

UNIVERSIDADE CATÓLICA DE PERNAMBUCO
CENTRO DE CIÊNCIAS JURÍDICAS
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
CURSO DE DOUTORADO EM DIREITO
CORSO DI DOTTORATO IN SCIENZE GIURIDICHE
UNIVERSITÀ DI PISA

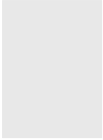
**ANÁLISE SOBRE A ADEQUAÇÃO AO ORDENAMENTO PROCESSUAL DAS
NORMAS SOBRE PROTEÇÃO DE DADOS PESSOAIS DURANTE A REALIZAÇÃO
DE AUDIÊNCIAS POR VIDEOCONFERÊNCIA NO BRASIL E NA ITÁLIA.**

Aline Taraziuk Nicodemos

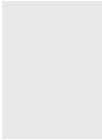
Recife

Pisa

2024



Aline Taraziuk Nicodemos



**ANÁLISE SOBRE A ADEQUAÇÃO AO ORDENAMENTO PROCESSUAL DAS
NORMAS SOBRE PROTEÇÃO DE DADOS PESSOAIS DURANTE A REALIZAÇÃO
DE AUDIÊNCIAS POR VIDEOCONFERÊNCIA NO BRASIL E NA ITÁLIA.**

Tese apresentada aos Programas de Pós-Graduação em Direito da Universidade Católica de Pernambuco e *Università di Pisa*, como requisito parcial para obtenção do título de Doutora em Direito.

Área de concentração: Direito Processual, digital e internacional.

Linhas de pesquisa:

Processo, Hermenêutica e Efetividade de Direitos.

Impresa, Diritto Internazionale, Diritto dell'Unione Europea, Processo Civile.

Orientador: Prof. Dr. Alexandre Freire Pimentel

Diretrice: Prof.ssa Dott.ssa Francesca Martines

Recife
Pisa

2024

N633a

Nicodemos, Aline Taraziuk.

Análise sobre a adequação ao ordenamento processual das normas sobre proteção de dados pessoais durante a realização de audiências por videoconferência no Brasil e na Itália, / Aline Taraziuk. Nicodemos, 2024.

194 f. : il.

Orientador (es): Alexandre Freire Pimentel, Francesca Martines.

Tese (Doutorado) - Universidade Católica de Pernambuco. Università di Pisa. Programa de Pós-graduação em Direito. Doutorado em Direito, 2024.

1. Direito Processual. 2. Processo judicial.
3. Direito à privacidade. 4. Tecnologia e direito.
5. Brasil [Lei geral de proteção de dados pessoais (2018)].
6. Parlamento Europeu. General Data Protection Regulation.
7. Internet nos serviços jurídicos. I. Título.

CDU 347.9

Luciana Vidal - CRB-4/1338

FOLHA DE APROVAÇÃO

Aluno (a): Aline Taraziuk Nicodemos

Título da Tese

**Análise sobre a Adequação ao Ordenamento Processual das Normas sobre
Proteção de Dados Pessoais Durante a realização de audiência por
videoconferência no Brasil e na Itália.**

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Direito da
Universidade Católica de Pernambuco (UNICAP) para obtenção do título de
Doutor (a) em Direito. A presente tese foi defendida e aprovada em 31/10/2024
pela banca examinadora e constituída pelos professores:

Alexandre Freire Pimentel

Orientador

Documento assinado digitalmente

gov.br

PALOMA MENDES SALDANHA

Data: 27/04/2025 17:36:55-0300

Verifique em <https://validar.itl.gov.br>

Paloma Mendes Saldanha

Examinadora Interna

Documento assinado digitalmente

gov.br

GUSTAVO FERREIRA SANTOS

Data: 28/04/2025 10:47:44-0300

Verifique em <https://validar.itl.gov.br>

Gustavo Ferreira Santos

Examinador Interno



Francesca Martins

Examinadora Externa

Documento assinado digitalmente

gov.br

DIOGO RAIS RODRIGUES MOREIRA

Data: 25/04/2025 16:07:12-0300

Verifique em <https://validar.itl.gov.br>

Diogo Rais Rodrigues Moreira

Examinador Externo



Leonardo Pasquali

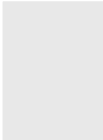
Examinador Externo

Recife

2024



A Deus e aos anjos do céu. A eles, que de onde estiverem, sei que olham, cuidam e torcem por mim: mainha, painho e voinha. Foi onde tudo começou. A minha família, minha raiz e minha fortaleza.



Agradecimentos

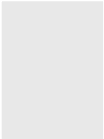
Antes de todos os agradecimentos eu preciso dizer da importância desse período em minha vida e o significado desse título, que vai muito além de um grau acadêmico e profissional. É a realização de um sonho e muitas pessoas embarcaram comigo nessa jornada e sonharam e torceram por mim.

Dentro desse sonho eu tive mais sonhos, lindos, alguns atropelos e superações, mas eu acreditei na força interior, na fé e eu considero o final desse doutorado uma verdadeira vitória. Foram quase 4 anos que me fizeram ser mais forte. A vida me desafia e é impressionante como sempre estou pronta para enfrentar cada luta que aparece no caminho.

Para tudo isso acontecer foi uma grande equipe por trás. Primeiramente, a minha gratidão a Deus, o Senhor de todos e de todas as coisas, Aquele que me permitiu realizar todas as conquistas e ultrapassar todos os obstáculos. A Jesus, por trazer a verdade, o amor, me colocando em situações que me permitiram fazer escolhas, ainda que algumas vezes erradas. O Senhor me banha, todos os dias, de esperanças de uma nova aurora em minha vida. Generosamente me deram mais que o necessário para estar aqui agora com essa bagagem cheia de coisas boas no coração.

Aos espíritos de luz, anjos que Deus permite estarem comigo nessa vida e sempre se fazem presentes e deixam a certeza de que eu não estou só. Aos ciganos, que com muito amor, paciência e compreensão, persistência crença em mim, luzes que me acompanham e me acompanharam nessa trajetória, especialmente o cigano Emílio Rossini, que não me abandona nunca. Graças a Deus. Poderia escrever um livro contando todas as vezes que se fez presente da forma que eu pudesse compreender que estava ali. E a Yan que não soltou a minha mão e cuida e cuidou de mim. A Antônio Wladimir que com toda sua sabedoria e amor me guiou os passos para alcançar os meus objetivos. Só consigo dizer que a beleza de tudo que eu vejo e o que sinto são coisas difíceis de descrever. Tenho limitações para compreender o tanto que eu recebo e eu só posso agradecer muito, não somente por esse projeto recheado de coisas boas, mas por tudo e sempre. Meus olhos materiais não os veem, mas ainda bem que eu posso sentir ou entender as mensagens enviadas nos meus dias bons e naqueles nem tão bons. Eu tenho sorte de tê-los comigo.

