CURSO RDP

Rumo à Magis
@cursorumoamagis

Grupo RDP

INTENSIVO

ENAM 2025.1

EXAME NACIONAL DA MAGISTRATURA

Formação Humanística

Direito Digital

SUMÁRIO

DIREITO DIGITAL

Direito Digital. 4ª Revolução industrial. Tecnologia no contexto jurídico. Automação do processo. Inteligência Artificial e Direito. Audiências virtuais. Cortes remotas. Ciência de dados e Jurimetria. Resoluções do CNJ sobre inovações tecnológicas no Judiciário. Persecução Penal e novas tecnologias. Crimes virtuais e cibersegurança. Deepweb e Darkweb. Provas digitais. Criptomoedas e Lavagem de dinheiro. Noções gerais de contratos Inteligentes, Blockchain e Algoritmos. LGPD e proteção de dados pessoais.

Neste material, vamos trabalhar um tema muito importante para o ENAM, tendo em vista se tratar de uma das grandes preocupações enfrentadas pelo Poder Judiciário na atualidade. Sendo assim, durante a sua leitura, busque assimilar de que forma o direito digital influenciará não apenas os seus acertos nas provas, mas também a sua atuação futura enquanto Juiz ou Juíza. Vamos lá?

1. TEORIA DO DIREITO DIGITAL

1.1 Quarta Revolução Industrial

A 4ª Revolução Industrial representa uma nova era de transformação tecnológica, marcada pela integração de avanços em diversas áreas, como inteligência artificial (IA), robótica, Internet das Coisas (IoT), e computação quântica. Diferente das revoluções industriais anteriores, que ocorreram em ritmo linear, essa nova fase se destaca por sua evolução exponencial, combinando múltiplas tecnologias que estão mudando profundamente a economia, os negócios e a sociedade.

De acordo com Klaus Schwab[1], Presidente do Fórum Econômico Mundial, três principais elementos comprovam que a quarta revolução industrial já é uma realidade:

a) **Velocidade**: "ao contrário das revoluções industriais anteriores, esta evolui em um ritmo exponencial e não linear".
b) **Amplitude** e **profundidade**: ao utilizar-se da revolução digital como base, leva a uma mudança de paradigmas sem precedentes.
c) **Impacto sistêmico**: envolve a transformação de sistemas inteiros entre países e dentro deles.

Um dos principais aspectos dessa 4ª revolução é a interconexão das etapas produtivas. Isso significa que máquinas, sistemas e até mesmo seres humanos estão cada vez mais conectados, comunicando-se de forma global e flexível. Na indústria, esse conceito se traduz na Indústria 4.0, onde fábricas inteligentes utilizam sistemas ciber-físicos para criar produtos personalizados, otimizando recursos e aumentando a eficiência da produção.

Você sabe o que é a chamada Internet das Coisas? A Internet das Coisas (IoT, do inglês *Internet of Things*) é um conceito que se refere à conexão de objetos físicos à internet, permitindo que eles se comuniquem entre si e com outros dispositivos, coletando e trocando dados automaticamente. Esses objetos podem incluir uma

[1] NASCIMENTO, Filippe Augusto dos Santos. **Manual de Humanística** – Introdução às Ciências Humanas e a Teoria do Direito para Carreiras Jurídicas / Filippe Augusto dos Santos Nascimento – 3.ed., rev., atual. e ampl. – São Paulo: Editora Juspodivm, 2024. 976 p.

vasta gama de dispositivos, como eletrodomésticos, carros, sensores, máquinas industriais, sistemas de iluminação e muito mais.

Suas principais características são:

Conectividade: Os dispositivos são conectados à internet, o que lhes permite enviar e receber informações. Isso transforma objetos "comuns" em dispositivos inteligentes, capazes de interagir e responder ao ambiente ao seu redor.

Sensores: Muitos dispositivos IoT são equipados com sensores que monitoram o ambiente, como temperatura, movimento, luz, umidade, entre outros. Esses sensores capturam dados em tempo real, que são então processados e utilizados para diferentes finalidades.

Automação e Controle Remoto: A IoT permite que dispositivos sejam controlados remotamente via internet, seja por meio de aplicativos em smartphones, computadores ou outros dispositivos conectados. Por exemplo, você pode acender as luzes da sua casa ou ajustar a temperatura do termostato usando um aplicativo no seu celular, mesmo estando a quilômetros de distância.

Interoperabilidade: Dispositivos IoT de diferentes fabricantes podem se comunicar e trabalhar juntos em um sistema integrado. Por exemplo, um sistema de segurança doméstica pode combinar câmeras de diferentes marcas, sensores de movimento e fechaduras inteligentes para criar um ambiente de segurança coeso.

Análise de Dados: Os dados coletados pelos dispositivos IoT podem ser analisados para identificar padrões, prever comportamentos ou otimizar operações. Por exemplo, uma fábrica pode usar dados de sensores em suas máquinas para prever falhas antes que elas ocorram, evitando paradas inesperadas na produção.[2]

A amplitude dessa revolução vai além das máquinas conectadas. Ela engloba descobertas simultâneas em áreas como nanotecnologia, biotecnologia, e energias renováveis, que estão transformando os domínios físicos, digitais e biológicos. Tecnologias como a IA não apenas realizam tarefas complexas de forma autônoma, mas também começam a entender, prever e até influenciar os desejos e comportamentos humanos.

Essa fusão de tecnologias cria oportunidades, mas também traz desafios, como a necessidade de adaptação a um mundo e, especificamente, do Poder Judiciário, para analisar essas interações onde as fronteiras entre os seres humanos e as máquinas se tornam cada vez mais tênues.

Veja abaixo os **três processos históricos que precederam a 4ª Revolução Industrial:**

1ª Revolução Industrial

A Primeira Revolução Industrial marcou a transição de uma economia baseada em produção manual para uma economia de produção mecanizada. Esse período foi caracterizado pelo surgimento de máquinas movidas a vapor, que permitiram a produção em grande escala de bens manufaturados. A introdução de fábricas transformou a indústria têxtil e outras áreas, aumentando a eficiência e a produtividade, e alterou drasticamente a estrutura econômica e social das sociedades.

[2] NASCIMENTO, Filippe Augusto dos Santos. **Manual de Humanística** – Introdução às Ciências Humanas e a Teoria do Direito para Carreiras Jurídicas / Filippe Augusto dos Santos Nascimento – 3.ed., rev., atual. e ampl. – São Paulo: Editora Juspodivm, 2024. 976 p.

2ª Revolução Industrial

A Segunda Revolução Industrial trouxe avanços significativos com o desenvolvimento da eletricidade, que se tornou a principal fonte de energia, substituindo o vapor. Esse período viu também melhorias substanciais nos meios de transporte e comunicação, com a invenção do automóvel e do avião, que revolucionaram a mobilidade, e do telefone, que transformou a comunicação. Esses avanços promoveram a globalização e a integração econômica, acelerando o ritmo das inovações tecnológicas e industriais.

3ª Revolução Industrial

A Terceira Revolução Industrial, conhecida também como Revolução Digital, foi impulsionada pelo advento da tecnologia digital e pela criação da internet, que revolucionou a forma como as informações são processadas e compartilhadas globalmente. A introdução de computadores pessoais e de telefones celulares facilitou o acesso à informação e a comunicação instantânea. Além disso, surgiram novas fontes de energia, como a nuclear, a solar e a eólica, diversificando as opções energéticas e promovendo o desenvolvimento sustentável.

Essas três revoluções industriais estabeleceram as bases tecnológicas, econômicas e sociais que culminaram na 4ª Revolução Industrial, caracterizada pela fusão de tecnologias físicas, digitais e biológicas.

1.2 Tecnologia no contexto jurídico

A transformação digital no Poder Judiciário, impulsionada pela 4ª Revolução Industrial, é um fenômeno que reflete a incorporação de tecnologias avançadas na prestação de serviços jurídicos, visando aumentar a eficiência, acessibilidade e transparência do sistema judicial. Este processo, denominado de "Direito 4.0", abrange tanto a regulação dos conflitos e a proteção dos indivíduos diante dos novos riscos tecnológicos, quanto a aplicação de digitalização e outras tecnologias no processamento de demandas judiciais.

O **"Direito 4.0"** surge como uma evolução na ciência jurídica, afetando profundamente o modo como as atividades judiciais são conduzidas. Essa evolução é marcada pela digitalização dos processos e pela introdução de tecnologias como a *Computational Law* (Direito Computacional) e a *Legal Technology* (Tecnologia Jurídica), que permitem automatizar tarefas, aprimorar a tomada de decisões e facilitar o acesso à justiça.

Segundo Wolfgang Hoffmann-Riem[3], a tecnologia traz diversas vantagens para o contexto jurídico, incluindo:

1. Apoio às atividades jurídicas tradicionais.
2. Substituição parcial ou total de regras legais.
3. Aprimoramento dos meios de execução processual.
4. Facilitação de pesquisas jurídicas e avaliação de precedentes.

[3] NASCIMENTO, Filippe Augusto dos Santos. **Manual de Humanística** – Introdução às Ciências Humanas e a Teoria do Direito para Carreiras Jurídicas / Filippe Augusto dos Santos Nascimento – 3.ed., rev., atual. e ampl. – São Paulo: Editora Juspodivm, 2024. 976 p.

5. Automatização de processos.
6. Redução de custos processuais.
7. Aumento da velocidade e eficiência dos processos.
8. Melhoria na preparação e execução de decisões.
9. Facilitação do acesso à justiça.

No Brasil, o Conselho Nacional de Justiça (CNJ) tem implementado várias iniciativas para modernizar o sistema judiciário, destacando-se:[4]

- Juízo 100% Digital: permite que todas as etapas processuais sejam realizadas de forma eletrônica e remota, sem a necessidade de comparecimento físico aos fóruns.
- Balcão Virtual: facilita o contato direto entre os cidadãos e o Judiciário por meio de videoconferência e outras ferramentas digitais.
- Plataforma Digital do Poder Judiciário (PDPJ): promove a cooperação entre tribunais e a modernização do Processo Judicial Eletrônico, integrando sistemas e promovendo o uso de tecnologias em nuvem.
- Aprimoramento dos Registros Processuais Primários: foca na padronização e no treinamento dos tribunais para melhorar a eficiência na gestão dos processos.
- Plataforma Codex: desenvolvida pelo Tribunal de Justiça de Rondônia em parceria com o CNJ, que consolida dados processuais, facilita pesquisas inteligentes, automatiza a alimentação de dados estatísticos e apoia a criação de modelos de Inteligência Artificial (IA).
- Plataforma Sinapses: trata-se de um sistema nacional que armazena, treina e audita modelos de IA, estabelecendo parâmetros para sua implementação.
- Cartório do Futuro: elimina o conceito tradicional de cartório, permitindo uma centralização de serviços que agiliza o atendimento e reduz o número de processos por unidade.

