. (TST - RR: 211625120155040014, Relator: Hugo Carlos Scheuermann, Data de Julgamento: 26/08/2020, 1ª Turma, Data de Publicação: 28/08/2020).

Questões Trabalhistas – Questões Práticas.

Monitoramento de E-Mails Corporativos

RECURSO DE REVISTA. ACÓRDÃO REGIONAL PUBLICADO NA VIGÊNCIA DA LEI Nº 13.015/2014 E ANTERIORMENTE À LEI Nº 13.467/2017. 1. PROVA ILÍCITA. "E-MAIL" CORPORATIVO. ACESSO E UTILIZAÇÃO DO CONTEÚDO DAS MENSAGENS DOS EMPREGADOS PELO EMPREGADOR. POSSIBILIDADE. NÃO CONHECIMENTO. I. Consoante entendimento consolidado neste Tribunal, o e-mail corporativo ostenta a natureza jurídica de ferramenta de trabalho . Daí porque é permitido ao empregador monitorar e rastrear a atividade do empregado em e-mail corporativo, isto é, checar as mensagens, tanto do ponto de vista formal (quantidade, horários de expedição, destinatários etc.) quanto sob o ângulo material ou de conteúdo, não se constituindo em prova ilícita a prova assim obtida. II. Não viola os arts. 5º, X e XII, da Constituição Federal, portanto, o acesso e a utilização, pelo empregador, do conteúdo do "e-mail" corporativo. III. Acórdão regional proferido em consonância ao entendimento desta Corte Superior . IV. Recurso de revista de que não se conhece. 2. (...). (TST - RR: 13474220145120059, Relator: Alexandre Luiz Ramos, Data de Julgamento: 23/06/2020, 4ª Turma, Data de Publicação: DEJT 26/06/2020)

Questões Trabalhistas: Justa Causa – Violação de Segredos da Empresa

"EMENTA: 195/70 - JUSTA CAUSA - VIOLAÇÃO DE SEGREDO DA EMPRESA - CONCORRÊNCIA DESLEAL - Caracteriza justa causa por violação de segredo da empresa e concorrência desleal à prática de atos consistentes em apropriação e comercialização irregular de programas de informática desenvolvidos pela empresa. (TRT 15ªR - Ac. 644/00 - Proc. 29388/98 - 1ª T - Rel. Juiz Eduardo Benedito de Oliveira Zanella - DOESP 18.01.2000)".

"VIOLAÇÃO DE SEGREDO DA EMPRESA - Empregado que remete para terceiro, empregado de concorrente da Ré, documento interno por esta elaborado, comete ato passível de dispensa por justa causa. (TRT-1 - RO: 10035020115010034 RJ , Relator: Giselle Bondim Lopes Ribeiro, Data de Julgamento: 03/09/2012, Nona Turma, Data de Publicação: 11-09-2012)".

LGPD NO TRABALHO

TRT-2 mantém justa causa de empregado que enviou dados sigilosos a conta pessoal

9 de novembro de 2021, 16h50

https://www.conjur.com.br/2021-nov-09/mantida-justa-causa-trabalhador-enviou-dados-sigilosos-mail-pessoal

O empregado que transfere dados sigilosos da empresa a uma conta pessoal incorre em falta disciplinar grave, que enseja a dispensa por justa causa — ainda que não haja dolo e que as informações não sejam repassadas a terceiros.

Com esse entendimento, a 1ª Turma do Tribunal Regional do Trabalho da 2ª Região manteve a dispensa por justa causa aplicada a um atendente de telemarketing que enviou para seu e-mail pessoal uma lista com dados sigilosos de uma empresa de vale refeição, que contratou os serviços de telemarketing. Entre os dados, havia números de CNPJ, CPF e de cartões da vale refeição, além dos valores carregados em cada um deles.

(...)

O desembargador citou a sentença de primeira instância que destacou a importância econômica da extração e publicação de dados atualmente, com menção à Lei Geral de Proteção de Dados Pessoais (LGPD) e à responsabilização civil daqueles que controlam ou operam tais dados.

Por fim, segundo a decisão, não há prova de dolo por parte do trabalhador ou de que havia intenção de transmitir tais dados a terceiros; porém, ainda assim há motivo para a justa causa.

- Investigação dos **Crimes Eletrônicos** no Ambiente Corporativo (Procedimentos e Meios de Prova).

Analise:

Concorrência desleal na internet: Caso Magalu x Via Varejo

Um caso recente de concorrência desleal que vem ganhando os holofotes se refere à Magalu (Magazine Luiza) e a Via Varejo (Casas Bahia, Ponto Frio e Extra).

Ele se baseia no fato de que a Magazine Luiza identificou, próximo à Black Friday 2021, que ao pesquisar as palavras-chave “Magalu” e “Magazine Luiza” o Google apresentava nos resultados algumas concorrentes da rede de varejo.

A partir disso, então, identificou a concorrência desleal. Afinal, nesses casos a Via Varejo utilizou-se de anúncios patrocinados no Google que se baseavam em palavras-chaves que se relacionam a outra marca.

Inclusive, essas palavras possuem registro de marca que se relaciona com a Magazine Luiza. Note que o uso delas por outras marcas vai contra a propriedade que pertence à Magalu. E não só isso! Também busca enganar o cliente.

Dessa forma, atualmente tramita um processo que indica a concorrência desleal da Via Varejo em relação à Magalu. Da mesma maneira, um processo desta última contra a primeira também foi ajuizado pelos mesmos motivos.

Para referência: Processos: 1128548-85.2021.8.26.0100 (Magazine Luiza) e 1130874-18.2021.8.26.0100 (Via Varejo).

Como advogado da Magalu, esclareça para a Diretoria como você pretende comprovar a violação por parte da Via Varejo.

Fontes: https://www.verifact.com.br/concorrencia-desleal-na-internet/ e https://www.migalhas.com.br/quentes/358798/magalu-e-via-varejo-acionam-a-justica-por-concorrencia-desleal.

MEIOS DE PROVA

Código de Processo Civil (CPC):

Art. 369 Todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa.

Código de Processo Penal (CPP):

Art. 155. O juiz formará sua convicção pela livre apreciação da prova produzida em contraditório judicial, não podendo fundamentar sua decisão exclusivamente nos elementos informativos colhidos na investigação, ressalvadas as provas cautelares, não repetíveis e antecipadas.

Art. 157. São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais.

ESPÉCIES DE PROVA

Provas documentais – Qualquer tipo de documento, relatório, fotos, imagens, vídeos, etc.*
Provas orais – Depoimentos das partes e testemunhas.
Provas periciais – Análises sobre determinados fatos, conteúdos de dispositivos eletrônicos e documentos por um perito de confiança do juiz.

*Sobre quebra de sigilo (registro de ligações efetuadas e recebidas), interceptação telefônica (nenhum dos dois interlocutores sabem que a conversa está sendo gravada por um terceiro), escuta telefônica (um dos dois interlocutores sabe que eles estão sendo gravados por um terceiro) e gravação clandestina (um dos interlocutores é quem grava a conversa), importante saber que os três primeiros precisam de autorização judicial.

MEIOS DE PROVA

"A utilidade da prova digital passa necessariamente pela observância de três fatores principais: (i) autenticidade; (ii) integridade; e (iii) preservação de cadeia de custódia. " (Thamay, 2020).

- Por **autenticidade** deve ser entendida a qualidade da prova digital que permite a certeza com relação ao autor ou autores do fato digital. Ou seja, é a qualidade que assegura que o autor aparente do fato é, com efeito, seu autor real.

- **Integridade** deve ser entendida a qualidade da prova digital que permite a certeza com relação à sua completude e não adulteração. A prova digital íntegra é aquela isenta de qualquer modificação em seu estado ou adulteração desde o momento da realização do fato até a apresentação do resultado prova.

- **Cadeia de custódia da prova digital**, ou seja, é preciso preservar a autenticidade e a integridade em todo processo de produção da prova digital, desde sua identificação, coleta, extração de resultados, até a apresentação no processo ou procedimento de destino. A ideia é construir verdadeiro registro histórico da evidência, de toda a vida da prova. A ideia é que se alguém seguir os mesmos passos já dados na produção da prova, o resultado será exatamente o mesmo. Nesse ponto, é importante sinalizar datas, horários, quem teve acesso, onde o acesso foi feito e até quaisquer alterações inevitáveis relacionadas.

THAMAY, Rennan; TAMER, Maurício. **1. Teoria Geral da Prova e a Prova Digital** In: THAMAY, Rennan; TAMER, Maurício. **Provas no Direito Digital: Conceito da Prova Digital, Procedimentos e Provas Digitais em Espécie**. São Paulo (SP):Editora Revista dos Tribunais. 2020. Disponível em: https://www.jusbrasil.com.br/doutrina/provas-no-direito-digital-conceito-da-prova-digital-procedimentos-e-provas-digitais-em-especie/1147564455. Acesso em: 9 de Maio de 2023.

FONTES DE PROVAS NO MEIO DIGITAL

Provas

Logs: Quebra o paradigma de que o anonimato é possível, já que o *log* salva todas as informações de sites que determinado usuário acessou, bem como de que localidade se deu tal acesso.

Endereço de IP ou *Internet Protocol*: Para se conseguir informações sobre um IP dinâmico (onde para cada conexão se atribui um endereço de IP diferente), o investigador deverá, por meio de ordem judicial, solicitar ao Provedor de aplicação (sites, redes sociais, etc.) responsável, informando o dia e hora, para que esta possa localizá-lo, sem isto, fica inviável visto que o número muda constantemente. Por sua vez, ao **acessar um site, uma rede social ou aplicativo, um número IP (data e hora) essas empresas são obrigadas a registrar os usuários que se conectaram.**

Websites: O indicado é imprimir a *interface* daquele *website*, que contenham indícios de *cybercrimes*, e também fazer *downloads* dos conteúdos, com o uso de ferramentas que produzam uma assinatura digital, haja vista que a qualquer momento estes podem ser deletados para tentar dificultar possíveis investigações.

Redes Sociais: Os usuários dessas redes, cada vez mais tem exposto suas vidas, o que tanto facilita o *cybercrimonoso*, como facilita provar alguns *cybercrimes*. Diante destes casos, o investigador deverá, em regra munido de ordem judicial, solicitar às empresas administradoras dessas redes sociais, que forneça os *logs* dos usuários investigados, e, caso seja necessário, poderá também solicitar a interceptação telemática.

Emails: Deve-se primeiro analisar o chamado “cabeçalho”, onde possui o remetente, destinatário, assunto, bem como o IP contendo local, data e hora do envio. O que não significa que será de fácil resolução, já que facilmente pode ser criada uma conta de *e-mail* para disseminar esses crimes. Porém, cabe analisar as informações do IP, a fim de descobrir de onde partiram os envios.

PROVAS.

INVASÃO DE DISPOSITIVO INFORMÁTICO - materialidade – prova oral e documentos acostados aos autos comprovando a invasão do sistema operacional do site da vítima, da obtenção de informações sigilosas e da alteração de dados do sistema. – réu que não se desincumbiu de atestar o alegado – não acolhimento – declaração de vítima apontando o réu como sendo o autor do delito – validade – versão da vítima confirmada pelos e-mails e pelo restante da prova documental acostada aos autos. CAUSA DE AUMENTO – art. 154-A, § 2º, do CP - e-mail, comprovante de depósito e prova oral indicando o prejuízo econômico suportado pela vítima. (TJ-SP 30036070720138260586 SP 3003607-07.2013.8.26.0586, Relator: Lauro Mens de Mello, Data de Julgamento: 24/08/2017, 6ª Câmara de Direito Criminal, Data de Publicação: 29/08/2017).

"*A materialidade do crime restou comprovada através do boletim de ocorrência, dos e-mails acostados aos autos, os quais comprovam a invasão e a ausência de contratação por parte da vítima*, do auto de exibição e apreensão, do laudo pericial, o qual comprova a invasão do computador da vítima, e da prova oral coligida, os quais indicam que houve a invasão do computador da vítima G.A.M. mediante violação de seu mecanismo de segurança, a qual resultou na obtenção de informações sigilosas a seu respeito*."

*Réu alegou que foi contratado pela vítima, a fim de afastar o art. 154-A

PROVAS.