Eu eternamente irei agradecer aos que me deram a vida, que me amaram e que continuam me amando em um outro lugar e graças a Deus eu tenho a plena convicção de que andam comigo. Uma mãe e um pai não deixam seus filhos sozinhos, eles só estão presentes de outra forma. Vocês são a minha essência e, como disse uma vez a Monja Cohen, uma mãe não

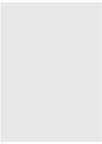


morre, ela sempre tá em algum momento, quando a gente vai montar um prato vem aquela voz da mãe na cabeça: põe legumes, alface...ela tem razão, a gente escuta por onde quer que passemos e eu digo que estão em cada momento de todos os meus passos. De onde estiverem, saibam que criaram pessoas fortes, dedicadas, que tem caráter e amor sólidos. Vocês fazem falta, a saudade nunca acaba. Queria brindar com vocês aqui e ver o sorriso de vocês, dando aquele abraço. Que bom que um dia iremos nos encontrar. Eu estarei cheia de coisas para falar com vocês. Mainha, aí tem café da manhã? Para a gente poder acordar e já começar a conversar? Você é incrível! Alguns me chamam de Cristininha. Eu tenho orgulho. Painho, eu já vi o brilho dos seus olhos em sonho certa vez e eles brilhavam de um modo magnífico, acho que quanto mais belo, mais feliz é. Olha, aquela menininha que falava sem parar hoje é uma mulher de garra! Continua faladeira. Você tá preparado para me ouvir tagarelar? Iremos almoçar nos domingos? Ah, vocês não sabem quantas recordações afetivas deixaram e que me alimentam até hoje. É por tudo isso e muito mais que eu estou aqui. Obrigada meus eternos amores.

À voinha, dona Nilda. Incentivadora constante dos meus estudos. Não media esforços para que tivesse o que fosse necessário para minha formação e bem-estar e de meus irmãos. Certamente eu sou bem melhor por tudo que a senhora fez. Eu terminei os estudos. A senhora nunca imaginou que eu fosse continuar tanto e fazer tudo isso...O sucesso da gente enchia a senhora de alegria e orgulho. É, voinha, cheguei aqui. Obrigada por alimentar o meu interior de ideais tão necessários, eles estão bem enraizados. Obrigada pelas tantas e tantas tentativas para que tivéssemos o melhor. Tenha certeza de que tudo valeu a pena.

A tio Sony e à Baby. Sem o apoio de vocês eu jamais conseguiria. Um sonho não se sonha só. Desde o início me incentivaram a construir o que fosse necessário para minha formação. Isso vem de muito tempo e eu sei... não começou agora, vem muito antes do mestrado...Me lembro do dia que tivemos a conversa sobre eu fazer a seleção do doutorado. Vocês já sabiam de tudo que eu queria. Ainda disseram que eu iria poder fazer parte dele na Itália. E à Clarissa com sua miniatura Nina, por estarem comigo. Lembro ainda hoje quando liguei para você dizendo que passei no doutorado e chorava horrores dizendo que tinha conseguido. Senti do lado de cá a sua alegria pela minha alegria. Você é prima irmã. Difícil de dizer o tudo. É na saúde e na doença, nas alegrias e nas tristezas. Obrigada.

À Alice e a Alex, vocês são aquelas correntes, por mais largas que estejam, eu sempre os vejo crescendo comigo. Um dia entenderemos o porquê de tantas e tantas coisas nas nossas vidas. Mas estamos aqui. Que feliz dividir isso com vocês. Somos e seremos sempre vencedores. Essa vitória não é só minha, assim como me vejo pertencente a vitória de vocês.

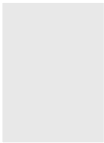


Ainda iremos muito mais longe. Obrigada por estarem comigo, por falarem o que precisa ser dito. Para além de todas as dificuldades eu tive exemplos de vocês. Vamos juntos! Alice, obrigada por ser uma fiel escudeira. Se não houvesse seu apoio com certeza eu não teria chegado aqui, porque mais que qualquer outra coisa, o amor é a maior riqueza que podemos ter e você fez o amor se concretizar em companhia e cuidado. Arregaçou as mangas de uma forma que não sei de onde você tirou forças. Abriu as portas da sua casa, com Léo e Bernardo e não mediram esforços. Um dia eu cuidei de você, quando era pequena, e hoje você cuida de mim. E olha, tô forte! Boazinha! Pronta para outra! Alex, você me deu lições com algumas palavras que ecoam até hoje e você nem sabe. Eu sei que estamos longe, mas sei que você tá perto. Aprendemos a lidar com distâncias físicas. Sei que foram muitas preocupações, mas deu tudo certo! Vim e venci!

A todos os outros irmãos Adelma, Junior, Aluizio, obrigada! Aluizio (Brother), Carine e Luiza, a torcida de vocês emana energia que eu sinto de longe. Com certeza foi impulso para que tudo seguisse da melhor forma. E foi! Obrigada pelo incentivo e torcida para que tudo acontecesse da melhor forma e como Deus quis. Estou realizada.

Nessa tortuosa caminhada da vida tive cias, ombros, afetos, eu agradeço por tudo isso e muito mais aos meus outros tios. Tia Ana e Tio Cláudio, por tudo que fizeram por mim. Os cuidados genuínos comigo serão inesquecíveis. Durante tempos de desafios que forma tantos... Um deles, quando estava no processo seletivo, fui acometida pelo COVID. Todos os dias vocês deixavam minhas refeições na minha porta, mesmo sabendo que eu não sentia gosto de nada. Aqueles atos não eram meros alimentos para o corpo, eram carinhos diante do isolamento físico e pelos efeitos da doença que eram amenizados com esse amor. A tia Aleksy, tia Tereza, Camila e Igor, pela torcida a todo tempo para que eu conseguisse o que eu tanto desejava, alcançar essa vitória. Obrigada.