As formas de automação incluem a extração de indicadores das decisões judiciais, agrupamento automático de processos semelhantes, interpretação automatizada de petições, uso de robôs e IA no processamento de dados, preenchimento automatizado de atos processuais, automatização da Penhora Online, identificação de precedentes e direcionamento indicativo de decisões judiciais para casos específicos. Essas inovações visam aumentar a eficiência, reduzir o tempo de trâmite processual e garantir uma justiça mais acessível e eficaz.

VICTOR: a inteligência artificial do STF[5]

O sistema VICTOR é uma ferramenta de inteligência artificial (IA) desenvolvida pelo Supremo Tribunal Federal (STF) do Brasil, com o objetivo de auxiliar na triagem e análise de processos judiciais, especialmente no reconhecimento de temas de repercussão geral. Esse sistema foi criado para lidar com o enorme volume de processos que chegam ao STF, ajudando a otimizar o tempo dos ministros e a tornar o processo de análise mais eficiente.
As principais contribuições do sistema para a rotina do Tribunal incluem:

[4] *Ibidem.*
[5] https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=380038. Acesso em: 26 de agosto de 2024

Automação da Triagem de Recursos: O VICTOR é capaz de identificar, de forma automática, se um recurso extraordinário trata de temas de repercussão geral já reconhecidos pelo STF. Isso é feito por meio do reconhecimento de padrões textuais e da análise do conteúdo dos processos, facilitando a separação daqueles que necessitam de maior atenção por parte dos ministros.

Redução de Tempo: Com o uso do VICTOR, o tempo gasto na triagem de processos é significativamente reduzido. O sistema pode analisar milhares de processos em um período de tempo muito curto, permitindo que os ministros e suas equipes se concentrem em questões mais complexas e de maior relevância.

Precisão: O VICTOR foi treinado com base em milhares de decisões já proferidas pelo STF, o que lhe confere uma capacidade elevada de precisão na identificação dos temas de repercussão geral. Isso ajuda a evitar erros na triagem e a manter a consistência no tratamento dos processos.

Auxílio à Tomada de Decisão: Embora o VICTOR não substitua a análise humana, ele serve como uma ferramenta de apoio à decisão, oferecendo sugestões e análises que podem ser utilizadas pelos ministros para acelerar o julgamento dos casos.

Impacto na Eficiência Judiciária: A implementação do VICTOR é parte dos esforços do STF em modernizar o Judiciário brasileiro, utilizando tecnologias avançadas para lidar com a sobrecarga de processos e melhorar a eficiência na prestação jurisdicional.

Essas medidas visam criar um ambiente de justiça mais acessível, eficiente e transparente, adaptado às demandas de uma sociedade cada vez mais digitalizada. A transformação digital no Poder Judiciário é, portanto, um passo crucial para o fortalecimento do Estado de Direito na era da informação.

1.3 Inteligência artificial

No campo jurídico, a IA está sendo utilizada em várias frentes. Uma das mais notáveis é a automação de tarefas repetitivas e burocráticas, como a triagem de processos e a análise de documentos. Ferramentas de IA são capazes de processar grandes volumes de dados em frações de segundo, facilitando a identificação de padrões, a extração de informações relevantes e a classificação de documentos jurídicos. Esse tipo de automação permite que profissionais do Direito foquem em atividades mais complexas e estratégicas.

Outra funcionalidade da IA que tem se mostrado promissora é na ***Resolução Online de Disputas*** (ODR, na sigla em inglês). Plataformas de ODR utilizam IA para facilitar a mediação e a arbitragem entre partes conflitantes, proporcionando soluções rápidas e eficientes sem a necessidade de intervenção humana. Esse tipo de tecnologia é especialmente útil em disputas de menor valor ou em questões que podem ser resolvidas por meio de regras claramente estabelecidas.

No entanto, apesar das vantagens, o uso da IA no Direito levanta uma série de questões éticas e jurídicas. Um dos principais desafios é garantir a transparência e a explicabilidade dos algoritmos utilizados. Decisões automatizadas ou sugeridas por IA precisam ser compreensíveis para as partes envolvidas, a fim de

garantir a justiça e a imparcialidade do processo. Além disso, há preocupações sobre a privacidade dos dados e a possibilidade de vieses embutidos nos algoritmos, que poderiam resultar em discriminação ou injustiças.[6]

Para melhor compreendermos esses vieses, faz-se necessária uma rápida explicação acerca do funcionamento desses algoritmos. Romulo Valentini ensina que os algoritmos fazem a inteligência artificial funcionar da seguinte maneira:

Nessa equação, o algoritmo é elemento neutro, desprovido de juízos de valor. As falhas algorítmicas das quais decorrem esses vieses decorrem, portanto, da má programação humana, ocorridas na fase do *imput*. Uma das falhas mais conhecidas e comentadas no meio jurídico tem sido o racismo algorítmico, que merece um ponto específico, dada a sua importância.

1.3.1 Racismo algorítmico

Racismo algorítmico é o termo utilizado para descrever a discriminação ou os vieses raciais que podem surgir a partir do uso de algoritmos em sistemas tecnológicos, especialmente naqueles que utilizam inteligência artificial (IA) e aprendizado de máquina (*machine learning*). Esses algoritmos, que são criados para tomar decisões ou fazer previsões com base em grandes volumes de dados, podem acabar reproduzindo e amplificando preconceitos existentes na sociedade, levando a resultados injustos e discriminatórios.

O racismo algorítmico pode surgir de diversas maneiras:

a) **Dados de Treinamento com Viés**: Os algoritmos de IA são treinados com grandes conjuntos de dados. Se esses dados contêm vieses raciais — por exemplo, se refletem práticas discriminatórias passadas ou se são desproporcionalmente representativos de uma raça em particular — o algoritmo pode aprender e perpetuar esses vieses.

b) **Desigualdade na Coleta de Dados**: Quando os dados usados para treinar ou alimentar um algoritmo são coletados de forma desigual ou de fontes que não representam toda a diversidade da sociedade, o sistema pode falhar em tratar igualmente todos os grupos. Por exemplo, se um algoritmo de

[6] NASCIMENTO, Filippe Augusto dos Santos. **Manual de Humanística** – Introdução às Ciências Humanas e a Teoria do Direito para Carreiras Jurídicas / Filippe Augusto dos Santos Nascimento – 3.ed., rev., atual. e ampl. – São Paulo: Editora Juspodivm, 2024. 976 p.

reconhecimento facial é treinado principalmente com imagens de pessoas brancas, ele pode ter dificuldades em identificar pessoas de outras etnias, levando a erros ou tratamentos desiguais.

c) Design e Implementação dos Algoritmos: Os próprios desenvolvedores de algoritmos podem, inconscientemente, incorporar vieses em suas decisões sobre como um algoritmo deve operar. Isso pode ocorrer nas escolhas de quais dados utilizar, nos critérios de decisão programados ou na forma como os resultados são interpretados.

Dentre alguns exemplos de como essa falha pode influenciar processos sistematizados, estão:

- Reconhecimento Facial: Estudos têm mostrado que muitos sistemas de reconhecimento facial apresentam taxas de erro significativamente mais altas ao tentar identificar pessoas de etnias não brancas. Isso ocorre porque esses sistemas foram, em grande parte, treinados em imagens de pessoas brancas, resultando em um viés que leva a falhas quando usados com pessoas de outras etnias.

- Justiça Criminal: Nos Estados Unidos, sistemas de IA têm sido usados para prever a probabilidade de reincidência de criminosos, ajudando a determinar sentenças ou decisões de liberdade condicional. No entanto, esses sistemas foram criticados por apresentar vieses raciais, tratando de forma mais severa réus negros em comparação com réus brancos com histórico semelhante.

- Empréstimos e Finanças: Algoritmos utilizados para avaliar a concessão de crédito ou empréstimos também podem discriminar grupos raciais específicos, se os dados históricos usados para os treinar contêm preconceitos, como negar crédito a indivíduos de minorias raciais.

As consequências do racismo algorítmico são graves, pois podem perpetuar desigualdades sociais e econômicas existentes, reforçar estereótipos e contribuir para a marginalização de certos grupos raciais. Além disso, a percepção de imparcialidade dos sistemas tecnológicos pode levar a uma aceitação generalizada de decisões injustas, dificultando a luta contra o racismo estrutural.

Notícia veiculada no ano de 2022 mostra como a inserção de dados pode ser falha e perpetuar análises preconceituosas. A foto de Michael B. Jordan foi utilizada dentre imagens presentes em um ***Termo de Reconhecimento Fotográfico da Polícia Civil do Ceará****. A apresentação das fotos resultou na apreensão de um adolescente de 17 anos como suspeito de envolvimento em uma chacina.*

Fonte: https://g1.globo.com/ce/ceara/noticia/2022/01/07/astro-do-cinema-michael-b-jordan-aparece-em-lista-de-procurados-pela-policia-do-ceara.ghtml

Para mitigar o racismo algorítmico, é essencial que os desenvolvedores de tecnologia adotem práticas responsáveis, como:

- **Diversidade nos Dados**: Garantir que os dados usados para treinar algoritmos sejam representativos de toda a população, evitando a perpetuação de vieses.
- **Auditoria e Transparência**: Realizar auditorias regulares nos sistemas de IA para identificar e corrigir possíveis vieses, além de tornar esses processos transparentes para o público.
- **Inclusão de Diversidade nas Equipes**: Assegurar que as equipes responsáveis pelo desenvolvimento e implementação de algoritmos sejam diversas, refletindo uma ampla gama de perspectivas.
- **Regulamentação e Políticas**: Implementar políticas e regulamentações que exijam o desenvolvimento ético de IA, prevenindo a discriminação e promovendo a justiça social.