RECURSO ESPECIAL. PROVA OBTIDA DE REGISTRO DE CONVERSAS MANTIDAS VIA APLICATIVO WHATSAPP. COMPUTADOR PERTENCENTE À EMPRESA VÍTIMA. E-MAIL CORPORATIVO. VIOLAÇÃO DO DIREITO A INTIMIDADE. NULIDADE. NÃO OCORRÊNCIA. INTIMAÇÃO ACERCA DA EXPEDIÇÃO DE CARTA PRECATÓRIA. DEFESA CIENTE. NULIDADE RELATIVA. CERCEAMENTO DE DEFESA. INEXISTÊNCIA. QUESTÃO NÃO ARGUIDA NA FASE DE ALEGAÇÕES FINAIS. PRECLUSÃO. AUSÊNCIA DE DEMONSTRAÇÃO DO PREJUÍZO. PRINCÍPIO PAS DE NULLITÉ SANS GRIEF. ALEGADA VIOLAÇÃO DE SÚMULA. IMPOSSIBILIDADE. INCIDÊNCIA DA SÚMULA 518/STJ. RECURSO ESPECIAL CONHECIDO EM PARTE E NÃO PROVIDO. 1. O e-mail corporativo, por se tratar de uma ferramenta de trabalho, fornecida pelo empregador, não se equipara às correspondências pessoais, não havendo falar em violação à intimidade do recorrente quando o empregador acessa arquivo de mensagens que se encontrava em computador utilizado como ferramenta de trabalho e de propriedade da empresa. 2. (....) 5. Recurso especial conhecido em parte e, nessa parte, não provido. (STJ - REsp: 1875319 PR 2020/0117825-7, Relator: Ministro NEFI CORDEIRO, Data de Julgamento: 15/09/2020, T6 - SEXTA TURMA, Data de Publicação: DJe 23/09/2020)

PRODUÇÃO DE PROVAS EM PROCESSOS

Medida Judiciais

Produção Antecipada de Provas – Art. 381/CPC – Medida Preparatória para um Procedimento Judicial.

I - haja fundado receio de que venha a tornar-se impossível ou muito difícil a verificação de certos fatos na pendência da ação;

II - a prova a ser produzida seja suscetível de viabilizar a autocomposição ou outro meio adequado de solução de conflito;

III - o prévio conhecimento dos fatos possa justificar ou evitar o ajuizamento de ação.

O **Marco Civil da Internet** determina que provedor responsável pela guarda somente será obrigado a disponibilizar os registros de forma autônoma ou associados a dados pessoais ou a outras informações para contribuir com a identificação do usuário ou do terminal, **mediante ordem judicial**.

E o prazo de guarda dos registros é por apenas **6 (seis) mese**.

Tutela de Urgência – Art. 300/CPC – Medida adotada no próprio Procedimento Judicial.

A tutela de urgência será concedida quando houver elementos que evidenciem a probabilidade do direito e o perigo de dano ou o risco ao resultado útil do processo.

*Determinar que a parte deixe de fazer ou faça determinada obrigação;

* Exibição de Documentos ou Coisa.

O PROBLEMA DO PRINT SCREEN COMO PROVA.

Art. 422 (CPC). Qualquer reprodução mecânica, como a fotográfica, a cinematográfica, a fonográfica ou de outra espécie, tem aptidão para fazer prova dos fatos ou das coisas representadas, se a sua conformidade com o documento original não for impugnada por aquele contra quem foi produzida.
§ 1º As fotografias digitais e as extraídas da rede mundial de computadores fazem prova das imagens que reproduzem, devendo, se impugnadas, ser apresentada a respectiva autenticação eletrônica ou, não sendo possível, realizada perícia.

Se o *print screen* for impugnado, portanto, a parte que o utilizou no processo terá que fornecer mecanismos para que ele possa ser autenticado. Se a publicação original tiver sido removida, será virtualmente impossível provar a autenticidade do *print screen* sem os referidos metadados, ou mesmo realizar perícia sobre ele. Com isso, a prova pode ser considerada inválida.

Por isso, a utilização de ata notarial. Todavia, a tecnologia Blockchain pode ser utilizada como uma solução mais rápida ou barata.

PRODUÇÃO DE PROVAS: ATA NOTARIAL

ATA NOTARIAL

Ata Notarial – Arts. 364 e 405/CPC - É o **instrumento público** através do qual o tabelião descreve, por seus sentidos, uma determinada situação ou um determinado fato que lhe é apresentado pelo interessado, e o translada para seus livros de notas ou para outro documento.

O art. **364 do CPC** determina que a narrativa dos fatos realizada pelo tabelião, ou seu funcionário, por meio de documento público, goza de fé pública. Possibilita o registro de fatos com um grau de detalhamento e confiabilidade extraordinário, especialmente considerando a possibilidade de ser complementada com documentos contendo registros de imagens e sons dos eventos relatados.

BLOCKCHAIN

O art. 369 do CPC não deixa dúvidas que a utilização da tecnologia *blockchain* não envolve qualquer ilicitude, trata-se de alternativa admitida no direito brasileiro.

Como a utilização da tecnologia *blockchain* ser uma novidade, **recomenda-se as partes ajustarem contratualmente que a comprovação de determinado fato se dará por meio de dados armazenados com tecnologia *blockchain***. Trata-se de negócio jurídico processual lícito (art. 190), ainda que o juiz do processo possa determinar a produção de outros meios de prova.

Dessa forma, o armazenamento de dados com tecnologia *blockchain* faz com que **o ônus da prova, em regra, recaia sobre a parte que contesta a autenticidade das informações**, que, entretanto poderá ser dirimida por todos os meios de prova admitidos em direito, inclusive a pericial.

Veja a matéria: "Magistrada considera válido registro de prova em Blockchain em ação sobre conteúdo ofensivo": https://www.migalhas.com.br/quentes/298803/magistrada-considera-valido-registro-de-prova-em-blockchain-em-acao-sobre-conteudo-ofensivo

BLOCKCHAIN COMO FONTE DE PROVA PROCESSUAL: CASES

Em 2016, o estado de Vermont, nos Estados Unidos, também editou regra probatória sobre o assunto (12 V.S.A. § 1913):

"(1) Um registro digital registrado eletronicamente em tecnologia *blockchain* deverá ser auto-autenticado de acordo com a Vermont Rule of Evidence 902, se for acompanhado por uma declaração escrita de uma pessoa qualificada, feita sob juramento, declarando a qualificação da pessoa para fazer o registro. certificação e:

(A) a data e hora em que o registro entrou no *blockchain*;
(B) a data e hora em que o registro foi recebido do *blockchain*;
(C) que o registro foi mantido no *blockchain* como uma atividade regular conduzida; e
(D) que o registro foi realizado no exercício de atividade regularmente conduzida como uma prática regular".

Texto original, em inglês, disponível em **https://law.justia.com/codes/vermont/2016/title-12/chapter-81/section-1913**

Junho/2018 - Corte da Internet de Hangzhou (China) - considerou que o conteúdo de uma página na internet mantida em serviço de armazenamento com tecnologia *blockchain* por iniciativa da autora consistia em prova suficiente para a condenação do réu por infração à lei de direitos autorais.
Entre outros fatores, considerou-se que (i) a empresa responsável pelo serviço de armazenamento não tinha interesse pessoal no litígio; (ii) que o mecanismo de preservação da prova utilizado pela autora está disponível para todas as pessoas; (iii) que o risco de que as informações tenham sido de alguma forma adulteradas com a utilização da tecnologia *blockchain* era baixo e; (iv) que as informações armazenadas por meio de referida tecnologia eram mantidas de forma descentralizada em várias máquinas (https://go.dennemeyer.com/hubfs/blog/pdf/Blockchain%2020180726/20180726_BlogPost_Chinese%20Court%20is%20first%20to%20accept%20Blockchain_Judgment_EN_Translation.pdf?t=1533233132812).

Setembro/2018 - Suprema Corte Popular da China editou regra explícita, admitindo a tecnologia *blockchain* ou análoga como fonte de prova nos processos judiciais em curso nas cortes de Internet daquele país:

> *"As cortes de internet reconhecerão dados digitais que são submetidos como evidência, caso as partes interessadas tenham coletado e armazenado estes dados por meio de blockchain com assinatura digital, registros de tempo confiáveis e verificação de valor de hash, ou por meio de uma plataforma de depósito digital, que seja capaz de provar a autenticidade de tal tecnologia utilizada"*

- Regulamentos Internos em **Cibersegurança**.

Lei Geral de Proteção de Dados e a Segurança da Informação

Principais Dispositivos da LGPD Relacionados com a Segurança da Informação

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

Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I - o modo pelo qual é realizado;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.

Lei Geral de Proteção de Dados e a Segurança da Informação

Principais Dispositivos da LGPD Relacionados com a Segurança da Informação

Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

PADRÕES FRAMEWORKS E CONTROLES DE SEGURANÇA CIBERNÉTICA

Normas de Segurança da Informação	Normas para Proteção de Dados
ABNT NBR ISO/IEC 27001:2013 — Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos.	**ABNT NBR ISO/IEC 27701:2019** — Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes;
ABNT NBR ISO/IEC 27002:2013 — Tecnologia da Informação — Técnicas de Segurança — Código de Prática para controles de segurança da informação;	**ABNT NBR ISO/IEC 29134: 2020** - Tecnologia da Informação – Técnicas de Segurança – Avaliação de Impacto de Privacidade – Diretrizes
ABNT NBR ISO/IEC 27005:2011 — Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação;	**ABNT NBR ISO/IEC 29151; 2020** - Tecnologia da Informação – Técnicas de Segurança – Código de Prática para Proteção de Dados Pessoais
ABNT NBR ISO/IEC 31000:2018 — Gestão de riscos – Diretrizes.	

Opção – Uso do NIST: https://www.nist.gov/cyberframework/related-programs

ANPD – GUIA ORIENTATIVO DE SEGURANÇA DA INFORMAÇÃO PARA AGENTES DE TRATAMENTO DE DADOS DE PEQUENO PORTE.

Em outubro/2021 a ANPD publicou o Guia de orientação de segurança da informação para agentes de tratamento de pequeno porte.

*Microempresas e Empresas de Pequeno Porte;
* Startups
*Microempreendedor individual; e
*Organizações sem fins lucrativos.

- https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf

- O guia indica medidas administrativas e técnicas de segurança da informação e um checklist para facilitar a visualização das sugestões que serão adotadas (https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/checklist-vf.pdf)

SEGURANÇA DA INFORMAÇÃO – APLICAÇÃO COMO MEIO DE PROVA

DIREITO DO CONSUMIDOR. RESPONSABILIDADE CIVIL. INTERMEDIAÇÃO DE VENDAS EM SITE DA INTERNET. AUSÊNCIA DE DEFEITO NA PRESTAÇÃO DE SERVIÇOS. SEGURANÇA DA INFORMAÇÃO. 1 - Na forma do art. 46 da Lei 9.099/1995, a ementa serve de acórdão. Recurso próprio, regular e tempestivo. Pretensão condenatória de reparação por danos materiais, em virtude de fraude em venda em site da internet. Recurso do autor visa à reforma da sentença que julgou improcedente o pedido. 2 - Responsabilidade Civil. Fraude em compra em plataforma de comércio eletrônico. Mercado livre. **O fornecedor de serviços responde pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, salvo se comprovar a culpa exclusiva do consumidor ou de terceiros (art. 14, § 3º, do CDC).** O autor contratou os serviços de intermediação de venda do Mercado Livre (plataforma de comércio eletrônico) para alienar seu aparelho telefônico. Alega ter recebido e-mails falsos confirmando o pagamento e a compra do produto, razão pela qual enviou o aparelho telefônico ao suposto comprador. **No caso, houve negligência por parte do autor em não observar se, de fato, houve a realização do pagamento do produto. Os procedimentos de segurança não foram seguidos pelo autor, que presumiu a realização do pagamento unicamente pelo e-mail fraudulento, sem confirmar em sua conta no Mercado Livre.** Há, ainda, suspeita de que o autor tenha fornecido seu e-mail a terceiro, conforme mensagem juntada pelo recorrido (ID 11727245 - Pág. 12). **Ademais, não há demonstração de que ocorreu defeito na segurança que a ré disponibiliza aos seus usuários, razão pela qual não se vislumbra falha na prestação de serviço**. Assim, uma vez que o prejuízo suportado decorreu de culpa exclusiva do autor e de terceiro, não se mostra devida a reparação por danos materiais. Sentença que se confirma pelos seus próprios fundamentos. 3 - Recurso conhecido, mas não provido. Custas processuais e honorários advocatícios, fixados em 20% do valor da causa, pelo recorrente vencido. (TJ-DF 0724579-87.2019.8.07.0016, Relator: AISTON HENRIQUE DE SOUSA, Data de Julgamento: 13/12/2019, Primeira Turma Recursal, Data de Publicação: Publicado no DJE : 27/01/2020 . Pág.: Sem Página Cadastrada.)