À Karine, Christiane, tia Vera e tio Jarbas. Vocês não só acreditaram em mim, mas na força que eu precisei arranjar para alcançar a finalização desse trabalho do jeito que eu gostaria que fosse. Karine e Christiane emprestaram os ouvidos de uma doutoranda no auge do seu trabalho com todos os falatórios de praxe que um estudante tem nessa fase. Karine teve até a missão de ler a tese. Me orientou e acho que consegui. Christiane ouviu lamentos de todas as vezes que achei que não fosse conseguir e ela sempre disse: mas vai dar certo. É assim mesmo. Eu estou me vendo em você. A apreensão sobre o final dessa tese foi a tensão que rondou as nossas conversas. Ainda bem que vocês sabem o que eu estou falando. Tia Vera é uma



incentivadora, vibra com alegria as minhas vitórias e junto com tio Jarbas cuidaram de mim. São recordações de muito amor. A todos vocês obrigada por tudo, tudo.

Aos meus amigos, todos eles, que torcem vendo a luta. Uns acompanharam bem de perto e me questionavam se era isso que eu realmente queria. E quando eu afirmava que sim todos me acompanhavam. Torciam e torciam. Acreditaram que daria tudo certo. E deu.

À Karla, que ouviu várias lamúrias diárias, risos e choros, projetos e sonhos constantemente e esperava ansiosamente, como eu, as respostas das correções da tese. À Dani que do mesmo modo tava aqui comigo perguntando: honey, como você está? Deu certo? Graças a Deus! Aproveite! Vamos fazer aquele lanche! Essas aguentaram bastante coisa minha, me fizeram cia sempre...independente de onde eu estivesse. Vocês são incríveis. E não sei como aguentam ouvir tanta coisa. É praticamente uma terapia... obrigada, meninas.

À Thaísa, amiga com quem dividi e divido também os meus sonhos. Ela fica ali, esperando, acreditando e participando de tudo. É uma torcida grande. E fica feliz quando eu tô feliz! Se faz presente em cada passo que eu dou. Obrigada, minha querida!

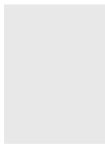
À Lulu que fica numa torcida incrível com Guila para que tudo dê certo. Que vibram e acreditam em tudo que acontece e o que está por vir. Tem um pequeno que nem sabe o que tá acontecendo, mas já manda energias positivas para mim: João Guilherme! Obrigada!!

À Paloma, que divide a felicidade dessa conquista, que sabe o valor disso tudo e sabe os obstáculos pelos quais eu passei. Me deu uma luz para iniciar essa jornada que termina com esse trabalho. Que ensina e inspira e que acompanha, apoia e torce por tudo! Obriagdaaa!

À Katiene, Rodrigo e o pequeno Ravi, que participaram da longa trajetória e hoje continuam ao meu lado. Torcem pelo meu crescimento, me apoiam e são verdadeiros parceiros. Cada palavra de incentivo chega com muita força aqui! Obrigada!

A Glebson, que além de meu coordenador, é meu amigo, que esteve comigo, se fazendo presente, que me lembrava que era possível, que eu deveria arriscar quando aparecia uma oportunidade. Ele me empurrou para conquistar. Que quando eu disse que iria para o outro lado do mundo, me apoiou e me deu suporte para que eu conseguisse fazer uma parte do meu doutorado fora.

Aos amigos do Lar da Fraternidade Francisco de Assis, desde os dirigentes Marlea e Neto, aos colaboradores, em especial Mônica e Mayana, que torceram todos os dias para que tudo desse certo nessa trajetória cheia de obstáculos que é a vida. Amigos que vibraram com



minhas vitórias, se preocuparam com todas as dificuldades que surgiam e me ajudaram a ficar em pé, junto com a espiritualidade amiga. A esses amigos de caminhada, de força e de apoio meu muito obrigada.

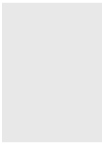
À família Barros de Araújo: Dany, Dr. Wilson, Finha e em especial a Netinho que tanto me ajudou para que eu conseguisse ultrapassar os meus desafios e então poder dar continuidade ao Doutorado. Vocês são demais! Dany, uma amiga. Esteve de longe, mas sempre perto, que deu o primeiro socorro chamando Netinho para me ajudar. Netinho, obrigada por enfrentar comigo as dificuldades que apareceram no ano de 2023. Eu sei que dei um trabalhão e mesmo assim você não largou a mão. Obrigada por tudo.

Aos amigos Carolina Izidoro, Júlia e Marciel, que antes de chegar a Itália já me davam um suporte imenso. Durante o tempo que estivemos juntos vivemos coisas incríveis, alguns difíceis, outros de plena satisfação. Estiveram nos momentos de muitas alegrias e naqueles que enfrentei dificuldades. Obrigada pelo apoio, a amizade e pelo carinho que tiveram comigo. Acreditem, vocês também fazem parte dessa história.

Rodrigo Deodato, um amigo que pude conhecer melhor nessa passagem por Pisa e pude estreitar os laços logo quando cheguei. Foram aproximadamente 2 meses que compartilhamos na Itália. Muitos almoços e jantares, muitas risadas que tornaram os dias agradáveis e leves. Incrivelmente, foram fantásticos dias na Toscana. Temos muitas histórias, amigo. Foi um prazer poder dividir esses dias, regados a vinhos, debates, cultura explicada detalhadamente, arte e gargalhadas. Uma grata surpresa poder ter estado com você em uma fase tão importante. Obrigada!

Pedro Monteiro, que surpresa boa conhecer você! Obrigada por compartilhar dias de conversas intermináveis, explicações, orientações de direito, cultura, arte, filosofia e tantas outras coisas que emendávamos em nossas conversas. Delas saíram muitas ideias e aprendizados. Foi divertido, agradável e enriquecedor ter você por perto. Tenha certeza de que ficará marcado nas minhas memórias e vai fazer falta não ter o contato diário com você! Mas espero você em Recife para podermos lembrar os dias alegres que tivemos! Obrigada!!