Em síntese, o racismo algorítmico é um fenômeno que precisa ser reconhecido e enfrentado ativamente para garantir que a tecnologia seja usada de forma justa e equitativa, promovendo igualdade e inclusão em vez de reforçar desigualdades históricas.

1.4 Automação do processo

A ascensão da Inteligência Artificial (IA) e a aplicação crescente de algoritmos em processos decisórios têm levantado questões éticas e jurídicas fundamentais. Esses sistemas, muitas vezes, operam com pouca transparência, o que pode levar a decisões que são percebidas como insensíveis ou até discriminatórias. A literatura sobre o tema destaca a necessidade de uma abordagem cautelosa, que considere não apenas a eficiência dos algoritmos, mas também as implicações humanas e sociais dessas tecnologias.

Uma preocupação central é a responsabilidade pelas decisões tomadas por sistemas automatizados. A delegação de decisões críticas a algoritmos levanta a questão de quem é responsável pelos erros ou

injustiças resultantes. Além disso, há a questão da transparência e explicabilidade desses sistemas: como os resultados são gerados e quais dados foram utilizados no processo decisório?[7]

O respeito aos direitos fundamentais é outro ponto crítico. Decisões automatizadas não podem violar garantias básicas, como o direito à privacidade e à não discriminação. Além disso, é essencial assegurar que as decisões possam ser revisadas por humanos, permitindo a reversibilidade em casos de erros ou injustiças.

A transparência é particularmente importante no contexto jurídico, onde as decisões automatizadas podem ter implicações profundas na vida das pessoas. Isso exige que os algoritmos sejam auditáveis e que seus critérios de decisão sejam claros e compreensíveis. A falta de transparência pode levar a uma perda de confiança no sistema jurídico como um todo.

Nesse sentido, Juarez Freitas e Thomas Bellini Freitas[8] pontuam algumas diretrizes éticas (*guidelines*) que devem ser somadas à utilização de decisões automatizadas, sendo elas:

a) Indelegabilidade da decisão intrinsecamente humana.
b) Respeito aos direitos e às garantias fundamentais.
c) Respeito à sustentabilidade e ao bem-estar multidimensional, ecossistêmico e intergeracional.
d) Avaliação permanente de seus impactos.
e) Transparência e explicabilidade.
f) Supervisão humana e reversibilidade.

Finalmente, o tratamento de dados pessoais é uma preocupação constante. A Lei Geral de Proteção de Dados (LGPD) no Brasil, por exemplo, estabelece diretrizes rigorosas sobre como os dados pessoais devem ser manejados, particularmente em processos automatizados. A lei assegura que os indivíduos tenham o direito de saber como seus dados estão sendo utilizados e de contestar decisões automatizadas que afetam sua personalidade.

OBS.: Sobre o tema, reputamos válida a leitura da **Resolução n. 332/2020 do CNJ** que dispõe sobre o uso da Inteligência Artificial pelo Poder Judiciário.

Essas questões mostram que, embora a IA ofereça benefícios significativos, sua implementação em processos decisórios deve ser acompanhada de uma reflexão ética e jurídica profunda, garantindo que as inovações tecnológicas respeitem os direitos humanos e mantenham a confiança pública.

ALGORITMOS DESENVIESANTES: Segundo Filippe Augusto dos Santos, algoritmos desenviesantes são sistemas de Inteligência Artificial projetados para mitigar vieses e ruídos nas decisões humanas, em vez de simplesmente substituir a atuação humana. Eles podem aprimorar a tomada de decisão, por exemplo, ao identificar

[7] NASCIMENTO, Filippe Augusto dos Santos. **Manual de Humanística** – Introdução às Ciências Humanas e a Teoria do Direito para Carreiras Jurídicas / Filippe Augusto dos Santos Nascimento – 3.ed., rev., atual. e ampl. – São Paulo: Editora Juspodivm, 2024. 976 p.
[8] *Ibidem.*

sentenças que divergem do entendimento de um tribunal (*distinguishing*) ou ao alertar um julgador sobre possíveis desvios de seus próprios precedentes (*overruling*), ajudando-o a reconsiderar a decisão e a evitar influências indevidas. Esses algoritmos atuam como ferramentas para promover decisões mais justas e coerentes, combatendo os vieses que poderiam distorcer o julgamento.[9]

1.5 Justiça 4.0

De acordo com o site do Conselho Nacional de Justiça (CNJ), a Justiça 4.0, representa um marco na modernização do sistema judiciário brasileiro, com o objetivo de tornar a Justiça mais acessível, ágil e eficiente por meio da incorporação de novas tecnologias e inovações processuais. Esse projeto estratégico envolve um conjunto abrangente de programas e iniciativas que transformam a forma como os serviços judiciais são prestados e geridos em todo o país.[10]

Aa Lei nº 14.195/2021 modificou o art. 246, a fim de estabelecer que a citação será feita **preferencialmente** por **meio eletrônico**, no prazo de até 2 (dois) dias úteis, contado da decisão que a determinar, por meio dos endereços eletrônicos indicados pelo citando no banco de dados do Poder Judiciário.

Qual **forma de citação deverá ser preferencialmente realizada?**	
Antes da Lei nº 14.195/2021: Citação pelo **CORREIO**	Depois da Lei nº 14.195/2021: Citação por **MEIO ELETRÔNICO**
Art. 246. A citação será feita: (...)	Art. 246. A citação será feita **preferencialmente por meio eletrônico** (...)
Art. 247. A citação será feita pelo correio para qualquer comarca do país, exceto: (...)	Art. 247. A citação será feita por meio eletrônico ou pelo correio para qualquer comarca do País, exceto: (...)

Contudo, a Lei nº 14.195/2021 traz as hipóteses em que não será feita a citação por meio eletrônico ou pelos correios:

> Art. 247. A citação será feita por meio eletrônico ou pelo correio para qualquer comarca do País, exceto: (Redação dada pela Lei nº 14.195, de 2021)
> I - nas **ações de estado**, observado o disposto no art. 695, § 3º ;
> II - quando o **citando for incapaz**;
> III - quando o **citando for pessoa de direito público**;
> IV - quando o citando **residir em local não atendido pela entrega domiciliar de correspondência;**
> V - quando o autor, justificadamente, a **requerer de outra forma**.

[9] NASCIMENTO, Filippe Augusto dos Santos. **Manual de Humanística** – Introdução às Ciências Humanas e a Teoria do Direito para Carreiras Jurídicas / Filippe Augusto dos Santos Nascimento – 3.ed., rev., atual. e ampl. – São Paulo: Editora Juspodivm, 2024. 976 p.
[10] https://www.cnj.jus.br/tecnologia-da-informacao-e-comunicacao/justica-4-0/. Acesso em 26 de agosto de 2024

O § 1º do art. 246 do NCPC, com a nova redação dada pela Lei nº 14.195/2021, deixa claro que as empresas **públicas** e **privadas** são obrigadas a manter cadastro nos sistemas de processo em autos eletrônicos, para efeito de recebimento de citações e intimações, as quais serão efetuadas preferencialmente por esse meio.

Porém, as **microempresas** e **as pequenas empresas** somente se sujeitam a essa regra quando **não** possuírem endereço eletrônico cadastrado no sistema integrado da Rede Nacional para a Simplificação do Registro e da Legalização de Empresas e Negócios (Redesim). Neste caso, deverá haver compartilhamento de cadastro com o órgão do Poder Judiciário, incluído o endereço eletrônico constante do sistema integrado da Redesim, nos termos da legislação aplicável ao sigilo fiscal e ao tratamento de dados pessoais. Inclusive porque seria inimaginável que uma empresa de âmbito nacional tivesse que fazer cadastro em todos os tribunais do país. [11]

Sobre a citação, não podemos esquecer de que na ação de usucapião de imóvel, os **confinantes serão citados pessoalmente**, **exceto quando tiver por objeto unidade autônoma de prédio em condomínio,** caso em que tal citação é dispensada.

A citação será feita pelo correio para qualquer comarca do país, **exceto** (esse rol despenca):

> I - nas ações de estado, observado o disposto no art. 695, § 3º ;
> II - quando o citando for incapaz;
> III - quando o citando for pessoa de direito público;
> IV - quando o citando residir em local não atendido pela entrega domiciliar de correspondência;
> V - quando o autor, justificadamente, a requerer de outra forma.

ANOTA QUE VAI CAIR: Nos condomínios edilícios ou nos loteamentos com controle de acesso, será válida a entrega do mandado a funcionário da portaria responsável pelo recebimento de correspondência, que, entretanto, poderá recusar o recebimento, se declarar, por escrito, sob as penas da lei, que o destinatário da correspondência está ausente.

Ainda sobre o art. 246 do Código de Processo Civil, é muito importante citarmos a respeito do domicílio judicial eletrônico, desenvolvido pelo Programa Justiça 4.0 e fruto de parceria entre o CNJ e o Programa das Nações Unidas para o Desenvolvimento (Pnud).

Segundo o CNJ, o Domicílio Eletrônico é solução 100% digital e gratuita que facilita e agiliza as consultas para quem recebe e acompanha citações, intimações e demais comunicações enviadas pelos tribunais. Em 2022, a Resolução 455 do CNJ determinou que as comunicações processuais fossem realizadas exclusivamente pelo Domicílio, regulamentando o previsto no art. 246 da Lei 13.105/2015 (Código de Processo Civil). Segundo o normativo, o cadastro passou a ser obrigatório para União, estados, Distrito Federal, municípios, entidades

[11] Recomendo a aula do professor Edilson Vitorelli sobre a referida Lei nº 14.195/2021: https://www.youtube.com/watch?v=E855XzXma10.

da administração indireta e empresas públicas e privadas. Além de garantir maior rapidez aos processos judiciais, a digitalização e a centralização das informações permitem economia de recursos humanos e financeiros utilizados na prestação de serviços pelo Poder Judiciário. Com a implementação do sistema, os tribunais podem reduzir em 90% os custos de envio das comunicações antes expedidas pelos Correios ou por meio de visita de oficiais de Justiça.[12]

A **Resolução nº 455 de 27/04/2022**, no entanto, foi alterada pela **Resolução n. 569, de 13/8/2024,** trazendo algumas alterações importantes, como as apontadas abaixo: [13]

Resolução n. 455/2022	Nova resolução (2024)
A pessoa física ou jurídica citada tem prazo de três dias úteis para dar ciência da citação.	Para pessoas jurídicas de direito público, o sistema considerará o prazo de 10 dias corridos para ciência das citações.
Se não é registrada ciência na citação, a comunicação expira e a parte é citada por outro meio.	Para pessoas jurídicas de direito público, se não se registrar ciência na citação dentro do prazo de 10 dias corridos, o sistema considerará ciência tácita. Para pessoas jurídicas de direito privado, se não se registrar ciência na citação dentro do prazo de três dias úteis, a comunicação expirará e a parte será citada por outro meio.
Tribunais devem enviar todas as comunicações processuais.	Tribunais devem enviar para o Domicílio somente comunicações processuais de vista pessoal, ou seja, quando a parte é responsável por registrar a ciência.
O prazo processual abrirá no momento em que o destinatário da comunicação processual obtiver acesso ao conteúdo da comunicação.	Para citações, o prazo para resposta começa a correr no quinto dia útil seguinte à confirmação. Para intimações, o prazo para resposta começa a correr no momento em que o destinatário da comunicação processual obtém acesso ao conteúdo da comunicação.