APELAÇÃO. AÇÃO INDENIZATÓRIA. Prestação de serviços. Direito do Consumidor. Autor que realizou anúncio de venda no site da ré. Recebimento de e-mail fraudulento indicando a compra do produto. Envio realizado pelo autor**. Inobservância, pelo autor, dos Termos e Condições de uso do site**. Regras claras indicando que o produto só deve ser enviado após o cômputo do valor da compra na conta mantida junto ao site da ré. **Disponibilização de informações claras e exaurientes, no site da ré, acerca de e-mails falsos e formas de identificação de fraudes. Descumprimento dos termos de uso, por parte do autor**, que foi elemento único e determinante para o sucesso da fraude. Inexistência de responsabilidade da ré, diante de fato exclusivo do consumidor, nos termos do artigo 14, §3º, inciso II, do CDC. Dever de indenizar afastado. Sentença mantida. Recurso não provido.
(TJ-SP - 1005178-61.2018.8.26.0072, Relator: Ana Lucia Romanhole Martucci, Data de Julgamento: 14/09/2020, 33ª Câmara de Direito Privado, Data de Publicação: 15/09/2020)

LGPD - PRINCIPAIS DOCUMENTOS

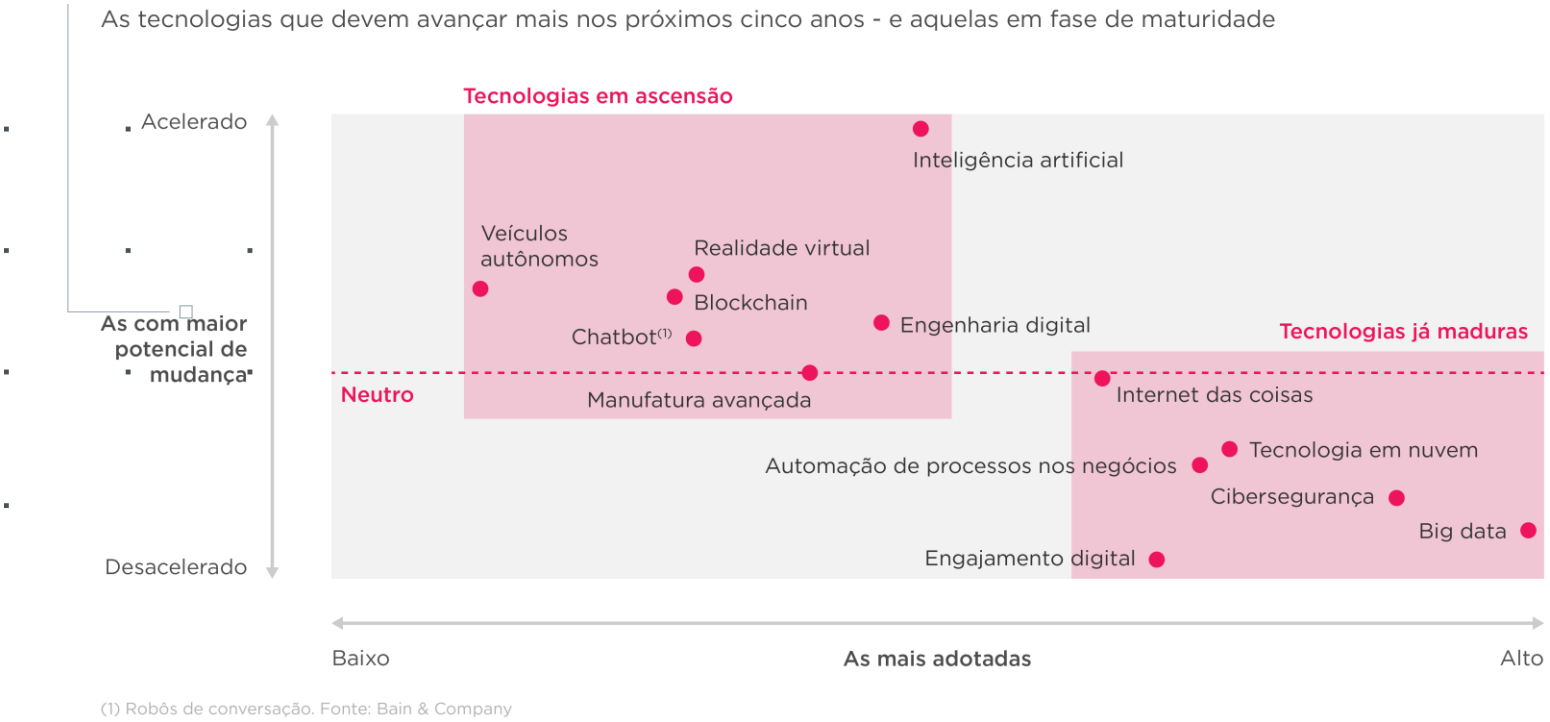
Documento	Objetivo
Política Corporativa de Proteção de Dados Pessoais	Documento com todas as diretrizes a serem adotadas pela Companhia no tratamento de Dados Pessoais.
Inventário de Tratamento de Dados Pessoais (ou ROPA – Registro das Atividades de Tratamento para LGPD)	Processo de rastreamento e inventários dos dados coletados e tratados dentro da organização. É exigido pela LGPD aos controladores e operadores (art.37). https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd. Guia para elaboração do inventário de tratamento de dados pessoais: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_inventario_dados_pessoais.pdf. Modelo de Resgistro das Operações de Tratamento de Dados Pessoais para Agentes de Tratamento de Pequeno Porte (ATPP): https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/modelo_de_ropa_para_atpp.pdf
Plano de Resposta para Incidentes com dados pessoais	Documento que estabelece as regras internas para comunicação de incidente com dados pessoais ao Encarregado, para que possa ser avaliado (inclusive se deve ser comunicado à Autoridade e Titulares), bem como direcionar os procedimentos para contenção e erradicação do problema e, ainda, recuperação de dados e serviços (Planos de Continuidade dos Negócios e Recuperação de Desastres). Define os comitês de crise.
Comunicado sobre incidentes para a sociedade e para a Agência Nacional de Proteção de Dados	As informações mínimas necessárias para a comunicação de incidentes de segurança estão previstas no parágrafo 1º, do artigo 48, da LGPD, são elas: (i) descrição da natureza dos dados pessoais afetados; (ii) informações sobres os titulares envolvidos; (iii) indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados; (iv) riscos relacionados ao incidente; (v) motivos da demora, no caso de a comunicação não ter sido imediata; e (vi) medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. Apesar de não ter sido expedido nenhum normativo do órgão sobre o tema, ao disponibilizar o formulário, a ANPD indicou o prazo de 02 (dois) dias úteis, contado da ciência do evento adverso, como razoável para a comunicação do incidentes.
Termos de Privacidade para funcionários e operadores.	Fundamental para contratação de funcionários e prestadores de serviços estarem cientes com as medidas de proteção de dados da organização. Inclui as principais responsabilidades jurídicas, direitos, deveres, segurança, disponibilidade e confincialidade.

LGPD - PRINCIPAIS DOCUMENTOS

Documento	Objetivo
Política de Segurança da Informação (PSI)	São as regras que ditam o acesso, o controle e a transmissão da informação em uma organização. É obtida pela implantação de uma gama de controles que incluem procedimentos de rotina (como as verificações de antivírus), infraestrutura de hardware e software, sua documentação como classificação da informação, redes, cloud, armazenamento físico, backup e restore, criptografia, BYOD, anonimização, entre outros.
Relatório de Impacto à Proteção de Dados	É 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. Em seu artigo 38, a Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei nº 13.709/2018, dispõe que a ANPD (Autoridade Nacional de Proteção de Dados) poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, observados os segredos comercial e industrial. Ainda, a referida Autoridade poderá solicitar ao Controlador a elaboração do RIPD, quando o tratamento for realizado com base em seu legítimo interesse (artigo 10, § 3º, LGPD), bem como para os agentes do Poder Público, com base no artigo 32 da LGPD.
Termos e Condições de Uso	Equiparam-se a um contrato de adesão, ou seja, aquele que não dá espaço para o assinante questionar as cláusulas ou pedir para que estas sejam alteradas. Assim, o consentimento do titular dos dados incide sobre os Termos de Uso. O usuário ou aceita ou Termos de Uso ou não terá como ter acesso ao produto ou serviço que está na plataforma digital que o titular está adentrando.
Política de Privacidade	A política objetiva dar visibilidade ao tratamento de dados pessoais em um determinado serviço, atendendo a princípios da Lei Geral de Proteção de Dados Pessoais (LGPD), endereçado aos usuários de um site, serviço ou sistema (titulares de dados), antes do início do tratamento dos seus dados pessoais, permitindo, quando aplicável, que o titular avalie se deseja que aquele agente efetue o tratamento de seus dados pessoais.

COMENTÁRIOS À LGPD

POR QUE OS DADOS PESSOAIS SÃO IMPORTANTES ?



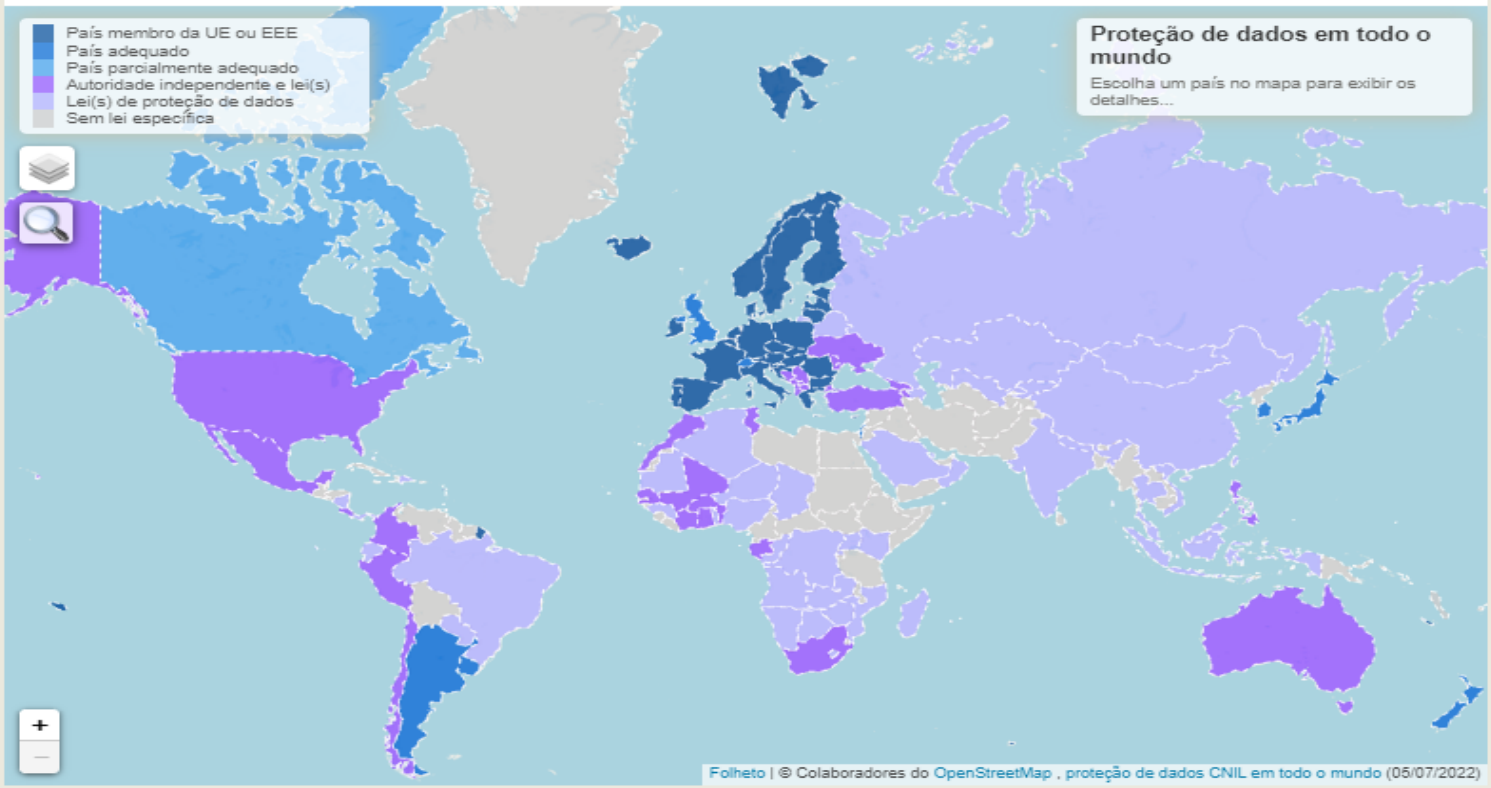
https://exame.abril.com.br/revista-exame/as-tendencias-evoluem/ – 26/09/2019

SÓ NO BRASIL EXISTE LEI DE PROTEÇÃO DE DADOS PESSOAIS ?

FIAP MBA+

CNIL.

MINHAS FERRAMENTAS DE CONFORMIDADE | PROTEÇÃO DE DADOS | TÓPICOS | O CNIL |



PROTEÇÃO E TRATAMENTO DE DADOS NO MUNDO

FIAP MBA+

ESTADOS UNIDOS	EUROPA (GDPR) 2018 DATA PROTECTION ACT (UK)
Caráter liberal - matéria regulada em contrato	Caráter Protetivo - Matéria Regulada em Legislação.

- Em 03/04/2017 Pres. Trump cancela leis sobre privacidade dos consumidores na internet. Estados podem legislar sobre o assunto (ex.: California Consumer Privacy Act CCPA – em vigor em janeiro/2020 – bem como lei similares em em todos os estados, mas voltadas para o consumidor. Em julho/20, foi também aprovada uma lei em Nova Iorque, a New York Stop Hacks and Improve Electronic Data Security Act - NY SHIELD).
- Mas existem algumas lei nacionais: Health Insurance Portability and Accountability Act (HIPAA), que exige que informações médicas de pacientes sejam protegidas, garantindo a privacidade e a segurança de dados pessoais;
- Children's Online Privacy Protection Act (COPPA), que regulamenta o uso e a coleta de informações relativas a crianças menores de 13 anos sem o consentimento dos pais, ou a Telemarketing Sales Rules (TSR), que estabelece normas e restrições para as ações de telemarketing.