Aos meus professores, todos que passaram na minha vida. Em especial, gostaria de agradecer ao meu orientador Alexandre Freire Pimentel, que mais que um mestre, é um amigo. Esteve comigo nessa etapa e nas adversidades que se apresentaram na caminhada da vida e, com calma, me dizia: pode contar comigo! Me aceitou como orientanda no Mestrado e desde lá não deixou de dar continuidade aos ensinamentos. E chegamos ao meu doutorado! Me deu



auxílio e palavras de conforto me fazendo acreditar que tudo daria certo! Obrigada pela parceria para terminar uma fase tão importante da minha vida. Obrigada, Pimentel!

Ao professor Marcelo Labanca que me abriu a porta para ir à Universidade de Pisa, mas que também é um amigo que estendeu a mão em vários momentos e apoiou a condução desse meu projeto de vida. Ele não tem a ideia da grandiosidade do que ele fez por mim. Me ajudou a realizar o sonho de ir estudar na Itália. Obrigada pela preocupação, pela ajuda em todo o processo para dar tudo certo no final.

Ao professor José Mário, com quem sempre conto na minha trajetória acadêmica, sempre tem uma palavra para aliviar o furacão em que, às vezes, a vida se transforma. Certa vez ele perguntou como estavam as coisas e eu olhei com aquela cara de assustada e cansada e ele disse: calma, o semestre já está acabando. Obrigada, Zé!

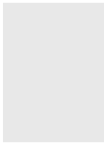
Professor Fábio Túlio, obrigada pelas aulas, pelo apoio e por acreditar no meu potencial. A oportunidade de elaborar trabalhos em parceria me ensinou muito mais que Direito. Me rememorou que o trabalho em cooperação traz muita riqueza e sou grata por ter aceitado trabalhar em coautoria comigo.

Ao professor Sérgio Torres, que desde o mestrado sempre foi um exemplo de profissional, professor e ser humano e, dentre as suas qualidades, a forma como conduz seu trabalho comprova uma habilidade bonita de se ver. Sempre uma pessoa que vibra com as vitórias dos seus alunos, me prestigiou ao saber que iria estudar na Itália. Obrigada pelo aprendizado, professor.

E a todos os outros mestres que passaram pela minha trajetória estudantil e profissional, que me preencheram de valiosos ensinamentos, me permitiram chegar à reta final da pesquisa e à conclusão do trabalho.

À *professoressa* Francesca Martines, que se disponibilizou em ser minha orientadora na Universidade de Pisa, dando um grande suporte durante o tempo em que estive na Itália, contribuindo de forma valorosa para a elaboração do trabalho de conclusão e a qual agradeço imensamente os ensinamentos. Obrigada pelas aulas, correções e incentivo para a finalização da pesquisa. Foi um grande desafio e uma experiência incrível! Obrigada!

Agradeço também ao *professore* Leonardo Pasquali, que deu suporte, orientação e proporcionou um trabalho em equipe que me trouxe muito aprendizado. Obrigada pela parceria



nesse processo para chegar à Pisa. Posso dizer que aprendi muito e só tenho que agradecer a oportunidade.

Aos coordenadores do PPGD da Unicap Profª. Érica Babini e Prof. Glauco pela compreensão, apoio e por estarem sempre disponíveis para me ajudar em tudo que foi necessário para que eu pudesse seguir com o curso. Não mediram esforços. Foram grandes desafios, todos enfrentados de mãos dadas. Eles estiveram comigo nas dificuldades e vibraram com as minhas vitórias. Obrigada!

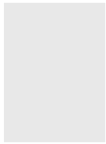
Aos demais professores do PPGD que estiveram comigo nesses anos e me permitiram crescer. Ajudaram na reformulação de pensamentos tornando-os mais maduros. Aprendizados que abrem os horizontes. Formidável! Como dizia Paulo Freire, “Educação não transforma o mundo, educação muda as pessoas. Pessoas transformam o mundo”. A vocês meus agradecimentos.

Aos Programas de Pós-graduação da Universidade Católica de Pernambuco e da *Università di Pisa* dos quais tenho muito orgulho de ter sido aluna e muita gratidão. Estudar em Universidades tão importantes e prestigiadas não apenas me traz satisfação, e sim, me deixa honrada em fazer parte delas.

À CAPES, da qual fui bolsista para estudar na Universidade Católica de Pernambuco e fui bolsista através do programa de incentivo à pesquisa no país e no exterior, quanto para o Doutorado sanduiche na Itália. Instituição que me oportunizou estudar, desenvolver pesquisa de qualidade para oferecer a sociedade um retorno estruturado, alimentando a ciência que é a fonte da transformação social.

À Estácio Recife, aos amigos de trabalho e todos que a compõem, por me apoiarem na decisão de me afastar das atividades de sala de aula como professora para o período na Itália, sem perder o laço que, com meu retorno, me permite dar continuidade com a docência. Obrigada pela torcida e pelo incentivo.

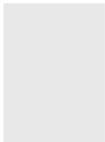
À cidade de Pisa que me acolheu por incríveis 6 meses e onde pude conhecer mais de perto e com detalhes a história, cultura e beleza que ela tem. Deixei alguns amigos que me saudaram com um até breve. E, assim, em breve voltarei. Foram dias muito felizes que me preencheram de boas energias tornando tudo mais leve. Seguramente não foi apenas uma experiência acadêmica, mas uma oportunidade de transformação pessoal. Volto outra Aline. Obrigada a todos que me ajudaram para que isso acontecesse e às amigas que pude encontrar.



Guardarei as melhores recordações de Pisa e de cada cantinho que passei na Itália e nos outros países que pude visitar.

A cada um que cruzou pelo meu caminho, seja por alguns minutos, por um dia ou por meses e anos, obrigada por fazerem parte da minha vida. Obrigada por quem torceu, quem vibrou, enviou pensamentos e energias positivas! Deu certo!

Entre altos e baixos, dias corridos outros lentos, entre doenças e saúde, finalizo esse momento com muito orgulho e agradecida. Pronta para os próximos capítulos dessa vida boa de se viver!