1.5.1 Portfólio de Projetos

O Portfólio de Projetos do CNJ reúne diversas iniciativas sob a égide da Justiça 4.0, promovendo uma visão integrada e estratégica de desenvolvimento e implementação das novas tecnologias. Este portfólio funciona como um guia para as ações coordenadas, garantindo que todos os projetos sejam executados de maneira eficiente e alinhada aos objetivos gerais de modernização da Justiça.

[12] Disponível em: https://www.cnj.jus.br/nova-resolucao-do-cnj-altera-prazos-e-regras-do-domicilio-judicial-eletronico/
[13] Disponível em: https://www.cnj.jus.br/nova-resolucao-do-cnj-altera-prazos-e-regras-do-domicilio-judicial-eletronico/

1.5.2 Plataforma Digital do Poder Judiciário

A Plataforma Digital do Poder Judiciário é uma ferramenta unificadora, que centraliza o acesso a diversos sistemas e serviços judiciais, oferecendo uma interface integrada e simplificada para magistrados, servidores, advogados e cidadãos. Esta plataforma é essencial para consolidar a digitalização do Judiciário, facilitando o trabalho colaborativo e o acesso remoto a informações e processos.

1.5.3 Plataforma Sinapses / Inteligência Artificial

A Plataforma Sinapses é um ambiente que permite a criação e utilização de algoritmos de Inteligência Artificial (IA) no Judiciário. Esta plataforma é fundamental para o desenvolvimento de soluções automatizadas que auxiliam na análise de processos, na produção de decisões mais rápidas e na identificação de padrões que podem ser usados para melhorar a eficiência e a justiça nas decisões.

1.5.4 Plataforma Codex

A Plataforma Codex é um repositório centralizado que armazena e organiza grandes volumes de dados processuais, permitindo a análise e o cruzamento de informações de forma mais eficiente. Ela é projetada para facilitar o trabalho dos operadores do Direito, proporcionando acesso rápido e estruturado às informações necessárias para a tomada de decisões informadas.

1.5.5 Balcão Virtual

O Balcão Virtual é uma solução que permite o atendimento remoto em tempo real, replicando o atendimento presencial que ocorre nos fóruns e tribunais, mas de forma online. Com isso, as partes, advogados e outros interessados podem ser atendidos sem a necessidade de deslocamento físico, garantindo mais praticidade e celeridade no atendimento das demandas judiciais.

1.5.6 BNMP 3.0

O Banco Nacional de Monitoramento de Prisões (BNMP) 3.0 é uma evolução do sistema anterior, que permite o acompanhamento em tempo real da situação de pessoas privadas de liberdade em todo o território nacional. Ele é crucial para garantir maior transparência e controle sobre a execução penal, contribuindo para a prevenção de irregularidades e a promoção de uma gestão mais eficiente do sistema penitenciário.

1.5.7 Núcleos de Justiça 4.0

Os Núcleos de Justiça 4.0 são unidades especializadas que operam exclusivamente no ambiente digital, utilizando todas as ferramentas tecnológicas disponíveis para processar e julgar casos de maneira mais

rápida e eficiente. Nesses modalidade, os processos tramitam por meio do Juízo 100% Digital, no qual audiências e outros atos processuais são realizados de forma integralmente virtual.[14]

Aqui, inserem-se as chamadas **Cortes Remotas**, nomenclatura cunhada pelo britânico Richard Susskind. Para ele, há dois sentidos possíveis para a denominação. O primeiro, relaciona-se com a possibilidade de julgamentos virtuais, nos quais juízes humanos decidem, sem, contudo, estar em tribunais físicos. O outro, representa conceito mais amplo, pelo qual o Poder Judiciário se utilizaria da tecnologia para ampliar o Acesso à Justiça.[15]

1.5.8 Juízo 100% Digital

O programa Juízo 100% Digital permite que todas as fases de um processo judicial sejam realizadas de forma totalmente virtual, eliminando a necessidade de qualquer contato físico entre as partes, o juiz e os servidores. Essa iniciativa é especialmente importante em tempos de pandemia, mas também se projeta como uma solução permanente para acelerar os processos e reduzir custos operacionais.

1.5.9 Painel das Resoluções

O Painel das Resoluções é uma ferramenta que disponibiliza de forma transparente e organizada todas as resoluções do CNJ. Ele facilita a consulta e o acompanhamento das normativas que regem o funcionamento do Judiciário, permitindo que magistrados, advogados e o público em geral tenham acesso fácil às informações necessárias para o cumprimento das regras e procedimentos.

1.5.10 Domicílio Judicial Eletrônico

O Domicílio Judicial Eletrônico é uma solução que permite a escolha de um endereço eletrônico oficial para o recebimento de citações, intimações e notificações judiciais. Esta ferramenta promove maior segurança e rapidez na comunicação processual, reduzindo os custos com notificações físicas e evitando atrasos decorrentes de problemas na entrega de documentos.

1.5.11 *Sniper*

O Sniper é uma ferramenta que a partir do cruzamento de dados e informações de diferentes bases de dados, destaca os vínculos entre pessoas físicas e jurídicas de forma visual, permitindo identificar relações de interesse para localização de bens e ativos, otimizando processos de execução e cumprimentos de sentença.

[14] NASCIMENTO, Filippe Augusto dos Santos. **Manual de Humanística** – Introdução às Ciências Humanas e a Teoria do Direito para Carreiras Jurídicas / Filippe Augusto dos Santos Nascimento – 3.ed., rev., atual. e ampl. – São Paulo: Editora Juspodivm, 2024. 976 p.
[15] *Ibidem*.

1.5.12 Sistema Nacional de Gestão de Bens (SNGB)

O Sistema Nacional de Gestão de Bens (SNGB) centraliza a administração de todos os bens apreendidos e confiscados pela Justiça em processos criminais. Este sistema garante que os bens sejam geridos de forma transparente e eficiente, evitando perdas e desvios, e assegurando que os recursos oriundos desses bens sejam revertidos em prol da sociedade.

1.5.13 Prevjud

O Prevjud é uma iniciativa voltada para a prevenção de litígios judiciais. Através de análises preditivas e outras ferramentas tecnológicas, o programa busca identificar potenciais conflitos antes que eles se tornem ações judiciais, propondo soluções alternativas que possam resolver as disputas de forma mais célere e menos onerosa.

A Justiça 4.0, com seus diversos programas e iniciativas, representa um avanço significativo para o sistema judiciário brasileiro, utilizando a tecnologia como uma aliada poderosa na promoção de uma justiça mais célere, acessível e eficiente. A integração dessas plataformas e sistemas não só moderniza o Judiciário, mas também assegura que os direitos fundamentais sejam respeitados em um ambiente cada vez mais digital.

1.6 Jurimetria

Filippe Augusto dos Santos lembra que a Jurimetria é uma disciplina inovadora que utiliza métodos estatísticos para analisar e compreender o funcionamento do Direito e suas interações com a sociedade. Originada nos Estados Unidos através dos estudos de Lee Loevinger, que focava na análise estatística dos precedentes para prever o Direito futuro.[16]

No Brasil, a disciplina é trabalhada por Marcelo Guedes Nunes, segundo o qual a Jurimetria consiste na aplicação de métodos estatísticos para investigar o funcionamento de uma ordem jurídica, combinando os pilares jurídico, estatístico e computacional. A disciplina não busca prever o Direito de forma determinística, mas sim compreender e modelar o comportamento coletivo em resposta às normas jurídicas, aproximando os resultados jurídicos das expectativas sociais.

Por meio da análise de grandes volumes de dados jurídicos, a Jurimetria auxilia juízes, advogados e legisladores a tomar decisões mais informadas, baseadas em modelos estatísticos que refletem a realidade social. Exemplos de sua aplicação incluem estudos sobre os impactos de medidas provisórias no tempo de abertura de empresas, o controle de constitucionalidade pelo STF durante a pandemia de COVID-19, e a reincidência criminal no Brasil.

Além disso, o Conselho Nacional de Justiça (CNJ) utiliza a Jurimetria para desenvolver políticas públicas e avaliar estrategicamente o funcionamento do Judiciário brasileiro. Pesquisas sobre temas como a

[16] NASCIMENTO, Filippe Augusto dos Santos. **Manual de Humanística** – Introdução às Ciências Humanas e a Teoria do Direito para Carreiras Jurídicas / Filippe Augusto dos Santos Nascimento – 3.ed., rev., atual. e ampl. – São Paulo: Editora Juspodivm, 2024. 976 p.

judicialização da saúde, a justiça criminal, a mediação e conciliação no Judiciário, e a tramitação prioritária de processos envolvendo idosos e pessoas com deficiência são exemplos do uso prático da Jurimetria para melhorar a eficiência e a justiça no sistema jurídico.

2. PERSECUÇÃO PENAL E NOVAS TECNOLOGIAS

Todas essas inovações tecnológicas têm transformado profundamente diversas esferas da vida humana, incluindo a prática criminosa, que evoluiu para o ambiente digital, dando origem aos chamados **cibercrimes**.

Nesse contexto, Fillipe Augusto[17] alerta ser essencial entendermos a Cibersegurança, que é a sistemática utilizada para a proteção contra crimes virtuais. A Cibersegurança engloba uma abordagem mais ampla do que aquela utilizada para proteção contra os crimes em geral, voltada para a proteção contra várias ameaças que surgem com o uso da internet e das novas tecnologias, muitas das quais não configuram crimes, mas ainda assim comprometem a segurança digital.