GDPR está em vigor em todos os países-membros. É regulamento geral. Cada País membro da CE possui sua própria legislação, que obedece à norma geral, mas pode ser mais ou menos severa em determinados aspectos.

Opt-Out – Provedores e outros podem utilizar os dados, salvo se houver impedimento por parte do consumidor.	Opt-In - Exige consentimento prévio para uso dos dados pessoais.

PROTEÇÃO E TRATAMENTO DE DADOS NA AMÉRICA LATINA

PAÍS	LEGISLAÇÃO
ARGENTINA	Lei nº 25.326/2000 – A legislação atual da Argentina protege os dados pessoais armazenados em todas as plataformas de processamento públicas ou privadas. Além disso, os cidadãos têm acesso às suas informações em bancos de dados públicos.
CHILE	Lei nº 19.628/1999 – Está em análise no parlamento chileno uma nova legislação.
COLÔMBIA	Lei nº 15.821/2012 – Exige que todos os bancos de dados sejam registrados no Registro Nacional de Bancos de Dados. A atual legislação colombiana inclui a proteção dos direitos dos usuários, a criação de obrigações para quem coleta e gerencia dados, a regulamentação da proteção de dados pessoais financeiros e de crédito e o controle do Registro Nacional de Bancos de Dados.
MÉXICO	Lei Federal Mexicana de Proteção de Dados Pessoais em Poder de Particulares, de 2010.
PERU	Lei nº 29.733/2011 – A estrutura de proteção de dados pessoais do Peru tem como foco proteger os direitos dos sujeitos e garantir o cumprimento das obrigações das empresas de processamento de dados.
URUGUAI	Lei nº 18.331/2008.

QUANDO A LGPD ENTRA EM VIGOR ?

- A Lei Geral de Proteção de Dados – Lei nº 13.709/2018 (LGPD) entrou em vigor no dia 18/09/2020.
- Ou seja: agora, qualquer cidadão, titular dos dados pessoais, poderá questionar as empresas privadas ou órgãos públicos sobre como é feito o tratamento da sua informação pessoal. O Ministério Público, a SENACON (Secretaria Nacional do Consumidor), o PROCON e entidades coletivas, como o IDEC, também poderão promover ações contra as empresas, pedindo providências e indenizações por danos morais coletivos.
- Por outro lado, somente em 1º de Agosto de 2021, a Autoridade Nacional de Proteção de Dados (ANPD) passou a poder advertir e autuar as empresas.

TRATAMENTO DE DADOS PESSOAIS NA MÍDIA

LGPD: Justiça confirma liminar e determina que Serasa deixe de comercializar dados pessoais

por CS — publicado em https://www.tjdft.jus.br/institucional/imprensa/noticias/2021/julho/lgpd-justica-determina-que-serasa-deixe-de-comercializar-dados-pessoais

O juiz substituto da 5ª Vara Cível de Brasília confirmou decisão liminar da 2ª Turma Cível do TJDFT que determinou que a Serasa Experian pare de comercializar dados pessoais dos titulares por meio dos produtos **Lista Online** e **Prospecção de Clientes**, oferecidos pelo site da ré, sob pena de imposição das medidas para assegurar o cumprimento da ordem judicial, conforme legislação vigente.

O órgão ministerial afirma que o contratante dos serviços recebe uma ou mais bases de dados de contatos com informações como CPF, nome, endereço, telefones e sexo. O serviço pode ser segmentado por meio do uso de filtros, dentro de um universo potencial de 150 cinquenta milhões de CPFs. Destaca que essa **exposição generalizada é capaz de gerar um grande vazamento de dados**. Por último, ressalta o risco de utilização indevida dos referidos dados durante o período eleitoral.

O entendimento do magistrado é o de que a **comercialização de dados pessoais por meio dos produtos oferecidos pela ré é ilícita**, tal como concluíram os desembargadores do TJDFT, quando da concessão da tutela de urgência para suspensão da comercialização dos serviços, em maio deste ano. "A partir do desenvolvimento tecnológico, da economia mais voltada ao âmbito digital e das possibilidades concretas de tratamento de dados pessoais, é evidente o relevo do valor econômico das informações sobre a coletividade, pois relevantes para o objetivo institucional de várias instituições, públicas e privadas", pontuou o julgador.

A decisão ressalta, ainda, que o tratamento e o compartilhamento dos referidos dados, na forma como é feito pela ré, exigiria o **consentimento claro e expresso do indivíduo retratado**, condição para viabilizar o fluxo informacional realizado, com caráter manifestamente econômico. No caso dos autos, inexiste o indispensável consentimento em relação à universalidade de pessoas catalogadas.

(TJDFT - Proc. 0736634-81.2020.8.07.0001).

Principais Multas LGPD até o momento (SENACON)

Empresa	Valor
Facebook (Dez-2019)	R$ 6,6 milhões
Banco Itaú Consignado S.A.	R$ 9,6 milhões
CETELEM S.A.	R$ 4,0 Milhões
Banco Pan	R$ 8,8 milhões
Droga Raia/Drogasil (MT)	R$ 572 mil

Multa ao Facebook: https://brunobioni.com.br/wp-content/uploads/2020/01/SEI_08012.000723_2018_19-1-1.pdf

TRATAMENTO DE DADOS PESSOAIS NA MÍDIA

ANPD aplica a primeira multa por descumprimento à LGPD

A Coordenação-Geral de Fiscalização (CGF/ANPD) concluiu processo administrativo sancionador que resultou em aplicação de sanções de multa e de advertência por ofensas à Lei Geral de Proteção de Dados.

Publicado em 07/07/2023 14h29 Atualizado em 13/07/2023 09h32

Fonte: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd

A Coordenação-Geral de Fiscalização da ANPD (CGF/ANPD) publicou no Diário Oficial da União de ontem (06/07) sanção decorrente da conclusão de processo administrativo sancionador contra a empresa Telekall Infoservice (acesse aqui a publicação no DOU).

A CGF/ANPD concluiu que a empresa infringiu os arts. 7º e o 41 da LGPD, além do art. 5º do Regulamento de Fiscalização da ANPD.

Para a infração ao art. 7º da LGPD e ao art. 5º do Regulamento de Fiscalização foram aplicadas sanções de multa simples. O descumprimento ao art. 41 da Lei resultou em sanção de advertência.

Por se tratar de uma microempresa, o valor para cada infração ficou limitado a 2% do seu faturamento bruto, conforme art. 52, II, da LGPD, totalizando uma multa de R$14.400,00.

A fiscalização foi iniciada a partir de denúncia de que a empresa Telekall Infoservice estaria ofertando uma listagem de contatos de WhatsApp de eleitores para fins de disseminação de material de campanha eleitoral. Os fatos denunciados foram relativos à eleição municipal de 2020, em Ubatuba/SP.

A ANPD verificou que o tratamento de dados pessoais denunciado estava ocorrendo sem respaldo legal. Foi apurada ainda a falta de comprovação da indicação de encarregado pelo tratamento de dados pessoais pela empresa.

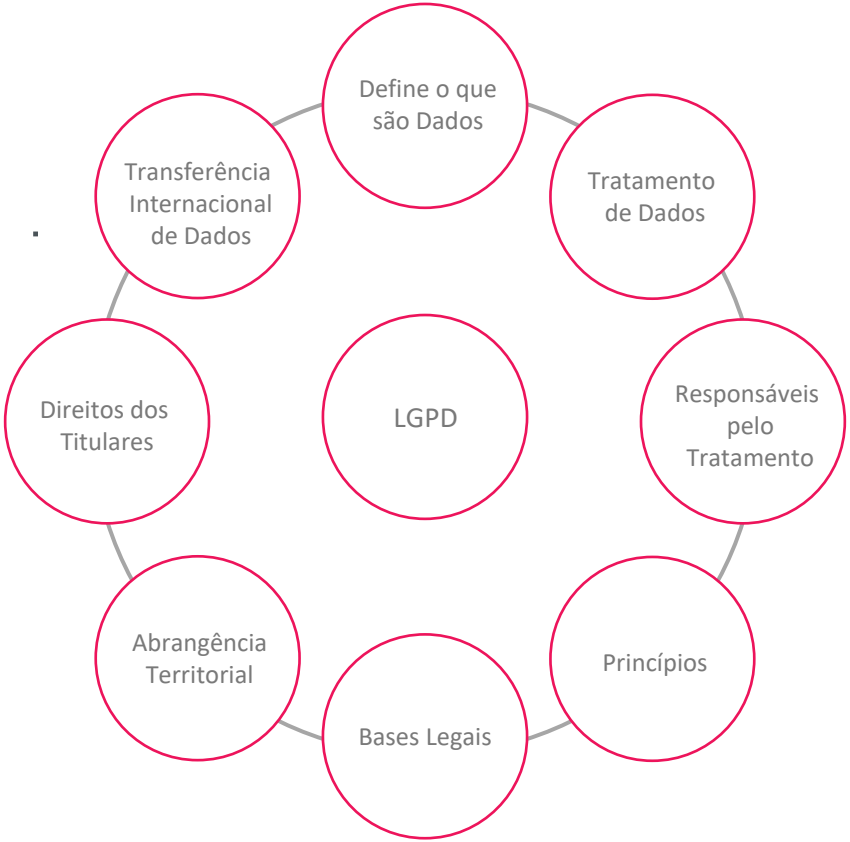
Embora seja uma microempresa, a Telekall não comprovou que não fazia tratamento de alto risco, condição necessária para excepcionalizar a exigência de designação do encarregado.

Diante dos indícios de infração à LGPD e do não atendimento de determinações da equipe de fiscalização pela empresa, a CGF/ANPD lavrou Auto de Infração, iniciando o Processo Administrativo Sancionador.

A Telekall Infoservice foi notificada da lavratura de Auto de Infração e apresentou sua defesa. Encerrada a instrução, a CGF/ANPD concluiu pela ocorrência de infração ao art. 7º e ao art. 41 da LGPD, e art. 5º da Resolução CD/ANPD nº 1/2021, aplicando as sanções acima descritas. O mesmo regulamento prevê a possibilidade de recurso da decisão ao Conselho Diretor da Autoridade.

Relatório que ensejou a autuação: https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_inforservice.pdf

O QUE MUDA COM A LGPD?



QUEM DEVE OBSERVAR A LGPD

- Devem observar a Lei: a pessoa natural, que realiza tratamento de dados pessoais para fins econômicos, ou por pessoa jurídica de direito público ou privado, que realiza tratamento de dados pessoais para qualquer fim.

A QUEM A LGPD NÃO SE DESTINA

Não se aplica:

a) Pessoa natural que realiza tratamento de dados pessoais para fins exclusivamente particulares e não econômicos.

b) Para fins exclusivamente:

i. jornalísticos e artísticos;

ii. acadêmicos, na hipótese dos arts. 7º e 11 da LGPD;

iii. pra fins de segurança pública, defesa nacional, segurança do Estado ou atividade de investigação e repressão de infrações penais (que deverão ser regidos por legislação especifica); e

iv. provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD.

DIREITO AO ESQUECIMENTO x LGPD

- Em 2021, o STF julgou um processo em que familiares da vítima de um crime de grande repercussão nos anos 1950, no Rio de Janeiro, buscavam reparação pela reconstituição do caso, em 2004, no programa “Linha Direta”, da TV Globo, sem a sua autorização, sob pretexto de direito ao esquecimento.

- Em outro caso, um médico postulou, com base no direito ao esquecimento, sustentando também o pleito nos artigos 17 e 18 da LGPD e no Enunciado 531 da VI Jornada de Direito Civil, a exclusão de matéria jornalística que relatava sua condenação por porte de drogas no passado e, ainda, a desindexação da referida matéria por provedor de buscas. O TJSP refletiu de forma curiosa sobre o deferimento do pleito em face do provedor de busca, aplicando a LGPD a essa hipótese e determinando a desindexação do conteúdo objeto da ação eis que comprovada a reabilitação após o cumprimento de pena, é assegurado o sigilo dos registros do condenado, aí incluído o direito à desindexação do conteúdo gerado.

- Artigo 17 - Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

- Artigo 18 - O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

IV - Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei".

DIREITO AO ESQUECIMENTO x LGPD – Liberdade de expressão e direito à informação x privacidade

STF - Recurso Extraordinário (RE) 1010606:

- "É incompatível com a Constituição Federal a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e licitamente obtidos e publicados em meios de comunicação social – analógicos ou digitais. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais, especialmente os relativos à proteção da honra, da imagem, da privacidade e da personalidade em geral, e as expressas e específicas previsões legais nos âmbitos penal e cível".

ABRANGÊNCIA TERRITORIAL

- A LGPD aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

- a) a operação de tratamento seja realizada no território nacional, **com exceção ao tratamento de dados provenientes de fora do território nacional**;

- b) os dados pessoais objeto do tratamento tenham sido coletados no território nacional (consideram-se dados coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta) e;

- c) a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos **localizados** no território nacional.