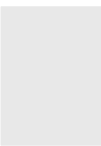


Resumo

O presente trabalho de pesquisa, requisito para conclusão do doutorado, se propôs a desenvolver um estudo acerca da adequação do judiciário à regulamentação de proteção de dados no Brasil e na Itália no que tange a realização de audiências por videoconferência. Para isso, iniciou-se a análise a partir do ponto em comum entre os dois países: o regulamento europeu - GDPR. O exame sobre essa regra se deu a partir da consideração da posição europeia exercendo influência em vários países, assim como aconteceu com o Brasil. A regulamentação brasileira utilizou como paradigma o regulamento europeu sobre proteção de dados. Desse modo, tornou-se significativo estudar o protagonismo europeu, bem como o desenvolvimento do GDPR e o entendimento sobre princípio da transparência e privacidade. Depois, debruçou-se sobre o desenvolvimento normativo na Itália, como um país pertencente à União Europeia, e sobre o Brasil no que diz respeito às regras processuais judiciais e proteção de dados para identificar a conformidade com o regramento geral. Por fim, o trabalho se propôs a analisar relatórios de acesso público sobre como vem ocorrendo a adequação do judiciário ao regulamento de proteção de dados em cada um dos tribunais selecionados, bem como se teve iniciativa de elaborar um questionário direcionado a dois tribunais com perguntas baseadas no estudo das legislações, sendo um italiano e um brasileiro, para compreender a rotina na realização das audiências por videoconferência nos tribunais referenciados aqui. E, diante da análise, foram feitas considerações sobre os desafios e vulnerabilidades que os dados pessoais coletados nas audiências remotas ficam sujeitos frente a internet e a sociedade hiperconectada. Para a pesquisa foram utilizadas bibliografias nacionais e estrangeiras, bem como documentos de acesso público. O objetivo foi responder à pergunta: A Itália e o Brasil estão adequados às suas respectivas regulamentações sobre proteção de dados no que tange a realização de audiência por videoconferência?

A pesquisa trouxe a hipótese de estarem adequados, entretanto, identificou-se que os relatórios não trazem detalhes sobre o cotidiano judiciário e não se obteve resposta aos questionários, impossibilitando compreender como são praticados os atos durante a realização das audiências remotas.

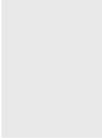
Palavras-chave: Privacidade; GDPR; LGPD; audiência videoconferência.



Abstract

This research paper, a requirement for the completion of the doctoral degree, aimed to develop a study on the adequacy of the judiciary to data protection regulations in Brazil and Italy concerning the conduct of hearings via videoconference. To achieve this, the analysis began with a common point between the two countries: the European Regulation - GDPR. The examination of this regulation considered the European position's influence on various countries, as happened with Brazil. The Brazilian regulation used the European data protection regulation as a paradigm. Thus, it became significant to study the European leadership, as well as the development of the GDPR and the understanding of the principles of transparency and privacy. Subsequently, the study focused on the normative development in Italy, as a member state of the European Union, and in Brazil regarding procedural judicial rules and data protection to identify compliance with the general regulation. Finally, the paper aimed to analyze public access reports on how the judiciary has been adapting to data protection regulations in each of the selected courts, as well as to create a questionnaire directed at two courts, one Italian and one Brazilian, with questions based on the study of the legislation, to understand the routine in conducting videoconference hearings in the referenced courts. The analysis led to considerations about the challenges and vulnerabilities that personal data collected during remote hearings face in the context of the internet and the hyper-connected society. The research utilized national and international bibliographies, as well as public access documents. The objective was to answer the question: Are Italy and Brazil in line with their respective data protection regulations when it comes to holding hearings by videoconference? The research hypothesized compliance; however, it was found that the reports did not provide details on judicial routines, and there was no response to the questionnaires, making it impossible to understand how acts are performed during remote hearings.

Keywords: Privacy; GDPR; LGPD; videoconference hearings



Resumo

Il presente lavoro di ricerca, requisito necessario per il conseguimento del dottorato, si proponeva di sviluppare uno studio sull'adeguatezza della magistratura alle normative sulla protezione dei dati in Brasile e in Italia per quanto riguarda lo svolgimento di udienze in videoconferenza. Per fare ciò, l'analisi è partita dal punto in comune tra i due Paesi: il regolamento europeo - GDPR. L'esame di questa norma si è basato sulla considerazione che la posizione europea esercita un'influenza in diversi Paesi, proprio come in Brasile. Le normative brasiliane hanno utilizzato il regolamento europeo sulla protezione dei dati come paradigma. È stato quindi importante studiare il ruolo europeo, nonché lo sviluppo del GDPR e la comprensione del principio di trasparenza e privacy. Si è quindi esaminato lo sviluppo normativo in Italia, in quanto Paese appartenente all'Unione Europea, e in Brasile per quanto riguarda le norme procedurali giudiziarie e la protezione dei dati, per individuare la conformità con le norme generali. Infine, il lavoro si è proposto di analizzare le relazioni pubblicamente disponibili su come il sistema giudiziario si è adattato alla normativa sulla protezione dei dati in ciascuno dei tribunali selezionati, nonché di sviluppare un questionario per due tribunali con domande basate sullo studio della legislazione, uno italiano e uno brasiliano, al fine di comprendere la routine dello svolgimento di udienze in videoconferenza nei tribunali qui citati. Alla luce dell'analisi, sono state fatte considerazioni sulle sfide e le vulnerabilità a cui sono soggetti i dati personali raccolti nelle udienze a distanza di fronte a Internet e alla società iperconnessa. La ricerca si è avvalsa di bibliografie nazionali ed estere, nonché di documenti pubblicamente accessibili. L'obiettivo era quello di rispondere alla domanda: L'Italia e il Brasile sono in linea con le rispettive normative sulla protezione dei dati quando si tratta di tenere udienze in videoconferenza? La ricerca ha ipotizzato che siano adeguate; tuttavia, è emerso che le relazioni non forniscono dettagli sulla gestione quotidiana del sistema giudiziario e non sono state ricevute risposte ai questionari, rendendo impossibile capire come vengono svolti gli atti durante le udienze a distanza.

Parole chiave: Privacy; GDPR; LGPD; audizioni in videoconferenza.