Entre as principais ameaças à Cibersegurança, destacam-se:

1. **Ameaças Políticas (Hacktivismo):** Consistem em ataques realizados por grupos de hackers que, motivados por causas sociais ou políticas, atacam governos, partidos políticos e grandes empresas. Embora esses ataques possam levantar questões sociais relevantes, eles podem envolver práticas criminosas.

2. **Ameaças Terroristas (Ciberterrorismo):** Envolvem ataques cibernéticos realizados por grupos extremistas ou subvencionados por nações hostis, com o objetivo de causar pânico e atacar valores ou infraestruturas de outros Estados. No Brasil, o ciberterrorismo é tipificado pela **Lei nº 13.260/16**, que assim dispõe:

> Art. 2º O terrorismo consiste na prática por um ou mais indivíduos dos atos previstos neste artigo, por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, quando cometidos com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública.
>
> § 1º São atos de terrorismo:
>
> (...)
>
> IV - sabotar o funcionamento ou apoderar-se, com violência, grave ameaça a pessoa ou servindo-se de **mecanismos cibernéticos**, do controle total ou parcial, ainda que de modo temporário, de meio de comunicação ou de transporte, de portos,

[17] *Ibidem.*

aeroportos, estações ferroviárias ou rodoviárias, hospitais, casas de saúde, escolas, estádios esportivos, instalações públicas ou locais onde funcionem serviços públicos essenciais, instalações de geração ou transmissão de energia, instalações militares, instalações de exploração, refino e processamento de petróleo e gás e instituições bancárias e sua rede de atendimento

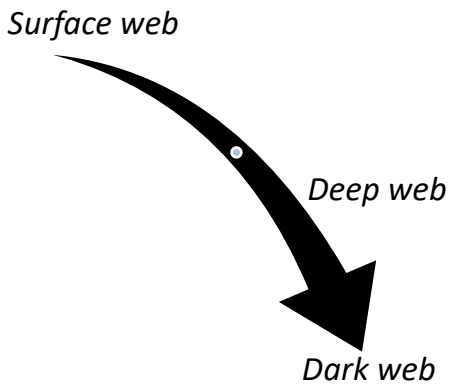
3. **Ameaças por Vingança:** Resultam de sentimentos de rejeição ou ressentimento, como ataques realizados por ex-empregados ou ex-parceiros amorosos, utilizando informações obtidas durante o período de confiança. Um exemplo é o crime de "Revenge Porn", previsto no Art. 218-C do Código Penal, que pune a divulgação não autorizada de conteúdos íntimos.

4. **Ameaças por Razões Financeiras:** Envolvem ataques virtuais com o objetivo de obter vantagem econômica ilícita, como fraudes e extorsões. Esses ataques representam uma ameaça significativa à segurança financeira e à privacidade dos usuários.

5. **Pedofilia na internet** (Art. 241-A do ECA).

6. **Invasão de dispositivo informático** (Art. 154-A do CP).

A doutrina[18] pontua que além do impacto direto dessas ameaças, é importante entender as diferentes camadas da internet, como a *Surface Web*, *Deep Web* e *Dark Web*. A ***Surface Web*** é a *internet* convencional acessada pela maioria das pessoas, enquanto a ***Deep Web*** refere-se a endereços não indexados por sistemas de busca. Dentro da Deep Web, há um segmento conhecido como ***Dark Web***, que é mais voltado para práticas criminosas, exigindo o uso de ferramentas de criptografia e proteção de dados para acesso.



Outro aspecto relevante no contexto de cibercrimes é o uso de **criptomoedas** para a lavagem de dinheiro. Criptomoedas, como o *Bitcoin*, utilizam a tecnologia *Blockchain* para garantir a validade das transações. No entanto, essa tecnologia também é explorada para ocultar valores de origem ilícita, dificultando o rastreamento pelas autoridades. Embora as criptomoedas não sejam completamente anônimas, a complexidade e descentralização do sistema tornam o controle sobre essas transações um desafio para as autoridades.

[18] NASCIMENTO, Filippe Augusto dos Santos. **Manual de Humanística** – Introdução às Ciências Humanas e a Teoria do Direito para Carreiras Jurídicas / Filippe Augusto dos Santos Nascimento – 3.ed., rev., atual. e ampl. – São Paulo: Editora Juspodivm, 2024. 976 p.

O que é *blockchain*?

Blockchain é uma tecnologia de registro distribuído que permite a criação de um banco de dados seguro, transparente e imutável, no qual as informações são armazenadas em blocos encadeados, formando uma cadeia (ou *chain*). Cada bloco contém um conjunto de transações ou dados, um registro do bloco anterior (chamado de hash), e um carimbo de tempo, o que garante a integridade e a ordem das informações.

Suas principais características são:

1. **Distribuído e Descentralizado:** ao contrário dos bancos de dados tradicionais, que são centralizados e controlados por uma única entidade, o blockchain é mantido por uma rede de computadores (nós) que operam de forma descentralizada. Cada nó na rede possui uma cópia completa da cadeia de blocos, e todas as transações são validadas por consenso entre os participantes.

2. **Imutabilidade:** uma vez que os dados são gravados em um bloco e o bloco é adicionado à cadeia, eles não podem ser alterados ou excluídos. Qualquer tentativa de modificar os dados em um bloco exigiria a alteração de todos os blocos subsequentes, o que é praticamente impossível em uma rede bem distribuída. Isso garante a integridade e a segurança dos registros.
3. **Transparência e Auditorabilidade:** todos os participantes da rede têm acesso à mesma versão do registro, o que torna o blockchain extremamente transparente. As transações podem ser auditadas por qualquer participante, embora os detalhes possam ser anonimizados ou criptografados, dependendo da implementação.

4. **Segurança:** a segurança do blockchain é garantida por criptografia avançada. As transações são criptografadas, e o processo de consenso (como a prova de trabalho, utilizada no Bitcoin) ajuda a proteger a rede contra-ataques maliciosos.

5. ***Smart Contracts*:** em algumas plataformas de *blockchain*, como a Ethereum, é possível criar contratos inteligentes (*smart contracts*). Esses são programas autoexecutáveis com regras e condições estabelecidas, que são automaticamente aplicadas quando as condições são atendidas. Isso permite a automação de processos complexos, como pagamentos e transferências de propriedade, sem a necessidade de intermediários.

Blockchain é amplamente conhecido por ser a tecnologia subjacente ao *Bitcoin* e outras criptomoedas, mas suas aplicações vão muito além do setor financeiro. Pode ser usado em uma variedade de indústrias, como cadeias de suprimento, votação eletrônica, registro de propriedades, e outras que demandem um registro confiável e seguro.

No Brasil, apesar de ainda não haver uma legislação específica sobre a lavagem de dinheiro por meio de criptomoedas, a prática pode ser enquadrada na Lei de Lavagem de Dinheiro (Lei nº 9.613/98), uma vez que envolve a ocultação de bens, direitos ou valores de origem ilícita.

2.1 Provas digitais

A revolução tecnológica em curso trouxe novas formas de interação, comunicação e transação, as quais geram uma vasta quantidade de informações digitais, que, por sua vez, passaram a exigir adaptações na condução dos processos judiciais. Nesse contexto, o sistema jurídico precisou se adequar para garantir que os fatos controvertidos ocorridos online possam ser comprovados de maneira eficaz e justa.

Tradicionalmente, as provas documentais em meio físico e as testemunhais têm sido os pilares na comprovação de fatos em processos judiciais. No entanto, diante da crescente complexidade das interações no ambiente digital, esses meios, por si só, já não conseguem abarcar todos os fatos que podem ser objeto de litígios. A introdução de **registros digitais** como prova tornou-se uma necessidade real e presente no Judiciário, refletindo as mudanças nas relações humanas e comerciais.

Os artigos 369 e 370 do Código de Processo Civil (CPC) brasileiro confirmam a abertura para o uso de provas digitais, mesmo que estas não estejam explicitamente previstas no código. Vejamos:

> Art. 369. As partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz.
>
> Art. 370. Caberá ao juiz, de ofício ou a requerimento da parte, determinar as provas necessárias ao julgamento do mérito.
>
> Parágrafo único. O juiz indeferirá, em decisão fundamentada, as diligências inúteis ou meramente protelatórias.

Além disso, o Marco Civil da Internet (Lei n. 12.965/2014), em seus artigos 13 e 15, impõe a obrigatoriedade de guarda dos registros de conexão, evidenciando um claro interesse legislativo em utilizar tais dados para fins probatórios.

> Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.
>
> § 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.
>
> § 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.

§ 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput.

§ 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º.

§ 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

§ 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no caput a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3º e 4º do art. 13.

§ 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Complementando essa abordagem, a Lei Geral de Proteção de Dados (LGPD), em seu artigo 7º, inciso VI, prevê que o tratamento de dados pessoais pode ser realizado para o exercício regular de direitos em processos judiciais, administrativos ou arbitrais. Isso demonstra a preocupação em garantir que os dados, inclusive os de terceiros, possam ser acessados para a defesa de direitos, o que naturalmente possui um grande potencial probatório.[19]

Veja que interessante esse caso, ocorrido em uma persecução penal, explicado pelo Professor Márcio Cavalcante do Dizer o Direito:[20]

> Caso adaptado: a Polícia Civil realizou operação para investigar e prender uma suposta organização criminosa de hackers que teria furtado dinheiro de correntistas de bancos. João foi um dos indivíduos preso e denunciado pelo Ministério Público por furto, organização criminosa e lavagem de dinheiro. A defesa de João impetrou habeas corpus argumentando que a imputação dos crimes está fundamentada em supostas provas digitais em relação às quais houve quebra da cadeia de custódia.
>
> As provas existentes contra João foram extraídas dos computadores apreendidos na sua residência, no entanto, não houve registro documental dos procedimentos adotados pela polícia para a preservação da integridade, autenticidade e confiabilidade dos elementos informáticos. Logo, houve quebra da cadeia de custódia (art. 158-A e seguintes do CPP).
>
> O STJ concordou. Não há como assegurar que os elementos informáticos periciados pela polícia são íntegros e idênticos aos que existiam nos computadores do réu, o que acarreta ofensa ao art. 158 do CPP com a quebra da cadeia de custódia dos computadores apreendidos pela polícia, inadmitindo-se as provas obtidas por falharem num teste de confiabilidade mínima.
>
> STJ. 5ª Turma. RHC 143169/RJ, Rel. Min. Messod Azulay Neto, Rel. Acd. Min. Ribeiro Dantas, julgado em 7/2/2023 (Info 763).