DADOS PESSOAIS

DADOS PESSOAIS

- Informação relacionada à pessoa natural identificada ou identificável (titular dos dados pessoais).
- Dados pessoais são informações relativas a uma pessoa viva, identificada ou identificável. Também constitui dados pessoais o conjunto de informações distintas que podem levar à identificação de uma determinada pessoa.
- **Exemplos: Nome, RG, CPF, Data de Nascimento, Número da Carteirinha, Endereço**.

DADOS PESSOAIS SENSÍVEIS

- 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.
- **Exemplos: Dados de Saúde do Cliente (informações sobre doenças, deficiências, riscos de doenças, relatório médicos, prontuários, resultados de exames, dados biométricos, informações genéticas, etc.**

DADOS PESSOAIS

DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES

- Para o tratamento, é necessário o consentimento específico e em destaque de pelo menos um dos pais ou do responsável legal (art. 14, §1º). Cabe ao controlador, com base nas tecnologias disponíveis, empreender todos os esforços razoáveis para confirmar que o consentimento de fato tenha sido dado por um dos pais ou pelo responsável legal (art. 14, §5º).

- **Exemplos**: **Dados dos dependentes menores de idade.**

DADOS ANONIMIZADOS

- Dados pessoais relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento, como por exemplo estatísticas, KPIs, relatórios sobre processos, índices de desempenho.

- Dados pessoais que tenham sido descaracterizados, codificados ou pseudonimizados, mas que possam ser utilizados para identificar uma pessoa, continuam a ser dados pessoais e são abrangidos pelo âmbito de aplicação do LGPD.

Dados Anonimizados e Pseudononimizados: Principais Aplicações:

Anonimização

- **Melhoria dos produtos**: Os relatórios estatísticos, que não contém dados pessoais, podem ser usados para melhorar as informações sobre seu cliente ou medir a audiência ou desempenho do seu produto, por exemplo.
- **Desenvolvimento de novos produtos**: Os dados anonimizados podem auxiliar no desenvolvimento de novos produtos, a partir da identificação do comportamento dos indivíduos, sem que seja necessário identificá-los.
- **Treinamento de algoritmos**: Dados sintéticos, ou seja, dados artificialmente criados a partir de situações do mundo real, podem ajudar no treinamento de algoritmos. Tais dados são anonimizados, pois os fatores identificativos são retirados e substituídos por dados sintéticos

Pseudonimização

- **Compartilhamento de informações internas**: Sempre que as demais áreas de negócios da empresa, que precisam ser envolvidas em procedimentos internos para atendimento ao cliente, não precisarem ter acesso aos dados pessoais do indivíduo, a pseudonimização dos dados pessoais pode ser uma medida sugerida.

- **Segurança**: As técnicas de pseudonimização são medidas adicionais de segurança. A dissociação de dados identificadores ou passíveis de identificação, e a criação de uma chave de identificação mantida separadamente, podem proteger os indivíduos e suas informações

DADOS PÚBLICOS

- A lei cita “dados pessoais cujo acesso é público”.
- A Lei de Acesso à Informação (LAI) e princípios constitucionais estabelecem que *“todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado”*.
- A LGPD define, por exemplo, que uma organização pode, sem precisar pedir novo consentimento, tratar dados tornados, anterior e manifestamente, públicos pelo titular (desde que fundamentado em uma das bases legais da Legislação).

RESPONSÁVEIS PELO TRATAMENTO DE DADOS

CONTROLADOR	OPERADOR
Administração de ciclo de vida do dado pessoal por base jurídica de tratamento;	Administração de ciclo de vida do dado pessoal com base no contrato de prestação de serviços;;
Necessidade de enquadramento do tratamento em base jurídica;	Observar as obrigações contratuais;
Decide sobre o dado pessoal;	É obrigado a perguntar sobre qualquer omissão ou obscuridade contratual;
Operacionaliza o atendimento do Titular;	Não responde pelos direitos do Titular diretamente;
Responde civilmente em todos os casos.	Responde por seus atos, pelo descumprimento da lei e pela desobediência ao contrato.

Art. 37. *O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse*.
A ANPD divulgou em 28/05/2021 o Guia Orientativo Sobre Agentes de Tratamento de Dados e Pessoais e do Encarregado: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-guia-orientativo-sobre-agentes-de-tratamento-e-encarregado

O art. 28 da GDPR (adaptado para LGPD, como referência).

•O tratamento de dados por Operador é regulado por contrato ou outro ato normativo ao abrigo da Legislação, que vincule o Operador ao responsável pelo tratamento, estabeleça o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e direitos do responsável pelo tratamento. Esse contrato ou outro ato normativo estipulam, designadamente, que o Operador:

a) Trata os dados pessoais apenas mediante instruções documentadas do responsável pelo tratamento, incluindo no que respeita às transferências de dados para países terceiros ou organizações internacionais, a menos que seja obrigado a fazê-lo pela legislação a que está sujeito, informando nesse caso o responsável pelo tratamento desse requisito jurídico antes do tratamento, salvo se a lei proibir tal informação por motivos importantes de interesse público;

b) Assegura que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;

c) Adota todas as medidas de segurança da informação exigidas na legislação;

d) O Operador oferece garantias suficientes de execução de medidas técnicas e organizativas adequadas para contratar outro operador (Suboperador) e não contrata outro operador sem que o responsável pelo tratamento tenha dado, previamente e por escrito, autorização específica ou geral;

e) Toma em conta a natureza do tratamento, e na medida do possível, presta assistência ao responsável pelo tratamento através de medidas técnicas e organizativas adequadas, para permitir que este cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos seus direitos;

f) Presta assistência ao responsável pelo tratamento no sentido de assegurar o cumprimento das obrigações tendo em conta a natureza do tratamento e a informação ao dispor do Operador;

g) Consoante a escolha do responsável pelo tratamento, apaga ou devolve-lhe todos os dados pessoais depois de concluída a prestação de serviços relacionados com o tratamento, apagando as cópias existentes, a menos que a conservação dos dados seja exigida ao abrigo do direito da legislação vigente; e

h) Disponibiliza ao responsável pelo tratamento todas as informações necessárias para demonstrar o cumprimento das obrigações previstas na legislação e facilita e contribui para as auditorias, inclusive as inspeções, conduzidas pelo responsável pelo tratamento ou por outro auditor por este mandatado.

i) Que o Operador informará imediatamente o responsável pelo tratamento se, no seu entender, alguma instrução violar a legislação vigente em matéria de proteção de dados.

J) Se o Operador contratar outro Operador (Suboperador) para a realização de operações específicas de tratamento de dados por conta do responsável pelo tratamento, são impostas a esse outro Operador (Suboperador) , por contrato as mesmas obrigações em matéria de proteção de dados que as estabelecidas no contrato ou outro ato normativo entre o responsável pelo tratamento e o Operador.

O ENCARREGADO

- Pessoa, indicada pelo controlador e operador, que atua como canal de comunicação entre o controlador e os titulares e o órgão competente.
  Obs. Na Europa é denominado DPO (Data Protection Officer).
- O texto original da LGPD previa que o encarregado seria “pessoa natural”. No entanto, a Medida Provisória nº 869 (atual Lei nº 13.853/2019) a palavra “natural” foi suprimida. Dessa forma, passou-se a admitir que empresas atuem como DPO, sem exclusão legal de uma ou outra possibilidade.
- A identidade e as informações de contato do DPO deverão ser divulgadas publicamente, de forma clara e objetiva, no site do Controlador.

O ENCARREGADO: Job Description

Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências

Orientar funcionários e contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

Receber Comunicações da ANPD e adotar providencias

Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

A ANPD publicou a Resolução CD/ANPD nº 2/2022, que regulamenta o tratamento jurídico diferenciado da LGPD para agentes de tratamento de pequeno porte (MEI, ME, EPP, startups, entidades sem fins lucrativos e pessoa naturais, desde que não realizem tratamento de dados em larga escala ou com dados que possam afetar interesses e direitos fundamentais dos titulares.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

- É o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

- A Autoridade Nacional atuará tanto com a fiscalização dos agentes de tratamento, quanto com a instrução dos titulares, tendo, como uma das suas competências, “promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança”. Compete também à ANPD a elaboração de diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, com a finalidade de nortear os agentes de tratamento para que atuem em conformidade com as normas.

- Papel similar (não são totalmente iguais) a EUROPEAN DATA PROTECTION SUPERVISOR (EDPS), Information Commissioner's Office - ICO (UK) e as demais autoridades nacionais europeias.

EXEMPLOS DE REGRAS DA LGPD PENDENTES DE REGULAMENTO DA ANPD.

- Padrões e técnicas utilizadas em processos de anonimização (art. 13, § 3°);
- Regras para elaboração do Relatório de Impacto à Proteção de Dados Pessoais (art. 38, caput);
- Prazo para comunicação de incidente de segurança (art. 48, § 1°);
- Prazo para solução de reclamação do titular (art. 55-J, inc. V);
- Normas de adequação progressiva de bancos de dados constituídos até a data de entrada em vigor da lei (art. 63).
- Definição de acesso a dados pessoais e de práticas de segurança para adequação de ambiente controlado e seguro no qual os dados serão tratados para fins de estudos de saúde pública por órgãos de pesquisa (art. 13, caput e § 3°);
- Termos e formato para atendimento de solicitação, pelo titular, de cópia eletrônica integral de dados pessoais coletados com base no consentimento ou contrato (art. 19, § 3°);
- Prazo diferenciado para atendimento de requisição de confirmação de existência ou de acesso a dados pessoais em formato simplificado ou completo para setores específicos (art. 19, § 4°);
- Padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados, segurança e tempo de guarda dos registros de operações de tratamento (art. 40);

ATENDIMENTO AOS DIREITOS DOS TITULARES DE DADOS

DIREITOS DOS TITULARES DE DADOS
Confirmação da existência de tratamento.
Acesso aos dados e finalidade do tratamento.
Correção de dados incompletos, inexatos ou desatualizados
Informação das entidades públicas e privadas com as quais o Controlador realizou uso compartilhado de dados.
Informação sobre a possibilidade de não fornecer consentimento e sobre consequências da negativa
Revogação do consentimento, nos termos do § 5.º do art. 8.º da Lei.
Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD.
Compartilhamento ou Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da Autoridade Nacional, observados os segredos comercial e industrial.
Eliminação dos dados pessoais tratados com o consentimento do(a) titular, exceto nas hipóteses previstas no art. 16 da Lei.

ATENDIMENTO AOS DIREITOS DOS TITULARES DE DADOS

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, **autorizada** a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

DECISÕES AUTOMATIZADAS

Art. 20. **O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade**.

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

TRATAMENTO DE DADOS

CASE: Maiores Multas Aplicadas na Europa

Empresa	Caso	Multa
Amazon	O regulador europeu reconheceu que a Amazon, usando a assistente virtual Alexa, coletou dados sobre vendedores e compradores no site, sem pedir seu consentimento. Posteriormente, as informações foram repassadas a terceiros.	**746 milhões de euros**
WhatsApp	A comissão de proteção de dados da Irlanda multou o WhatsApp em razão da forma como o app compartilhava dados com o Facebook.	225 milhões de euros
Google	Esse foi um dos primeiros grandes episódios da GDPR contra as Big Techs. Em 2019, a Google foi sentenciada a pagar uma generosa multa na França após falhar em dizer a seus usuários no país como seus dados seriam usados para publicidade.	50 milhões de euros
H&M	A companhia gravava entrevistas com funcionários que voltavam de licença, repleta de dados pessoais e médicos, e compartilhava o material com toda a gerência sem aprovação do trabalhador.	35 milhões de euros
TIM	Autuada na Itália, por conta de uma série de acusações, incluindo ligar mais de 155 vezes para um consumidor em potencial em apenas um mês.	27,8 milhões de euros

CASE: CNIL (FRANÇA) X GOOGLE

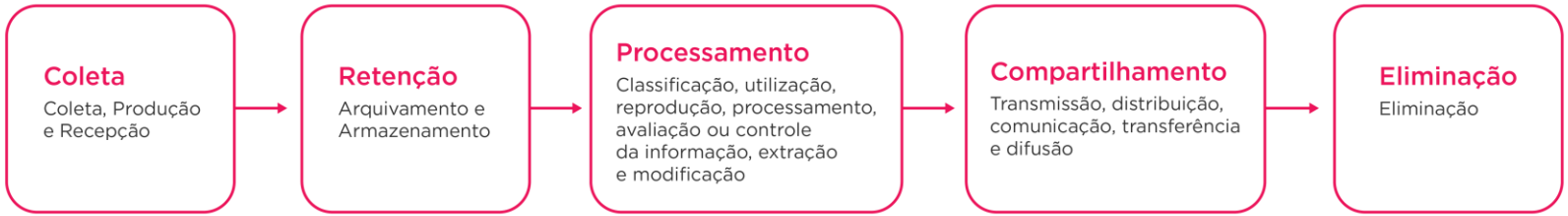
CASE: CNIL (FRANÇA) X GOOGLE

- **Esta decisão também foi importante**, pois o Conselho de Estado Francês , na sua decisão de 19 de junho de 2020 , validou a decisão da CNIL, afastando a alegação da Google LLC sobre a competência do CNIL, eis que a unidade europeia, localizada na República da Irlanda, não teria tomado as decisões de processamento de dados, que teria sido determinadas pela matriz nos EUA, razão pela qual a CNIL não teria jurisdição para aplicar a sanção. Esta decisão abriu a possibilidade para que diversas autoridades nacionais, como por exemplo a autoridade sueca, viesse a autuar a Google também.