SUMÁRIO

INTRODUÇÃO.....	14
1 A UNIÃO EUROPEIA COMO <i>MODELADOR DE NORMAS</i> EM MATÉRIA DE PROTEÇÃO DE DADOS.....	19
1.1 ASPECTOS GERAIS.....	19
1.2 DESENVOLVIMENTO CRONOLÓGICO DO GENERAL DATA PROTECTION REGULATION – GDPR E ALGUMAS CONSIDERAÇÕES SOBRE ESTE REGULAMENTO.....	34
1.3 PRINCÍPIO DA PRIVACIDADE E TRANSPARÊNCIA: VISÃO DA UNIÃO EUROPEIA	46
2 REGULAMENTAÇÕES E NORMATIVAS REFERENTES À PRIVACIDADE E PROTEÇÃO DE DADOS A PARTIR DO GDPR E DA LGPD PELA ITÁLIA E BRASIL	58
2.1 ASPECTOS GERAIS	58
2.2 REGULAMENTAÇÕES APÓS VIGÊNCIA DO GDPR DETERMINADAS PELO MINISTERO DELLA GIUSTIZIA NA ITÁLIA PARA O PODER JUDICIÁRIO QUANTO À PROTEÇÃO DE DADOS DURANTE OS PROCEDIMENTOS JUDICIAIS	70
2.3 REGULAMENTAÇÕES APÓS A VIGÊNCIA DA LGPD DETERMINADAS PELO CONSELHO NACIONAL DE JUSTIÇA NO BRASIL PARA O PODER JUDICIÁRIO QUANTO À PROTEÇÃO DE DADOS DURANTE OS PROCEDIMENTOS JUDICIAIS.....	81
3 IMPORTÂNCIA DO ACOMPANHAMENTO DA ADEQUAÇÃO DO JUDICIÁRIO ÀS LEIS DE PROTEÇÃO DE DADOS E A VULNERABILIDADE DESSE DIREITO	96
3.1 ASPECTOS GERAIS	96
3.2 EXISTÊNCIA DE ACOMPANHAMENTO NO BRASIL E ITÁLIA SOBRE O PODER JUDICIÁRIO E A ADEQUAÇÃO ÀS REGULAMENTAÇÕES SOBRE PROTEÇÃO DE DADOS PESSOAIS (RELATÓRIO E OFÍCIO AO TRIBUNAL.....)	102
3.3 PROSPECTIVAS SOBRE A VULNERABILIDADE DE DADOS PESSOAIS NA SOCIEDADE DA INFORMAÇÃO	140
CONSIDERAÇÕES FINAIS.....	163
REFERÊNCIAS BIBLIOGRÁFICAS.....	ERRO! INDICADOR NÃO DEFINIDO.
REFERÊNCIAS.....	173
ANEXOS.....	187

INTRODUÇÃO

A proposta de pesquisa no presente trabalho é de desenvolver um estudo voltado para a temática de proteção de dados pessoais no âmbito processual judicial, especificamente durante a realização de audiências por videoconferência. Dessa forma, a pesquisa segue uma perspectiva direcionada para um estudo sobre os ordenamentos jurídicos da Itália e do Brasil no que diz respeito a análise normativa e a coleta de dados pessoais durante a realização da audiência remota.

Assim, o estudo segue um olhar do uso das tecnologias e da internet e é conduzido fazendo um recorte da análise entre esses dois países. Esse exame secundário se dá sobre o aspecto normativo de cada uma das nações no que diz respeito a proteção de dados e regulamentações processuais de forma digital.

Considerando a atualidade imersa em um mundo tecnológico e digitalizado, torna o objeto de pesquisa de fundamental importância a nível nacional e internacional. E, aqui, propõe-se a abordar o Brasil e a Itália, delimitando-se a Recife, Pernambuco e Pisa, esclarecendo que a magnitude do assunto permite a extensão para outras nações que ainda não estão sendo desenvolvidas nesse trabalho.

Por questões metodológicas, o debate se limita sobre os dois países como recorte explorando e discorrendo sobre o assunto proposto. O trabalho visa a estudar a existência das normas protetivas dos dados pessoais e o referido cumprimento pelo judiciário durante a realização de atos processuais de forma virtual.

É preciso compreender que a pauta da pesquisa sobre proteção de dados foge de limites geográficos. Assim, inicia-se o trabalho com o capítulo que aborda a liderança no aspecto normativo da União Europeia, exercendo um papel de modelo para demais países não membros da UE.

Isso porque, o Regulamento Europeu tem ocupado um espaço internacional de influência, aqui intitulada de *Modelador de Normas (Norm-Shaper)*. Nesse diapasão, o início do trabalho debate a visão europeia sobre proteção de dados, demonstrando o nascimento do *General Data Protection Regulation*, buscando apontar o regramento e a perspectiva sobre direitos humanos.

O propósito é partir de um ponto em comum que é o regulamento europeu, tendo em vista seu protagonismo servindo de espelho no cenário internacional. Depois, faz-se o estudo sobre as legislações de proteção de dados sobre o Brasil e a Itália, analisando o contexto do surgimento dos regulamentos gerais e as consequências normativas a respeito da proteção de dados em processos judiciais.

Dessa forma, no primeiro capítulo analisa-se a posição da União Europeia de relevância, demonstrando uma tendência normativa utilizada como modelo em vários âmbitos jurídicos, tal como acontece com direito ambiental, e, agora, com proteção de dados. É, nesse diapasão, significativo estudar o protagonismo europeu para melhor compreensão sobre sua expansão e o seu desenvolvimento normativo sobre proteção de dados.

Dentre tantos braços sociais e considerando a importância de todos eles, a preocupação aqui se dá pela necessidade de análise e estudo constante sobre a efetividade das normas que regulamentam o direito a proteção de dados. São inúmeras áreas de atividades que incide essa norma, mas a pesquisa delimitou-se a estudar sobre a coleta, tratamento e armazenamento de dados durante as audiências por videoconferência, conforme será visto nos capítulos seguintes.

Assim, após estudo sobre a posição de *Modelador de Normas* da União Europeia no início do primeiro capítulo, o tópico 1.1 busca-se analisar todo o desenvolvimento legislativo sobre proteção de dados até chegar ao *General Data Protection Regulation*. Para isso, partiu-se da fundamentação do destaque internacional da União Europeia no intuito de compreender como foi formulado o direito à proteção de dados na Europa.

O estudo realizado sobre a construção normativa do GDPR tem como ideal demonstrar como se deu a formação desse Regulamento e qual o significado no cenário interno, antes da entrada em vigor e após. Nesse sentido, visa-se também demonstrar como se construiu o entendimento sobre o direito fundamental e a sua relevância no cenário das relações internacionais citando alguns exemplos em que se fez presente o debate sobre proteção de dados.