A falta de procedimentos para garantir a idoneidade e integridade dos dados extraídos de um celular apreendido resulta na quebra da cadeia de custódia e na inadmissibilidade da prova digital. STJ. 5ª Turma. AgRg no HC 828.054-RN, Rel. Min. Joel Ilan Paciornik, julgado em 23/4/2024 (Info 811).[21]

---

[19] NASCIMENTO, Filippe Augusto dos Santos. **Manual de Humanística** – Introdução às Ciências Humanas e a Teoria do Direito para Carreiras Jurídicas / Filippe Augusto dos Santos Nascimento – 3.ed., rev., atual. e ampl. – São Paulo: Editora Juspodivm, 2024. 976 p.

[20] CAVALCANTE, Márcio André Lopes. **São inadmissíveis as provas digitais sem registro documental acerca dos procedimentos adotados pela polícia para a preservação da integridade, autenticidade e confiabilidade dos elementos informáticos**. Buscador Dizer o Direito, Manaus. Disponível em: <https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/09859012c567eb2b02d10dddf624e9d3>. Acesso em: 28/08/2024

[21] CAVALCANTE, Márcio André Lopes. **A falta de procedimentos para garantir a idoneidade e integridade dos dados extraídos de um celular apreendido resulta na quebra da cadeia de custódia e na inadmissibilidade da prova digital**. Buscador Dizer o Direito, Manaus. Disponível em: <https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/646e058fac455de8d1e52c4c49baac06>. Acesso em: 28/08/2024

À vista disso, a evolução tecnológica exige que o Judiciário acompanhe as transformações da sociedade, incorporando novos tipos de provas que refletem a realidade digital. A integração de provas digitais no processo judicial não apenas amplia o leque de possibilidades probatórias, mas também fortalece a busca pela verdade e pela justiça em um mundo cada vez mais conectado e digitalizado.

Contratos Inteligentes ou *Smart Contracts*

A tecnologia *blockchain*, vista acima, também possibilitou o desenvolvimento dos contratos inteligentes, ou *smart contracts*. Como vimos, esses são protocolos computacionais digitais que desempenham funções semelhantes aos contratos tradicionais, como definir condições de transferência, garantias e termos de pagamento. Os contratos inteligentes possuem cinco características principais:

1. **Exclusividade Eletrônica:** existem apenas como linguagem de programação, sem versão física.
2. **Elevada Certeza: o**peram sob a lógica do Blockchain, eliminando a margem de discricionariedade.
3. **Natureza Condicional:** são automatizados, garantindo a auto-obrigação das cláusulas contratuais conforme programadas.
4. **Inviolabilidade:** são imutáveis, mantendo registros de todas as transações, inclusive tentativas de adulteração.
5. **Autoexecução:** as obrigações contratuais são automaticamente executadas conforme programadas, dispensando intermediários.

Inicialmente, os contratos inteligentes foram amplamente utilizados no mercado financeiro para a negociação de criptomoedas, mas a tecnologia pode ser aplicada em diversos setores. Sua capacidade de autoexecutoriedade tem o potencial de reduzir significativamente a litigância contratual e a necessidade de intervenção judicial. No entanto, a regulamentação desses contratos ainda é incipiente em muitos países, incluindo o Brasil.

Vejam como o assunto já foi cobrado por bancas tradicionais como **CEBRASPE** e **FGV** em provas para outros cargos jurídicos:

CAIU NA CÂMARA DOS DEPUTADOS – Consultor Legislativo – 2024 – FGV: Considerando os contratos inteligentes em blockchain, assinale a afirmação correta.
A) Contratos inteligentes não são vinculativos quando estabelecidos, mas meramente orientativos; embora apresentem potencial para simplificar e agilizar transações, a discussão em torno do seu reconhecimento legal e validação permanece como um ponto central de debate no âmbito jurídico.
B) Contratos inteligentes são autoexecutáveis e operam sem a necessidade de intermediários; no contexto desse procedimento, os acordos formalizados são registrados em uma blockchain, garantindo transparência, segurança e imutabilidade, proporcionando uma redução de custos e um aumento na eficiência.
C) A execução de contratos inteligentes pode ser alterada manualmente e de forma livre após sua implementação.
D) Contratos inteligentes são exclusivamente usados em transações financeiras.
E) Blockchain é uma tecnologia de registro centralizada e imutável que permite o armazenamento de dados e informações de forma segura e distribuída; o que o diferencia de bancos de dados ou softwares convencionais

é sua resistência à adulteração, uma vez que a alteração de dados em um bloco requer a manipulação de todos os blocos anteriores.[22]

CAIU NO MPC-SC – Procurador de Contas do Ministério Público – 2022 – CEBRASPE: As transformações digitais e o uso de tecnologias disruptivas constituem grandes desafios, especialmente em se tratando de seus aspectos jurídicos. A esse respeito, julgue o item seguinte.

Ao contrário do que ocorre com os contratos tradicionais, a execução dos contratos inteligentes (smart contracts) implementados com a tecnologia blockchain pode ser automatizada, o que proporciona a mitigação de riscos, dada a previsibilidade garantida pelos códigos programados com base nessa tecnologia.[23]

3. LEI GERAL DE PROTEÇÃO DE DADOS (LEI N. 13.709/19)

A Lei Geral de Proteção de Dados Pessoais (LGPD), sancionada no Brasil em agosto de 2018, representa um marco significativo na regulamentação do tratamento de dados pessoais no país. A LGPD tem como principal objetivo proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade dos cidadãos brasileiros (dentro e fora da internet, de modo que vale, por exemplo, para estabelecimentos físicos).

A importância da proteção desses dados pessoais foi ainda mais reforçada com a **Emenda Constitucional nº 115, de 2022**, que elevou esse direito ao status de direito fundamental, garantindo, no artigo 5º, inciso LXXIX, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

A LGPD estabelece normas claras e abrangentes para o tratamento de dados pessoais por parte de empresas e organizações, sejam elas públicas ou privadas. Isso inclui qualquer operação realizada com dados pessoais, como coleta, armazenamento, compartilhamento e eliminação, independentemente do meio utilizado. A lei se aplica a toda operação de tratamento de dados que ocorra em território nacional, ou que tenha por objetivo a oferta de bens ou serviços a indivíduos localizados no Brasil.

Um dos pontos centrais da LGPD é a definição dos princípios que devem nortear o tratamento de dados pessoais. Entre eles, destacam-se o respeito à privacidade, a autodeterminação informativa, a inviolabilidade da intimidade, honra e imagem, e a necessidade de transparência por parte das empresas no uso dos dados coletados. Além disso, a lei também estabelece a necessidade de consentimento do titular dos dados para o seu tratamento, exceto em situações específicas previstas na legislação, como o cumprimento de obrigações legais ou a proteção da vida.

SE LIGA: Conjugando a determinação do art. 20 da LGPD com a eficácia dos direitos fundamentais nas relações privadas, entende-se que o titular de dados pessoais deve ser informado sobre a razão da suspensão de seu perfil, bem como pode requerer a revisão dessa decisão, garantido o seu direito de defesa. A plataforma pode suspender imediatamente o perfil do motorista quando entender que a acusação é

[22] Gabarito: B.
[23] Correto.

suficientemente gravosa, informando-lhe a razão dessa medida, mas ele poderá requerer a revisão dessa decisão, garantido o contraditório. Se tiver sido conferido o direito de defesa ao usuário e ainda assim a plataforma concluir que restou comprovada a violação aos termos de conduta, não há abusividade no descredenciamento do perfil. Até mesmo porque não se afasta a possibilidade de revisão judicial da questão. STJ. 3ª Turma. REsp 2.135.783-DF, Rel. Min. Nancy Andrighi, julgado em 18/6/2024 (Info 817).[24]

Vejamos suas principais disposições:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

CAIU NO TST – Magistratura do Trabalho – 2023 – FGV: Entre os fundamentos da disciplina da proteção de dados pessoais estão o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.[25]

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
> II - realizado para fins exclusivamente:
> a) jornalístico e artísticos; ou
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou
> 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

[24] CAVALCANTE, Márcio André Lopes. **Não há óbice para a imediata suspensão do perfil profissional de motorista de aplicativo que pratica ato suficientemente gravoso, com a possibilidade de posterior exercício de defesa visando ao recredenciamento.** Buscador Dizer o Direito, Manaus. Disponível em: <https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/c05c903e3d997added79518f0e850026>. Acesso em: 28/08/2024

[25] Correto

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 nesta Lei.

§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

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

§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. (Redação dada pela Lei nº 13.853, de 2019) Vigência

CAIU NO TST – Magistratura do Trabalho – 2023 – FGV: Excluem-se do âmbito territorial de aplicação da LGPD, os dados pessoais 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 Lei.[26]

CAIU NO TST – Magistratura do Trabalho – 2023 – FGV: O tratamento de dados pessoais realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, não são incluídos no âmbito de aplicação da LGPD.[27]

CAIU NO TRF – 4ª REGIÃO – Magistratura Federal – Banca Própria: A Lei Geral de Proteção de Dados não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de investigação e repressão de infrações penais.[28]

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

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

II - **dado pessoal sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso,

[26] Correto
[27] Correto
[28] Correto

filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

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

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

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

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

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

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

IX - **agentes de tratamento:** o controlador e o operador;

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

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

XII - **consentimento:** manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

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

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

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

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

XVII - **relatório de impacto à proteção de dados pessoais:** documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais

que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

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

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

CAIU NO TST – Magistratura do Trabalho – 2023 – FGV: Dado pessoal sensível é aquele que trata 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.[29]

SE LIGA NA JURIS: O vazamento de dados pessoais NÃO gera dano moral presumido." STJ. 2ª Turma. AREsp 2.130.619-SP, Rel. Min. Francisco Falcão, julgado em 7/3/2023 (Info 766).