TRATAMENTO DE DADOS PESSOAIS E O CICLO DE VIDA DOS DADOS PESSOAIS

(FASES DO CICLO DE TRATAMENTO X ART. 5º, X, LGPD)

- O ciclo de vida de dados envolve as informações obtidas por uma empresa ou instituição, desde sua coleta até a sua devida destruição.
- Para implementar o correto tratamento de dados pessoais, o agente de tratamento deve conhecer os dados pessoais que gerencia e quais processos, projetos, serviços e ativos que existem no ciclo de vida do tratamento de dados pessoais.



Princípios do Tratamento de DADOS PESSOAIS

FINALIDADE	Apenas coletar dados pessoais para fins legítimos, informando com clareza o usuário a finalidade da coleta.
ADEQUAÇÃO	A Atividade de tratamento de dados deve ser compatível com a finalidade informada ao titular.
NECESSIDADE	Manter e utilizar apenas os dados essenciais, excluindo (ou anonimizando) os dados quando deixarem de ser relevantes.
LIVRE ACESSO	Ser capaz de apresentar ao titular os dados e a forma como são processados ao serem requisitados.
QUALIDADE	Manter os dados exatos e atualizados, segundo a necessidade do tratamento.
USO NÃO DISCRIMINATÓRIO	Não utilizar os dados para fins discriminatórios, ilícitos ou abusivos.
TRANSPARÊNCIA	Informar ao titular, com informações claras e acessíveis, sobre o tratamento e seus responsáveis.
PREVENÇÃO	Os sistemas utilizados para o tratamento de dados pessoais devem atender aos requisitos de segurança, aos padrões de boas práticas e de governança, aos princípios da Lei e às demais normas regulamentares.
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.
RESPONSABILIDADE	O Agente de tratamento deve demonstrar a eficácia das medidas e procedimentos adotados para o tratamento. Segundo a lei, as infrações serão aplicadas de forma inversamente proporcional ao que foi feito para proteção dos dados .

CONCEITOS DE PRIVACY BY DESIGN E PRIVACY BY DEFAULT

Privacy by Design

Privacy by Design significa que **todas as etapas** do processo de desenvolvimento de um produto ou serviço de uma empresa devem ter a **privacidade em primeiro lugar**.

O conceito de privacidade deve estar totalmente embutido no projeto, e não se aplica à iniciativas em que a privacidade é discutida somente na fase final.

- Privacidade deve ser o padrão dos sistemas de TI ou práticas de negócio (**Privacy By Default**).
- Proativo, e não reativo; preventivo, e não corretivo.
- Segurança e proteção de ponta a ponta durante o ciclo de vida de tratamento dos dados.
- Visibilidade e Transparência.
- Respeito pela privacidade do usuário.

Privacy by Default

A ideia de *Privacy by Default* (privacidade por padrão) significa que um produto ou serviço, ao ser lançado no mercado, deve ser entregue com a configuração de privacidade mais restritiva possível, de modo a que **apenas os dados indispensáveis sejam coletados**, cabendo ao próprio usuário, se assim desejar, habilitar de maneira informada e voluntária outras funcionalidades que ampliem o espectro de tratamento de seus dados pessoais.

A maioria das grandes empresas de tecnologia fazem justamente o contrário disso, ou seja, coletam o máximo de informações possíveis por padrão, mas **permitem que o usuário desative** a coleta de dados. Caso Privacy by Default fosse aplicado, **os aplicativos coletariam somente o necessário e permitiriam que o usuário ativasse a coleta de dados extras, caso achasse benéfico**.

FONTES:
AUTORIDADE ESPANHOLA: Gestión del riesgo y evaluación de impacto en tratamientos de datos personales (aepd.es)
AUTORIDADE NORUEGUESA: https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/data-protection-by-design-and-by-default/ .

TRATAMENTO DE DADOS PESSOAIS

- A empresa GURU comercializa maquiagens e artigos de luxo nos principais shoppings do mundo. Para estreitar o relacionamento com suas clientes, a GURU solicita, no momento do pagamento da compra, o nome completo e o endereço de e-mail para “envio de promoções”. Não há quaisquer outros esclarecimentos. Geralmente, a cliente não se opõe a tal pedido.

- Internamente, os dados recolhidos pela GURU também são encaminhados para outros parceiros comerciais que também comercializam artigos de luxo diferentes dos comercializados pela GURU, como automóveis, serviços vips para pets e hospedagem cinco estrelas.

- **O tratamento de dados pessoais realizado pela GURU é adequado?**

BASES LEGAIS PARA JUSTIFICAR O TRATAMENTO DE DADOS

DADOS ORDINÁRIOS	DADOS SENSÍVEIS
CONSENTIMENTO	CONSENTIMENTO
LEGÍTIMO INTERESSE	**GARANTIA DE PROTEÇÃO À FRAUDE E Á SEGURANÇA DO TITULAR EM CADASTROS SE SISTEMAS ELETRÔNICOS**
PROTEÇÃO AO CRÉDITO	
EXECUÇÃO DE CONTRATOS	
OBRIGAÇÃO LEGAL OU REGULATÓRIA	OBRIGAÇÃO LEGAL OU REGULATÓRIA
EXERCÍCIO REGULAR DE DIREITOS	EXERCÍCIO REGULAR DE DIREITOS
TUTELA DA SAÚDE	TUTELA DA SAÚDE
EXECUÇÃO DE POLÍTICAS PÚBLICAS DEFINIDAS PELA ADMINISTRAÇÃO PÚBLICA	EXECUÇÃO DE POLÍTICAS PÚBLICAS DEFINIDAS PELA ADMINISTRAÇÃO PÚBLICA
PROTEÇÃO À VIDA	PROTEÇÃO À VIDA
ESTUDOS POR ÓRGÃOS DE PESQUISA	ESTUDOS POR ÓRGÃOS DE PESQUISA

O CONSENTIMENTO

- A base da LGPD é o consentimento: ou seja, é necessário solicitar a autorização do titular dos dados, antes do tratamento ser realizado.
- E esse consentimento deve ser recebido de forma explícita e inequívoca. Não precisa ser escrito, mas o Controlador deve ter meios de provar que recebeu o consentimento (meio auditável, como por exemplo, logs).
- O não consentimento é a exceção: só é possível processar dados, sem autorização do cidadão, quando isso for indispensável para cumprir situações legais, previstas na LGPD e/ou em legislações anteriores, como a Lei de Acesso à Informação (LAI).
- Por exemplo, uma organização – pública ou privada – pode, sem precisar pedir novo consentimento, tratar dados tornados, anterior e manifestamente, públicos pelo cidadão.

O CONSENTIMENTO – Considerações relevantes.

Check Box em branco solicitando consentimento do titular para o tratamento de dados.

Não vincular o oferecimento do serviço à disponibilização do consentimento (exceto nas hipóteses em que o consentimento é efetivamente obrigatório para o tratamento).

Mensagem informando ao titular a possibilidade de revogar o consentimento.

Informações específicas sobre a finalidade do tratamento de dados.

Envio de e-mail aos responsáveis pelo menor solicitando confirmação quanto ao tratamento de dados.

Mecanismos que dificultem a revogação do consentimento pelo titular

TRATAMENTO DOS DADOS COM BASE EM LEGÍTIMO INTERESSE

*Para atender aos **interesses legítimos do controlador** ou de terceiro. Para efeitos de aplicação o legítimo interesse deve:*

- Ser lícito (ou seja, deve respeitar a legislação nacional aplicável.
- Ser definido de forma suficientemente clara para permitir a realização do teste de ponderação em relação aos interesses e aos direitos fundamentais do titular dos dados pessoais.
- Representar um interesse real e atual (ou seja, não deve ser especulativo – situação concreta).
- https://www.uc.pt/site/assets/files/475840/20140409_wp_217_parecer_6_2014_conceito_interesses_legitimos_resp_trat_diretiva_95.pdf

***Não prevalece, sobre direitos e liberdades fundamentais do titular.**

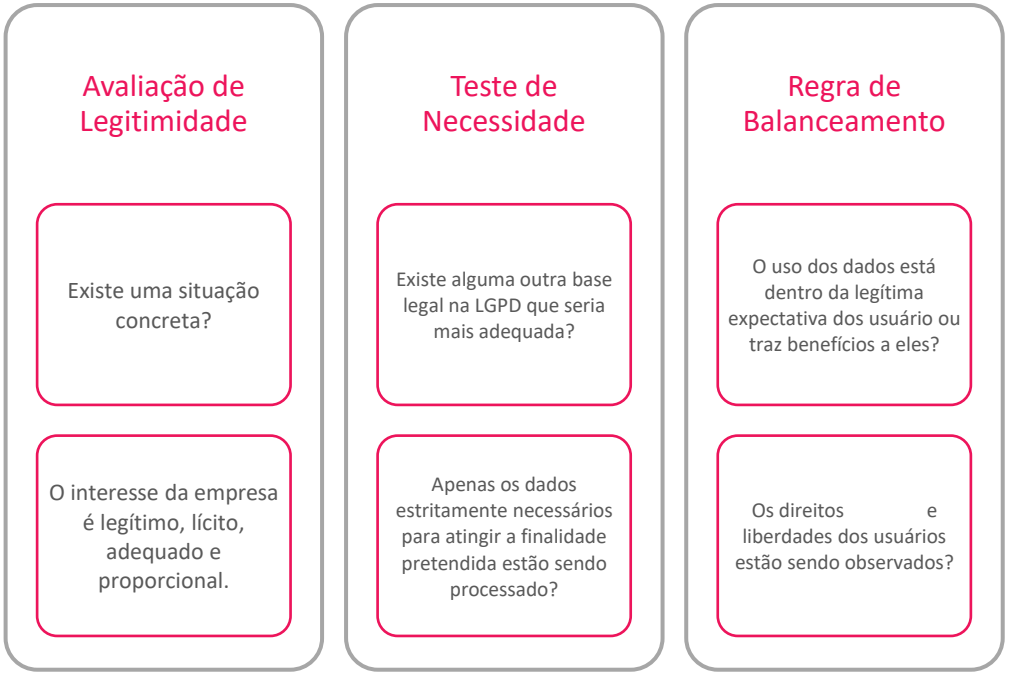
***O titular dos dados pessoais espera:**

***a) um benefício em seu favor e/ou;**

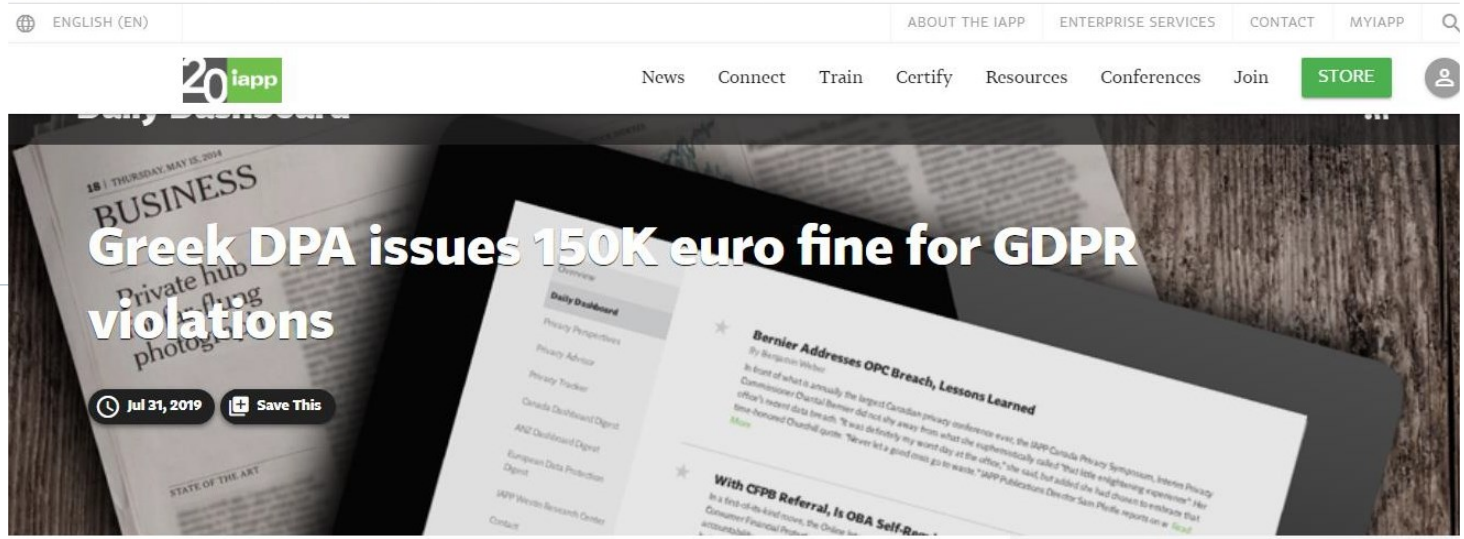
***b) existe uma legitima expectativa que autoriza o controlador realizar o tratamento de dados pessoais.**

*** Somente utilizar os dados pessoais necessários para o tratamento.**

TRATAMENTO DOS DADOS COM BASE EM LEGÍTIMO INTERESSE (Teste de Ponderação aplicado no LIA – Legitimate Interests Assessment)



CASE: HELLENIC DPA X PWC



CASE: ANÁLISE DO LEGÍTIMO INTERESSE

A Empresa **Enlight Tech** é uma subsidiária da Empresa **Lumina Inc.** A Empresa **Enlight Tech** não tem um departamento de RH, pois essa função é desempenhada centralmente na Empresa Lumina Inc. A Empresa **Enlight Tech** deseja confiar em legítimos interesses como base legal para transmitir dados de funcionários à Empresa **Lumina Inc,** sobre a) licenças médicas, b) levantamento sobre as doenças que acometeram seus funcionários, c) impacto destas doenças no desempenho dos colaboradores (faltas), para fins de administração eficiente do RH do grupo. Atenção, não há médico do trabalho envolvido neste caso.