Assim, o capítulo traz um debate sobre negociações internacionais e o respeito aos direitos dos cidadãos europeus. A União Europeia, em suas tratativas internacionais, busca levar em consideração como os países envolvidos protegem os dados pessoais dos cidadãos para a realização das atividades a que se propõem no acordo que vier a ser firmado.

Na sequência, foram analisados os princípios da transparência e privacidade, no que tange a visão europeia contextualizando com a temática proposta no trabalho. A reflexão tem importância porque traz os desafios para lidar com o cumprimento normativo, nos dois no sistema jurídico. No segundo sub tópico estuda-se o direito fundamental a proteção de dados e a garantia dos princípios processuais, citando aqui o da publicidade processual, ressalvados os de segredo de justiça.

Portanto, o capítulo 1 traz uma análise do cenário internacional com o protagonismo da União Europeia sobre a matéria de proteção de dados. O objetivo é demonstrar a visão europeia sobre o assunto, sinalizando a sua influência nas demais nações. Dessa forma, trata-se de um capítulo norteador da pesquisa aqui desenvolvida.

Nesse diapasão, o segundo capítulo busca abordar as normativas de um país europeu, aqui delimitando-se à Itália, bem como as do Brasil. A proposta é estudar as regras que se antecedem e sucedem a vigência dos seus respectivos regulamentos no que diz respeito a proteção de dados no âmbito processual. Dedica-se estudar especificamente ao que diz respeito aos regramentos quanto ao uso da tecnologia para realização dos atos processuais.

O intuito desse capítulo é compreender como cada país se encontrava legislativamente antes da vigência do regulamento geral e como se comportou após, no âmbito jurídico processual quando da necessidade de adequação à lei de proteção de dados. O intuito é compreender se os ordenamentos apresentam arcabouço normativo adequado às exigências dos regulamentos vigentes no que diz respeito à realização de audiências remotas, analisando-o.

Considerando que o GDPR e a LGPD trazem regramentos gerais, como a própria nomenclatura se apresenta, no que diz respeito ao judiciário, identifica-se a necessidade da existência de outras regras, instruções para que o órgão judicial de cada país se encontre adequado ao seu regulamento geral. Assim, investiga-se se o Poder Judiciário está pautado em regras em conformidade com a regulação de proteção de dados, para, posteriormente, a pesquisa se enveredar para análise do cotidiano das audiências por videoconferência.

A eleição da Itália para recorte da pesquisa se dá pelo fato de ser o país com sistema processual semelhante ao do Brasil. Concebendo que este último considerou como base para sua própria formação legal a lei processual italiana e, agora, o regulamento europeu, é importante saber como cada um desses países se comportam frente às novas exigências legais.

O direito italiano e o direito brasileiro têm muito em comum, nos mais variados pontos. O Brasil se inspirou em diversas normas do direito italiano para a estrutura de

seu ordenamento jurídico. Com o direito processual civil não foi diferente, havendo uma grande influência do processo civil italiano no brasileiro. Dentre tantos institutos italianos que serviram de exemplo para o direito brasileiro, tem-se o relativo à tutela cautelar, amplamente adotado no Código de Processo Civil de 1973, e que teve diversas mudanças quando do advento do atual diploma processual, em 2015.

(...)Há muitas semelhanças entre os institutos italiano e brasileiro, e com a mesma finalidade, qual seja, assegurar que o processo seja efetivo e que, quando do provimento final, realmente a parte requerente possa usufruir de seu direito, desde que devidamente comprovado¹.

Dessa forma, o panorama italiano traz contribuições sobre privacidade, demonstrando antecipação sobre regulamentação de proteção de dados. Isso porque apresenta o Código de Proteção de Dados e outras regulamentações associadas a essa temática. Apesar de outros países já terem abordado proteção de dados e privacidade com outros tipos normativos, a Itália inaugura um código sobre a matéria.

O Brasil, por sua vez, apresenta normativas que envolvem proteção de dados antes do surgimento da regulamentação específica. Marco Civil da Internet, Código de Defesa do Consumidor e a própria Constituição Federal. Após o regulamento, tem-se resoluções e orientações em matéria processual para que o judiciário se adeque às exigências da Lei Geral de Proteção de Dados. O capítulo segundo tratará da análise dessas normas, buscando identificar a relação com a LGPD e buscando identificar o recorte sobre a existência de regulamentações na área processual, em específico sobre audiências remotas.

Destarte, o segundo capítulo analisa o ordenamento de cada um dos países aqui elencados e suas nuances antes e depois dos regulamentos. O estudo é sobre a compreensão acerca das exigências legais de cada regulamento de proteção de dados e sobre a existência de regras sobre atos processuais em geral e as de audiências por videoconferência e a conformidade com as leis de proteção de dados.

Por consequência, no capítulo seguinte, faz-se o estudo sobre o funcionamento do judiciário a partir da prática cotidiana judicial. O estudo é voltado para a pesquisa sobre a existência de relatórios de acesso público que contenham informações sobre as atividades do judiciário e a sua respectiva correlação com os preceitos legais.

¹ CASTRO, Aldo Aranha de. A busca pela efetividade do acesso à justiça por meio da tutela provisória no direito processual civil brasileiro e da tutela cautelar no sistema italiano. I Encontro Virtual do CNPEDI. Acesso à Justiça I. Coordenadores: Juvêncio Borges Silva e Luiz Fernando Bellinetti. Florianópolis, 2020. Disponível em: <http://site.conpedi.org.br/publicacoes/olpbq8u9/ag5bl345/6YJcO6R9Pr32Q7fz.pdf> . Acesso em 14 out 2024. p. 198-199.

Isto posto, o capítulo 3 se propõe a investigar a atividade do judiciário, tanto através do envio de questionário aos tribunais como averiguar se há acompanhamento através de relatórios. O objetivo é confirmar a hipótese de adequação aos requisitos legais sobre o direito de proteção de dados no processo judicial, especialmente sobre a realização de audiências por videoconferência. Assim, visa-se analisar se há o rastreamento das atividades judiciais e a amostra coletada de questionário feita com o Tribunal de Justiça do Estado de Pernambuco e *Tribunale di Pisa*.