CAIU NO I ENAM – 2024 – FGV (Reaplicação): Maria, para se tornar usuária do serviço público de abastecimento de água, forneceu à concessionária Alfa seus dados pessoais, que consistiam em nome completo, endereço residencial, data de nascimento, números de telefone, CPF e identidade. Três meses depois, a concessionária sofreu um ataque de hackers em seus sistemas e os dados pessoais de diversos consumidores, inclusive de Maria, foram copiados pelos criminosos, que, em seguida, venderam-nos para empresas que trabalham com telemarketing.

Inconformada por ter seus dados pessoais indevidamente comercializados, Maria ajuizou ação indenizatória em face da concessionária Alfa, alegando que sofreu danos morais in re ipsa, haja vista que foram vazados seus dados classificados pela Lei Geral de Proteção de Dados Pessoais (LGPD) como dados pessoais sensíveis. De acordo com a jurisprudência do Superior Tribunal de Justiça e com a Lei nº 13.709/2018, os dados vazados de Maria

A) são classificados como dados pessoais sensíveis, mas não há que se falar em dano presumido, devendo Maria comprovar os danos morais que efetivamente sofrera para ter êxito em sua pretensão.

B) são classificados como dados pessoais sensíveis e os danos morais sofridos são presumidos, em razão da natureza desses dados pessoais e pela relação de consumo existente entre Maria e a concessionária.

C) não são classificados como dados pessoais sensíveis, mas a LGPD os considera como dados sigilosos e, por isso, inverte-se o ônus da prova para se estabelecer a responsabilidade objetiva da concessionária e o dano in re ipsa.

[29] Correto

D) não são classificados como dados pessoais sensíveis, mas a LGPD os considera como extensão do direito da personalidade, de maneira que a falha no tratamento de dados de Maria, como pessoa natural, por pessoa jurídica, tem o condão, por si só, de gerar dano moral indenizável.
E) não são classificados como dados pessoais sensíveis pela LGPD, e sim dados pessoais, cujo vazamento não gera dano moral presumido.[30]

CAIU NO I ENAM – 2024 – FGV: Uma sociedade empresária de telefonia sofreu ataque cibernético que levou ao vazamento dos dados pessoais de todos os seus usuários. Posteriormente, diversos usuários acionaram o Judiciário, requerendo a condenação da sociedade empresária e o pagamento de danos morais, com base na alegação de que estavam sendo importunados com ligações de empresas de telemarketing após o vazamento dos seus dados.

De acordo com o entendimento do Superior Tribunal de Justiça quanto ao tema, analise as afirmativas a seguir.

I. O vazamento de dados pessoais não tem o condão, por si só, de gerar dano moral indenizável, sendo necessária prova efetiva do dano ocorrido.
II. O vazamento de dados pessoais gera para o prejudicado direito à indenização, uma vez que o dano moral, em tais casos, é presumido, podendo a empresa de telefonia fazer prova de que não houve prejuízo ao titular dos dados expostos.
III. O vazamento de qualquer tipo de dado sem autorização do usuário configura violação dos direitos à intimidade e à privacidade e enseja a condenação ao pagamento de danos morais.

Está correto o que se afirma em

A) I, apenas.
B) I e II, apenas.
C) I e III, apenas.
D) II e III, apenas.
E) I, II e III.[31]

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os **seguintes princípios**:
> I - **finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - **adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - **necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

[30] Gabarito: E
[31] Gabarito: A

IV - **livre acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - **qualidade dos dados:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI - **transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
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;
VIII - **prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - **não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X - **responsabilização e prestação de contas:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

CAIU NO TJDFT – Magistratura Estadual – 2023 – CEBRASPE: De acordo com a Lei Geral de Proteção de Dados Pessoais, a compatibilidade do tratamento dos dados pessoais com as finalidades informadas ao titular, de acordo com o contexto do tratamento, consiste no princípio da

A) adequação.
B) finalidade.
C) qualidade dos dados.
D) transparência.
E) segurança.[32]

Em que pese o **tratamento da dados pessoais**, este somente poderá ser realizado mediante o fornecimento de consentimento pelo titular, que deve se dar por escrito. Ademais, deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização. No caso de dados tornados manifestamente públicos pelo titular, fica dispensada a exigência do consentimento previsto.

CAIU NO TST – Magistratura do Trabalho – 2023 – FGV: O consentimento dado pelo titular, para o tratamento de seus dados pessoais, poderá ser por escrito ou por outro meio que demonstre a manifestação de vontade do titular, não sendo necessária cláusula destacada das demais cláusulas contratuais, quando fornecido por escrito.[33]

[32] Gabarito: A
[33] Incorreto

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

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

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

a) cumprimento de obrigação legal ou regulatória pelo controlador;

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

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

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

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

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

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

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

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

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

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

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

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

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

CAIU NO TJ-ES – Magistratura Estadual – 2023 – FGV: O tratamento de dados pessoais sensíveis somente poderá ocorrer quando o seu titular autorizar.[34]

Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

§ 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

CAIU NO TJ-ES – Magistratura Estadual – 2023 – FGV: Poderá ser considerado dado pessoal aquele utilizado para formação do perfil comportamental de determinada pessoa natural, se identificada.[35]

CAIU NO TRF – 4ª REGIÃO – Magistratura Federal – 2022 – Banca Própria: Os dados pessoais anonimizados e pseudonimizados não são considerados dados pessoais para os fins da lei.[36]

Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

[34] Incorreto
[35] Correto
[36] Incorreto

§ 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.
§ 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.
§ 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.
§ 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

CAIU NO TRF 3ª REGIÃO – Magistratura Federal – 2022 – Banca Própria: Pesquisadores da área de saúde de uma Universidade pública federal estão realizando uma pesquisa para investigar a hipótese de que a COVID-19 impactou de maneira desigual a população negra no país. Para tanto, requereram o acesso à base de dados pessoais do Sistema Único de Saúde às autoridades sanitárias federais. Assinale a alternativa CORRETA quanto à incidência da Lei Geral de Proteção de Dados à hipótese:

A) Como o dado sobre a origem racial ou étnica é considerado um dado pessoal sensível pela legislação, apenas com o consentimento de cada indivíduo seria possível esse acesso.
B) Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, inclusive a origem racial ou étnica, desde que os estudos sejam mantidos em ambiente controlado e seguro, respeitando-se, sempre que possível, a anonimização ou pseudonimização dos dados, e observância dos padrões éticos nos termos da legislação.
C) O órgão de pesquisa será o responsável pela segurança da informação, admitindo-se, apenas em circunstâncias excepcionais, a transferência dos dados a terceiros como previsto na legislação.
D) A Lei Geral de Proteção de Dados não tem disciplina sobre tratamento de dados pessoais realizados para fins exclusivamente acadêmicos. [37]

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:
I - em formato simplificado, imediatamente; ou
II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.
§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.
§ 2º As informações e os dados poderão ser fornecidos, a critério do titular:

[37] Gabarito: B

I - por meio eletrônico, seguro e idôneo para esse fim; ou
II - sob forma impressa.
§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.
§ 4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.

CAIU NO TJ-GO – Magistratura Estadual – 2021 – FCC: O acesso a dados pessoais de terceiros depende de pedido de instauração de procedimento de desclassificação, dirigido à autoridade máxima do órgão detentor das informações.[38]

Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.
§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:
I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) ;
II - (VETADO);
III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.
IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou (Incluído pela Lei nº 13.853, de 2019) Vigência
V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades. (Incluído pela Lei nº 13.853, de 2019) Vigência
§ 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.

CAIU NO TJ-ES – Magistratura Estadual – 2023 – FGV: É sempre vedado ao poder público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso. [39]

[38] Incorreto
[39] Incorreto

Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.
§ 2º As atividades do encarregado consistem em:
I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
II - receber comunicações da autoridade nacional e adotar providências;
III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.
§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.
§ 4º (VETADO). (Incluído pela Lei nº 13.853, de 2019) Vigência

CAIU NO TJ-ES – Magistratura Estadual – 2023 – FGV: O operador é o responsável por indicar o encarregado pelo tratamento de dados pessoais, cuja identidade e informações de contato deverão ser públicas.[40]

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
§ 1º A comunicação será feita em **prazo razoável**, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
I - a descrição da natureza dos dados pessoais afetados;
II - as informações sobre os titulares envolvidos;
III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
IV - os riscos relacionados ao incidente;
V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:
I - ampla divulgação do fato em meios de comunicação; e
II - medidas para reverter ou mitigar os efeitos do incidente.

[40] Incorreto

> § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

CAIU NO TJ-ES – Magistratura Estadual – 2023 – FGV: O controlador deverá comunicar, no prazo de 48 horas, à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.[41]

CAIU NO TRF – 4ª REGIÃO – Magistratura Federal – 2022 – Banca Própria: O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de todos os incidentes de segurança. [42]

Outro aspecto fundamental da LGPD é a criação da **Autoridade Nacional de Proteção de Dados (ANPD)**. A ANPD é o órgão responsável por zelar pela proteção dos dados pessoais e pela aplicação da lei, fiscalizando e orientando as empresas sobre as melhores práticas a serem adotadas. Além disso, a ANPD tem o poder de aplicar sanções em caso de descumprimento das normas estabelecidas pela LGPD, que podem variar desde advertências até multas significativas.

IMPORTANTE: Em julho de **2023**, a Autoridade Nacional de Proteção de Dados (ANPD) **aplicou a primeira multa por descumprimento da Lei Geral de Proteção de Dados (LGPD).** A empresa Telekall Infoservice foi penalizada após uma denúncia que indicava a oferta de listagens de contatos de WhatsApp de eleitores para fins de campanha eleitoral durante as eleições municipais de 2020, em Ubatuba/SP. A ANPD concluiu que o tratamento de dados foi realizado sem base legal e que a empresa não nomeou um encarregado de proteção de dados, como exigido pela LGPD. Como resultado, a Telekall foi multada em R$14.400,00 e recebeu uma advertência.[43]

Sua composição se dá nos termos do art. 55-D, o qual dispõe o seguinte:

> Art. 55-D. O Conselho Diretor da ANPD será composto de 5 (cinco) diretores, incluído o Diretor-Presidente. (Incluído pela Lei nº 13.853, de 2019)
> § 1º Os membros do Conselho Diretor da ANPD serão escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, nos termos da alínea 'f' do inciso III do art. 52 da Constituição Federal, e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superiores - DAS, no mínimo, de nível 5. (Incluído pela Lei nº 13.853, de 2019)
> § 2º Os membros do Conselho Diretor serão escolhidos dentre brasileiros que tenham reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados. (Incluído pela Lei nº 13.853, de 2019)

[41] Incorreto
[42] Incorreto
[43] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd

§ 3º O mandato dos membros do Conselho Diretor será de 4 (quatro) anos. (Incluído pela Lei nº 13.853, de 2019)

§ 4º Os mandatos dos primeiros membros do Conselho Diretor nomeados serão de 2 (dois), de 3 (três), de 4 (quatro), de 5 (cinco) e de 6 (seis) anos, conforme estabelecido no ato de nomeação. (Incluído pela Lei nº 13.853, de 2019)

§ 5º Na hipótese de vacância do cargo no curso do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor. (Incluído pela Lei nº 13.853, de 2019)

Os membros do Conselho Diretor, por sua vez, somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar.