A empresa **Enlight Tech** , entretanto, precisa considerar se a transferência desses dados é realmente necessária para esse propósito e, em seguida, equilibrar isso contra os interesses dos indivíduos, antes que eles possam ter certeza de que o processamento é legal com base em legítimos interesses.

- **Você entende se a transferência de dados acima é possível por legítimo interesse?**
- **Haveria outra base legal para justificar o tratamento?**
- **O envio de dados poderia ser efetuado de outra forma?**

TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS

Pode ser efetuada:

- **Quando Autorizada pelo titular ou a ANPD autorizar a transferência**.
- **Quando o pais de destino deva ter adequado grau de proteção e relativa cooperação jurídica internacional (Está previsto na LGPD que o nível de proteção de dados do país estrangeiro ou do organismo internacional será avaliado pela ANPD (Art. 34).**
- **Quando o Controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos. do titular e do regime de proteção de dados previsto na LGPD.**
- **Quando a transferência resultar de compromissos assumidos em acordos de cooperação internacional ou necessária para a execução de políticas públicas ou atribuições do serviço público.**
- **Quando Proteção da vida ou incolumidade física do titular, ou**
- **É necessária para** atender as hipóteses previstas nos incisos II, V e VI do Art. 7º da LGPD (Art. 33, IX, da LGPD), isto é respectivamente: **para o cumprimento de obrigação legal ou regulatória pelo Controlador, 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 e para o exercício regular de direitos em processo judicial, administrativo ou arbitral**.

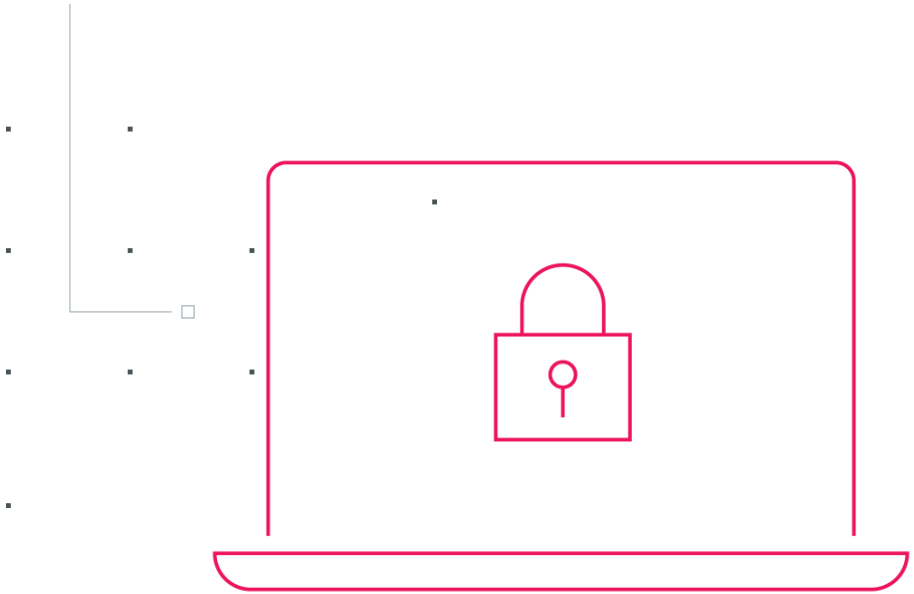
PENALIDADES: O QUE ACONTECE SE EU NÃO CUMPRIR A LGPD?

A partir de 1º de Agosto de 2021, a Autoridade Nacional de Proteção de Dados (ANPD) poderá advertir e autuar as empresas:

- Advertência, com indicação de prazo para adoção de medidas corretivas;
- Multa simples, de até 2% 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 milhões por infração;
- Multa diária, observado o limite total a que se refere o inciso ii;
- Publicização da infração após devidamente apurada e confirmada a sua ocorrência (Danos à Reputação da Empresa);
- Suspensão parcial do funcionamento do banco de dados por até 6 meses
- Proibição parcial ou total das atividades relativas ao tratamento de dados, até a regularização da atividade de tratamento pelo controlador
- Eliminação dos dados

O BÁSICO DA ADEQUAÇÃO À LGPD

POLÍTICA DE PRIVACIDADE



Política

de Privacidade

Nós levamos sua

privacidade a sério.

POLÍTICA DE PRIVACIDADE

A política de privacidade é um dos instrumentos de implementação do *privacy by design* e faz parte da estrutura de documentos para a proteção de dados.

A política objetiva dar visibilidade ao tratamento de dados pessoais em um determinado serviço, atendendo a princípios da Lei Geral de Proteção de Dados Pessoais (LGPD), endereçado aos usuários de um site, serviço ou sistema (titulares de dados), antes do início do tratamento dos seus dados pessoais, permitindo, quando aplicável, que o titular avalie se deseja que aquele agente efetue o tratamento de seus dados pessoais

POLÍTICA DE PRIVACIDADE

Conteúdo	Informações sobre a organização responsável pelo tratamento.
	Destinatário da Política, dados pessoais coletados e respectivas finalidades do tratamento, inclusive os dados não informados pelo usuário (exemplo: IP, localização etc.).
	Base jurídica do tratamento e quando houver tratamento de dados com fundamento no legítimo interesse, esclarecimentos acerca da justificativas para este tratamento.
	Prazo de retenção dos dados pessoais.
	Informações de contato do *Data Protection Officer* (DPO) ou encarregado de proteção de dados da organização.
	A versão e a data de atualização da política de privacidade e se possível, disponibilizar um repositório com as versões anteriores.
Outras questões relevantes	Sobre compartilhamento dos dados com terceiros e qual a finalidade, inclusive redes sociais;
	Sobre transferência internacional e qual a finalidade;
	Sobre o envio de e-mail marketing e como remover o consentimento, quando autorizado inicialmente pelo titular;
	Sobre decisões automatizadas;
	Sobre a proteção de dados de menores de idade;
	Sobre a proteção dos dados sensíveis.

POLÍTICA DE PRIVACIDADE

PwC: Política de Privacidade.

Política de Privacidade e Proteção de Dados - Cielo

IoT e Implicações Jurídicas

MARCO REGULATÓRIO DA IOT NO BRASIL: DECRETO Nº 9.854, DE 25.6.2019 - ATUAÇÃO

Tem por objetivo melhorar a qualidade de vida das pessoas e promover ganhos de eficiência nos serviços, por meio da implementação de soluções de IoT nos seguintes setores:

- Cidades: Elevar a qualidade de vida dos moradores, gestão integrada dos serviços em mobilidade, segurança e uso racional de recursos naturais e produtivos.
- Saúde: Ampliação do acesso à saúde no Brasil, melhoria da eficiência das unidades de saúde, visão integrada dos pacientes e descentralização da atenção à saúde.
- Rural: Aumento de produtividade e relevância mundial do Agronegócio do Brasil
- Industrias: Incentivar a produção de itens mais complexos e com alto valor agregado e melhorar a performance produtiva.

MARCO REGULATÓRIO DA IOT NO BRASIL: DECRETO Nº 9.854, DE 25.6.2019 - QUESTÕES TRIBUTÁRIAS

Serviço de Valor Agregado

O Decreto nº 9.854 estabeleceu que IoT é a infraestrutura que integra a prestação de **serviços de valor adicionado** com capacidades de conexão física ou virtual de coisas com dispositivos baseados em tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade.

Tributação

Com isso, afastou a incidência do ICMS-Comunicação sobre os serviços prestados em relação ao IoT (provável cobrança do ISS, com base na LC 106/03 - item 1.03 - *Processamento, armazenamento ou hospedagem de dados, textos, imagens, vídeos, páginas eletrônicas, aplicativos e sistemas de informação, entre outros formatos, e congêneres*, utilizado para tributar serviços como SaaS e IaaS.

Taxa de Fiscalização de Instalação

O Decreto nº 9.854, manteve a cobrança da Taxa de Fiscalização de Instalação das estações móveis do Serviço Móvel Pessoal, do Serviço Móvel Celular ou de outra modalidade de serviço de telecomunicações.

Todavia, a **Lei nº 14.108, de 16 de dezembro de 2020,** isenta os equipamentos M2M da Taxa de Fiscalização de Instalação, da Taxa de Fiscalização de Funcionamento, do Condecine, e isenta de licença prévia de funcionamento estas estações de IoT, de **01/01/2021 a 31/12/2025**.

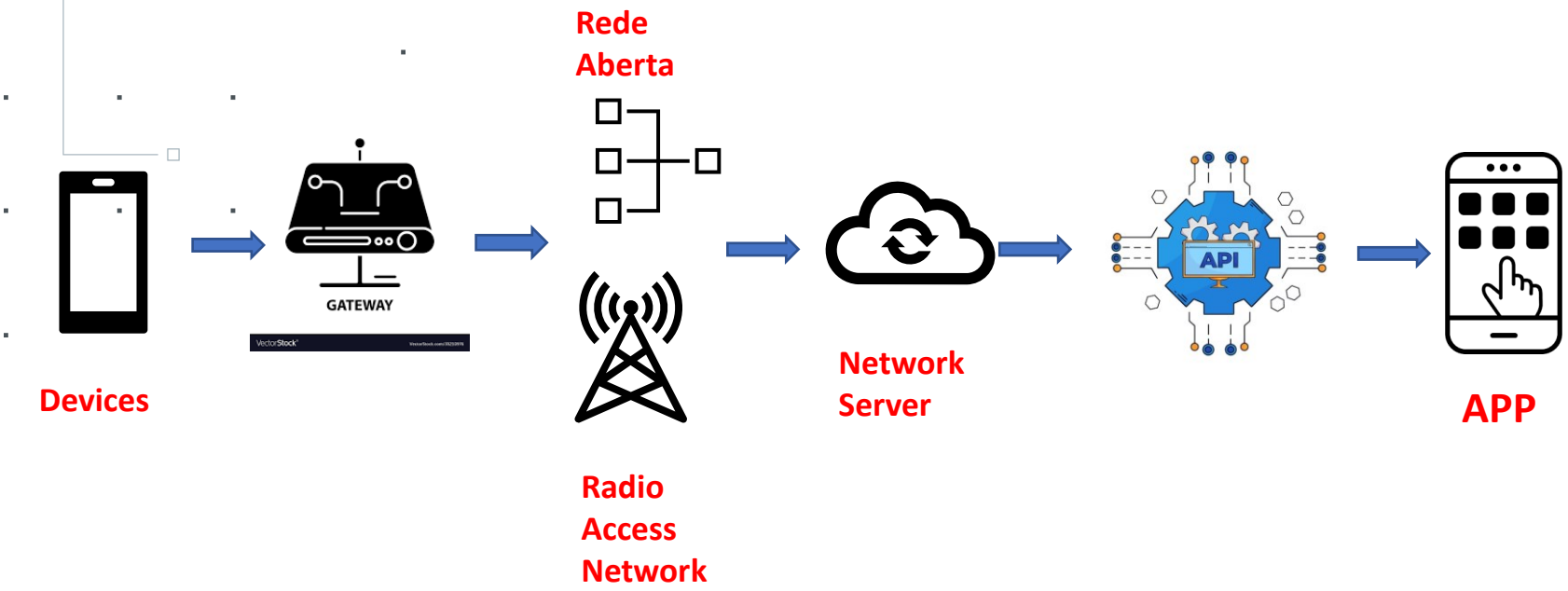
IoT e Implicações Jurídicas

Fonte: https://www.exin.com/br-pt/sera-a-internet-das-coisas-iot-imune-a-lgpd/

- A ideia básica da IoT é a fusão de tecnologias como a própria Internet, *Cloud Computing, RFID (Radio-Frequency IDentification), ZigBee*, inteligência artificial, *Machine Learning,* dentre outras aplicações que visam atender às demandas do mercado em geral.