CAIU NO TJ-RJ – Magistratura Estadual – 2023 – VUNESP: Considere que Letícia é membro do Conselho Diretor da Autoridade Nacional de Proteção de Dados (ANPD), ocupando o cargo de Diretora-Presidente. De acordo com a situação hipotética e com a Lei Geral de Proteção de Dados, é correto afirmar que Letícia

A) foi escolhida e nomeada pelo Presidente da República e previamente aprovada, por voto secreto, após arguição pública, pelo Senado Federal.
B) tem pelo menos 35 anos, reputação ilibada, mestrado na área de interesse e elevado conceito no campo de especialidade do cargo para o qual foi nomeada.
C) foi escolhida pelo Ministro de Estado Chefe da Casa Civil e nomeada pelo Presidente da República e tem mandato de dois anos, permitida uma recondução.
D) ocupa cargo em comissão do Grupo-Direção e Assessoramento Superiores - DAS, no mínimo, de nível 3.
E) poderá ser exonerada livremente do seu cargo, uma vez que se trata de cargo de comissão de livre nomeação e exoneração.[44]

Em um caso relevante envolvendo a Lei Geral de Proteção de Dados (LGPD), a Justiça confirmou uma liminar que determinou à **Serasa Experian** a suspensão da comercialização de dados pessoais por meio dos produtos "Lista Online" e "Prospecção de Clientes". A decisão foi tomada pela 5ª Vara Cível de Brasília, após ação civil pública movida pelo Ministério Público do Distrito Federal e Territórios (MPDFT). O MPDFT alegou que a prática de venda de dados como CPF, nome, endereço e telefone, sem consentimento específico, violava a LGPD, que exige o consentimento explícito dos titulares para cada finalidade de uso. A Serasa alegou que suas atividades estavam alinhadas com a lei, mas a Justiça considerou a comercialização ilegal e reforçou a necessidade de consentimento claro dos titulares para o tratamento e compartilhamento de seus dados[45].

Em um caso de vazamento de dados, a **Netshoes** foi condenada a pagar R$ 500 mil em indenização por danos morais coletivos, após a divulgação de informações pessoais de quase 2 milhões de clientes. O vazamento, ocorrido em 2017, expôs dados como nome, CPF, endereço e informações de pedidos. Entre os

[44] Gabarito: A
[45] Disponível em: https://www.tjdft.jus.br/institucional/imprensa/noticias/2021/julho/lgpd-justica-determina-que-serasa-deixe-de-comercializar-dados-pessoais

dados vazados, estavam informações de servidores públicos de órgãos como o Tribunal de Contas da União e o Supremo Tribunal Federal. Para evitar um processo maior, a Netshoes firmou um Termo de Ajustamento de Conduta (TAC) com o Ministério Público do Distrito Federal e Territórios (MPDFT), comprometendo-se a implementar medidas de segurança e adequar sua política de proteção de dados à Lei Geral de Proteção de Dados (LGPD). Em caso de descumprimento, a empresa estaria sujeita a novas ações cíveis, com indenizações que poderiam atingir R$ 10 milhões[46].

Em dezembro de 2020, uma falha de segurança no **Ministério da Saúde** expôs dados pessoais de 243 milhões de brasileiros, incluindo informações de pessoas já falecidas. O vazamento foi causado pela exposição indevida de login e senha de acesso ao sistema do Ministério, comprometendo dados como CPF, nome completo, endereço e telefone. O incidente afetou tanto cidadãos cadastrados no Sistema Único de Saúde (SUS) quanto em planos de saúde. Essa falha ocorreu apenas uma semana após um vazamento semelhante de dados de 16 milhões de pacientes que tiveram Covid-19. Apesar do Ministério afirmar que a base de dados e-SUS Notifica não foi acessada, a exposição levantou preocupações sobre a fragilidade dos sistemas de proteção de dados públicos no Brasil. A falha foi corrigida após a denúncia, e investigações foram iniciadas para apurar responsabilidades.[47]

Já em agosto de 2024, a Autoridade Nacional de Proteção de Dados (ANPD) suspendeu a proibição imposta à Meta (empresa responsável pelo Facebook, Instagram e WhatsApp) de utilizar dados pessoais para treinar sua inteligência artificial. Inicialmente, em julho, a ANPD havia expedido uma medida preventiva devido ao risco de danos graves aos titulares dos dados. No entanto, após a Meta apresentar um Plano de Conformidade, a ANPD autorizou a retomada, com restrições, do uso de dados.

Entre as exigências, a Meta deverá garantir que os dados de crianças e adolescentes não sejam utilizados no treinamento da IA e implementar medidas que ampliem a transparência sobre o uso de dados. Usuários serão notificados de forma clara e terão o direito de negar o uso de seus dados pessoais por meio de um formulário simplificado, acessível tanto por e-mail quanto diretamente nos aplicativos. A ANPD continuará monitorando o cumprimento dessas obrigações pela Meta.[48]

4. Audiências Virtuais

As audiências virtuais no Judiciário brasileiro, regulamentadas inicialmente pela **Resolução 354/2020** do Conselho Nacional de Justiça (CNJ), ganharam maior relevância durante a pandemia de Covid-19 e, posteriormente, foram consolidadas como parte permanente dos procedimentos judiciais. Com a Resolução 481/2022, que atualizou a norma anterior, foram introduzidas novas diretrizes para o uso das audiências telepresenciais e por videoconferência.

[46] Disponível em: https://www.jusbrasil.com.br/noticias/netshoes-tera-de-pagar-r-500-mil-por-vazamento-de-dados-de-milhoes-de-clientes/685006882

[47] Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml

[48] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/meta-cumpre-exigencias-da-anpd-e-podera-retomar-com-restricoes-o-uso-de-dados-pessoais-para-treinamento-de-inteligencia-artificial#

A Resolução 481/2022 estabelece que o juiz pode determinar, de ofício, a realização de audiências virtuais em situações específicas, como urgências, substituição de magistrado, mutirões, conciliações, mediações e em casos de indisponibilidade temporária do foro.

A norma também trata da participação de advogados e partes por videoconferência, desde que exista viabilidade técnica e conveniência, cabendo ao magistrado avaliar a pertinência. A participação de réus presos fora da sede da comarca por videoconferência é mantida, como forma de assegurar celeridade e segurança nos processos.

Essa Resolução 481/2022 reforça a necessidade de seguir as formalidades dos atos processuais, assegurando a publicidade dos atos e o respeito às prerrogativas processuais de todas as partes envolvidas, de acordo com os princípios constitucionais aplicáveis.

Mas é a **Resolução 508/2023 do CNJ** que regula a instalação **de Pontos de Inclusão Digital (PID)** pelo Poder Judiciário, com o objetivo de ampliar o acesso à justiça em localidades sem unidades físicas do Judiciário, como cidades, povoados e aldeias. A medida visa facilitar o atendimento a cidadãos que, de outra forma, precisariam se deslocar para obter serviços judiciais.

Os PIDs são salas equipadas com tecnologia para a realização de atos processuais, como depoimentos por videoconferência, além de permitir o uso de ferramentas como o Balcão Virtual. A resolução classifica esses pontos em diferentes níveis, de acordo com os serviços oferecidos e a integração com outros órgãos públicos, como Defensoria Pública e Ministério Público.

> Art. 2º Os Pontos de Inclusão Digital serão divididos em 4 (quatro) níveis, de acordo com os serviços que oferecem:
>
> I – **PID nível 0**: com atendimento virtual de apenas 1 (um) ramo do Poder Judiciário;
>
> II – **PID nível 1:** com atendimento virtual de pelo menos 2 (dois) ramos do Poder Judiciário;
>
> III – **PID nível 2:** com atendimento virtual de pelo menos 2 (dois) ramos do Poder Judiciário e pelo menos 1 (um) dos seguintes órgãos: Defensoria Pública, Ministério Público, Procuradorias Públicas e/ou Advocacia Pública da União, Polícias, Municípios e outros órgãos da administração pública direta e indireta de qualquer nível;
>
> IV – **PID nível 3**: com atendimento virtual de pelo menos 3 (três) ramos do Poder Judiciário e pelo menos 2 (dois) dos seguintes órgãos: Defensoria Pública, Ministério Público, Procuradorias Públicas e/ou Advocacia Pública da União, Polícias, Municípios e outros órgãos da administração pública direta e indireta de qualquer nível, além de sala e equipamentos para atendimento presencial destinado à realização de perícias médicas;

V – **PID nível 4:** com atendimento virtual de pelo menos 4 (quatro) ramos do Poder Judiciário e pelo menos 3 (três) dos seguintes órgãos: Defensoria Pública, Ministério Público, Procuradorias Públicas e/ou Advocacia Pública da União, Polícias, Municípios e outros órgãos da administração pública direta e indireta de qualquer nível, além de sala e equipamentos para atendimento presencial destinado à realização de perícias médicas, e ainda atendimento de cidadania com a cooperação de entidades privadas e da sociedade civil.

A resolução também estabelece metas para a instalação dos PIDs em municípios com até 50 mil habitantes, distantes de sedes de comarcas. Os tribunais devem providenciar a infraestrutura necessária para o funcionamento desses pontos, além de assegurar que as instalações sejam acessíveis e que as equipes locais recebam o treinamento adequado.

O texto prevê ainda que os atos processuais realizados nesses pontos sejam equiparados aos presenciais para todos os efeitos legais. A implantação dos PIDs é parte de uma estratégia de inclusão digital e busca aprimorar a prestação jurisdicional em localidades desassistidas.