- Com o advento de tecnologia de sensores mais baratos e de menor potência, evolução dos conceitos e técnicas de conectividade (em especial comunicações móveis), plataformas de computação em nuvem (que trazem consigo mobilidade e menores custos de manutenção), tecnologias de análises de dados em massa como Machine Learning, Big Data e inteligência artificial, a IoT ganhou força e se espalhou em projetos pelo mundo.

- No Brasil, atualmente, o grande problema enfrentado pelas empresas fornecedoras de IoT é o enquadramento do serviço como de telecomunicações (Telecom) ou de valor agregado (SVA).



IoT e LGPD

o Plano Nacional de Internet das Coisas define, em seu primeiro artigo, que terá como finalidade implementar e desenvolver a Internet das Coisas no país, com base na livre concorrência e na livre circulação de dados, observadas as diretrizes de segurança da informação e de proteção de dados pessoais. Deve-se então observar a Lei Geral de Proteção de Dados Pessoais (LGPD).

Os projetos de IoT, assim como quaisquer outros que contenham dados pessoais, deverão:

- **estar preparados para serem transparentes.**
- **possuir ferramentas que permitam a modificação de dados inexatos, impedir acréscimo de dados inexistentes, exclusão dos dados que estão ali sem o prévio consentimento do titular (desde que não haja amparo legal para tal);**
- **em caso de uma ocorrência de violação de dados, deve gerar trilhas de auditoria que permitam saber o que aconteceu, quando, por que e quem violou os dados.**
- **Definir as suas bases de dados de acordo com a finalidade da coleta de dados, adequação do tratamento e espécie de dados coletados.**

Direito em Inteligência Artificial

Caso Prático:

Em março/2018, uma mulher atravessava uma rua carregando uma bicicleta em Tempe, no Arizona, quando foi atingida por um carro da UBER que estava testando seu modo de direção autônomo. A vítima morreu em decorrência dos ferimentos.

Considere as seguintes premissas:

A vítima atravessou a rua fora da faixa de pedestre, por volta das 23 horas.

A Família da vítima processou a UBER (desenvolvedora do sistema de condução autônoma) e a Volvo (fabricante do veículo). Durante o processamento do feito, a UBER alegou que os sistemas estavam funcionando normalmente, mas a sensibilidade do software não entendeu a situação, eis que a mulher atravessou fora da faixa de pedestre, à noite, carregando uma bicicleta, sendo, portanto, uma situação inusitada em que a IA não “entedeu” a situação. A UBER ainda chamou à lide o motorista de backup que estava no veículo, responsabilizando este pois o mesmo deveria ter ficado atento para o ocorrido e poderia ter evitado o acidente.

Na sua opinião, quem deve ser responsabilizado pelo acidente acima noticiado?

INTELIGÊNCIA ARTIFICIAL – LEGISLAÇÃO A CAMINHO - OCDE

Em 22 de maio de 2019 - aprovado pelos 36 países membros da OCDE, em conjunto com a Argentina, o Brasil, a Colômbia, a Costa Rica, o Perú e a Roménia, conjunto de políticas orientadoras no âmbito da Inteligência Artificial , com as recomendações da OCDE identificam cinco princípios orientadores-base que se complementam e devem ser tidos em conta:

- A IA deve beneficiar o **desenvolvimento sustentável e o bem estar geral**.
- Os sistemas de IA devem ser concebidos de forma a respeitar **o estado de direito, os direitos humanos, os valores democráticos e a diversidade**.
- Os sistemas de IA devem ser **transparentes e assegurar uma divulgação responsável**, de modo a garantir que as pessoas compreendam os resultados provenientes do seu uso e possam geri-los corretamente.
- Os sistemas de IA devem **funcionar de forma robusta e segura**, durante todo o seu ciclo de vida. Os seus potenciais riscos devem ser continuamente avaliados e geridos.
- As organizações e **os indivíduos que desenvolvem, implantam ou operam sistemas de IA devem assegurar o seu bom funcionamento**, em conformidade com os princípios acima referidos.

INTELIGÊNCIA ARTIFICIAL – PARLAMENTO EUROPEU SALTA NA FRENTE

O Parlamento Europeu (PE), em 21/10/2020, está entre as primeiras instituições a apresentar recomendações sobre o que as regras da inteligência artificial (IA) devem incluir em matéria de ética, responsabilidade e direitos de propriedade intelectual. Estas recomendações abrem caminho para que a UE se torne líder mundial no desenvolvimento da IA. A proposta legislativa da Comissão é esperada para os próximos anos (https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/excellence-and-trust-artificial-intelligence_pt)

Um código ético para a IA

É preciso encontrar o equilíbrio entre a proteção dos cidadãos e a promoção do desenvolvimento tecnológico por meio de princípios orientadores, nomeadamente:

(i) correção de erros em decisões em âmbito da AI;

(ii) evitar o uso intrusivo da AI; e

(iii) Defeitos de concepção em sistemas de IA podem resultar em discriminação para determinadas pessoas.

Risk-based regulatory approach

- **A abordagem regulatória tem como premissa principal a hierarquização dos riscos oferecidos por sistemas e tecnologias que usam IA.**
- **Ao limitar as obrigações ao mínimo necessário para enfrentar o problema dos riscos atrelados à IA, a proposta da Comissão caracteriza-se por uma intervenção legal mínima, de forma a não embotar o desenvolvimento tecnológico ou criar custos desnecessários ao comércio de dispositivos e equipamentos artificialmente inteligentes**

Classificação dos Riscos

- "**Risco inaceitável**" (unacceptable risk): Será proibido tudo o que for considerado uma clara ameaça para os cidadãos da UE: desde a classificação social por parte dos governos aos brinquedos que utilizam a assistência vocal para incentivar crianças a adotarem comportamentos perigosos
- "**risco elevado**" (high-risk): neste caso as exigências regulatórias aumentam muito, passando pela obrigação de documentação, rastreabilidade, supervisão humana e outras imposições indispensáveis para mitigar consequências danosas aos usuários
- "**risco limitado**" (limited risk): Os sistemas de IA como os robôs de conversação (chatbots) estão sujeitos a obrigações mínimas de transparência, destinadas a permitir que aqueles que interagem com os conteúdos tomem decisões com conhecimento de causa. O utilizador pode então decidir continuar ou deixar de utilizar a aplicação.
- **risco mínimo**" (minimal risk) –a tolerância é quase plena, com pequenas exigências de transparência, como jogos de vídeo ou filtros de correio eletrônico não solicitado (spam) baseados na IA.

INTELIGÊNCIA ARTIFICIAL – LEGISLAÇÃO A CAMINHO - EUA

- A **Lei da Iniciativa Nacional de IA de 2020** (DIVISÃO E, SEC. 5001) tornou-se lei em 1º de janeiro de 2021, fornecendo um programa coordenado em todo o governo federal para acelerar a pesquisa e a aplicação de IA para a prosperidade econômica e a segurança nacional da nação. A missão da National AI Initiative é garantir a liderança contínua dos EUA em pesquisa e desenvolvimento de IA, liderar o mundo no desenvolvimento e uso de IA confiável nos setores público e privado e preparar a força de trabalho atual e futura dos EUA para a integração da IA sistemas em todos os setores da economia e da sociedade.

INTELIGÊNCIA ARTIFICIAL – LEGISLAÇÃO A CAMINHO - BRASIL

- A Câmara dos Deputados aprovou no final de 2021 a PL 21/2020, que estabelece princípios, direitos e deveres para o uso de inteligência artificial no Brasil, e dá outras providências.

- Todavia, o Presidente do Senado, ao escutar diversos setores econômicos, entendeu que seria melhor constituir uma comissão de juristas para subsidiar a elaboração de uma minuta de substitutivo que culminou no PL 2338/2023.

- Conceitos (**Agentes de Inteligência Artificial)**:

➢ **Fornecedor de sistema de Inteligência Artificial**: pessoa natural ou jurídica, de natureza pública ou privada, que desenvolva um sistema de Inteligência Artificial, diretamente ou por encomenda, com vistas a sua colocação no mercado ou a sua aplicação em serviço por ela fornecido, sob seu próprio nome ou marca, a título oneroso ou gratuito;

➢ **Operador de sistema de Inteligência Artificial**: pessoa natural ou jurídica, de natureza pública ou privada, que empregue ou utilize, em seu nome ou benefício, sistema de Inteligência Artificial, salvo se o referido sistema for utilizado no âmbito de uma atividade pessoal de caráter não profissional;

➢ **Autoridade competente**: órgão ou entidade da Administração Pública Federal responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional a ser designada pelo Poder Executivo.

INTELIGÊNCIA ARTIFICIAL – LEGISLAÇÃO A CAMINHO - BRASIL

PL 2338/23 – Principais Pontos

Considera inteligência artificial o sistema computacional, com graus diferentes de autonomia, desenhado para inferir como atingir um dado conjunto de objetivos, utilizando abordagens baseadas em aprendizagem de máquina e/ou lógica e representação do conhecimento, por meio de dados de entrada provenientes de máquinas ou humanos, com o objetivo de produzir previsões, recomendações ou decisões que possam influenciar o ambiente virtual ou real.

Esta Lei não se aplica aos processos de automação exclusivamente orientados por parâmetros predefinidos de programação que não incluam a capacidade do sistema de aprender a perceber e a interpretar o ambiente externo, bem como a interagir com ele, a partir das ações e das informações recebidas

INTELIGÊNCIA ARTIFICIAL – PL 2338/23 – Principais Pontos

Avaliação do Impacto Algorítmico	A metodologia da avaliação de impacto conterá, ao menos, as seguintes etapas: (a) preparação; (b) cognição do risco; (c) mitigação dos riscos encontrados; e (d) monitoramento. A autoridade competente será notificada sobre o sistema de alto risco, mediante o compartilhamento das avaliações preliminar e de impacto algorítmico.
Governança dos Sistemas de IA	Os agentes de IA, para qualquer sistema, independentemente do risco, deverão implementar ao longo de todo o seu ciclo de vida, desde a concepção inicial até o encerramento de suas atividades e descontinuação, ao menos: (i) Medidas de Transparência, gestão de dados adequados, legitimação do tratamento de dados, segurança da informação e supervisão humana capaz de compreender, interpretar e corrigir os resultados e decisões do sistema.
Classificação de Riscos	IA de risco excessivo são proibidas, como: (i) quando empregarem técnicas subliminares que tenham por objetivo ou por efeito induzir a pessoa natural a se comportar de forma prejudicial ou perigosa à sua saúde ou segurança ou contra os fundamentos da lei; (ii) quando explorarem quaisquer vulnerabilidades de grupos específicos de pessoas naturais e ; (iii) pelo poder público, para avaliar, classificar ou ranquear as pessoas naturais, com base no seu comportamento social ou em atributos da sua personalidade, por meio de pontuação universal, para o acesso a bens e serviços e políticas públicas, de forma ilegítima ou desproporcional.
Responsabilização	Os agentes de IA que causem dano patrimonial, moral, individual ou coletivo são obrigados a repará-lo integralmente, independentemente do grau de autonomia do sistema. Para IA de alto risco ou risco excessivo, **o fornecedor ou operador respondem objetivamente pelos danos causados**, na medida de sua participação no dano. Quando não se tratar de sistema de Inteligência Artificial de **alto risco**, a culpa do agente causador do dano será presumida, **aplicando-se a inversão do ônus da prova em favor da vítima**.

Bibliografia Básica

- BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed., rev., atual. e ampl. Rio de Janeiro: Forense, 2021. xxxii, 311 p.
- COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais: comentada**. 3. ed. rev. atual. e ampl. São Paulo: Revista dos Tribunais, 2020. 263 p.
- DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei geral de proteção de dados** 3. ed. São Paulo: Revista dos Tribunais, 2021. 368 p.
- DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados (Lei nº 13.709/2018): a caminho da efetividade: contribuições para a implementação da LGPD**. São Paulo: Revista dos Tribunais, 2020. 400 p.
- MALDONADO, Viviane Nóbrega; LIMA, Adriano Carlos de et al. (coord.). **Lei Geral de Proteção de Dados Pessoais: manual de implementação**. São Paulo: Revista dos Tribunais, 2020. 368 p.
- MENDES, Laura; BIONDI, Bruno Ricardo (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. xxii, 741 p. OLIVEIRA, Ricardo; COTS, Márcio (coord.). **O legítimo interesse e a LGPDP: Lei Geral de Proteção de Dados Pessoais**. São Paulo: Revista dos Tribunais, 2020. 312 p
- PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD**). 2. ed. São Paulo: Saraiva jur, 2020. 150 p.
- TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais: e suas repercussões no Direito brasileiro**. 2. ed. São Paulo: Revista dos Tribunais, 2020. 1072 p.

Sites Recomendados

- https://www.gov.br/anpd/pt-br
- https://ec.europa.eu/newsroom/article29/items/itemType/1358
- https://edpb.europa.eu/edpb_en
- https://www.ftc.gov/business-guidance/privacy-security/privacy-shield
- https://www.cnil.fr/en/data-protection-around-the-world
- https://ico.org.uk/
- https://iapp.org/

OBRIGADO

FIAP


FIAP