Dessa forma, o estudo sobre os relatórios disponibilizados pelos órgãos responsáveis pelo acompanhamento do judiciário podem apresentar informações sobre o desempenho, podendo conter os procedimentos de cada tribunal sobre o tratamento dos dados pessoais coletados em audiências remotas. A análise dessas informações serve para fomentar o debate investigando as necessidades contemporâneas que forem imediatamente identificadas a partir dos relatórios, bem como das respostas dos questionários.

Importante observar que o presente trabalho não tem o intuito de generalizar compreensão sobre os resultados obtidos e analisados. Isso porque, para uma visão ampla sobre o funcionamento de todo o judiciário, a pesquisa precisaria ser desenvolvida em mais de um tribunal e em outras cidades. O objetivo é identificar as lacunas e, a partir delas, permitir a discussão à luz do direito vigente.

Além disso, é pertinente afirmar que os questionários foram elaborados com indagações pautadas em conformidade com as exigências legais. São perguntas sobre o cotidiano judiciário, e que se encontram em anexo a esse trabalho, para analisar as condutas e atos processuais durante a realização de audiência por videoconferência em matéria de proteção de dados.

Apesar de as informações não retratarem todos os tribunais, os dados revelam uma realidade com importância significativa para pesquisa. Sinalizam o que pode ser aprofundado para melhoramento das atividades judiciais, ao menos no espaço estudado. Assim, o trabalho traz dados que permitem desenvolver estudos posteriores, direcionando pesquisas e planejamentos para que as instituições se aprimorem e estejam sempre o mais próximo do que preceitua a lei.

Portanto, o tópico 3.2 tem o propósito de analisar a instituição na realização de suas atividades de prestação jurisdicional, especificamente sobre as condutas dos serventuários durante a realização das audiências por videoconferência e a proteção de dados pessoais coletados durante esse ato.

Na sequência, a partir do que foi construído no decorrer da pesquisa, o último tópico que encerra o trabalho traz reflexões considerando a atualidade do ciberespaço, vulnerabilidade de direito a proteção de dados pessoais e a necessidade de constante aperfeiçoamento. Esse último ponto tem um posicionamento acerca de uma visão ampla sobre proteção de dados. Para isso, traz conceitos e teorias de estudiosos sobre tecnologia e sociedade.

Dessa forma, a pesquisa busca responder sobre o seguinte questionamento: A Itália e o Brasil estão adequados às suas respectivas regulamentações sobre proteção de dados no que tange a realização de audiência por videoconferência? A hipótese investigada é de que estão adequados.

Assim, para o desenvolvimento da pesquisa foi utilizada vasta doutrina que fundamenta os conceitos e ideias sobre o tema proposto fazendo a correlação com a proposta de pesquisa, bem como, busca-se análise de dados empíricos específicos (relatórios e resposta de questionário) com o intuito de fomentar o debate.

Isto posto, o presente trabalho não se propõe a exaurir o estudo, compreendendo sua magnitude. Busca contribuir acadêmica e socialmente para o desenvolvimento de uma melhor prestação jurisdicional e efetividade na proteção dos dados pessoais no âmbito do judiciário em todo o sistema processual, incluindo na realização das audiências por videoconferência.

A união europeia como *modelador de normas* em matéria de proteção de dados

Aspectos gerais

A proposta é de iniciar o trabalho analisando o papel da União Europeia frente a outras nações no que diz respeito a matéria de proteção de dados. Isso se justifica, nessa pesquisa, pela influência normativa do Regulamento que vem servindo como modelo sobre o assunto para vários países, e aqui se especificará o Brasil.

Neste primeiro momento, o estudo é voltado para o protagonismo europeu como algo marcante em outras matérias jurídicas de interesse comum às nações, como direito ambiental, com intuito de exemplificação desse destaque europeu no cenário mundial.

Depois, o olhar será direcionado a observar a origem e o fundamento da proteção de dados, analisando conceitos associados ao assunto, como o de privacidade, e a perspectiva do cenário entre outros países de forma exemplificativa. Aqui, em especial, abordar-se-á o regulamento europeu na Itália e a influência voluntária refletida no Brasil, servindo de base para o desenvolvimento dos próximos capítulos.

A delimitação entre os Estados eleitos se dá por questão de recorte metodológico, ainda que se reconheça ser matéria abrangente e que ultrapassa os limites geográficos, sendo tema comum a todos os países, haja vista que os dados estão inseridos no espaço virtual. Assim, o trabalho foca a abordagem nos dois países acima indicados, bem como, delimita, no decorrer da pesquisa, a matéria processual judiciária e direciona o estudo em específico para os atos judiciais virtuais.

Esse estudo permite ter uma compreensão de como cada país apresenta quanto à conformidade ao seu regulamento e suas normas internas. A análise leva em consideração que as regras partiram de um mesmo ponto, qual seja, o Regulamento Europeu, que criou princípios e regras com tendência mundial. Assim, tanto as normas italianas, quanto a LGPD seguiram as diretrizes do GDPR.

Em se tratando do Brasil, compreende-se que a norma europeia serviu de base, norteando a criação da regulamentação brasileira, entretanto, não se busca afirmar que caberá a este país seguir norma estrangeira, pois não há relação de subordinação entre Brasil e União Europeia. Todavia, é importante observar que houve a inspiração no regulamento europeu servindo de modelo para outros Estados na elaboração de sua norma sobre proteção de dados pessoais.

Assim, a abordagem metodológica, portanto, é a de analisar o tema a partir de um ponto em comum, regulamento europeu como modelo, como *modelador de normas*. Depois, o estudo é feito a partir dos desdobramentos normativos de cada ente soberano, um pertencente e outro não pertencente a UE que serão estudados nos seguintes capítulos, no que diz respeito a proteção de dados.

Ainda é importante contextualizar o trabalho a partir desse painel de globalização. Observa-se constante dinamicidade em todos os campos sociais, com uma permanente troca de informações, ideais, perspectivas, discussões políticas, econômicas, dentre outros temas e interesses compartilhados e, principalmente, atrelados ao uso das tecnologias.

Nesse interim, considerando que a pesquisa nesse capítulo é voltada para a problemática encontrada no momento da realização de audiências por videoconferência, a respeito do papel do judiciário quanto ao tratamento dos dados pessoais e adequação às suas respectivas

normativas, o trabalho parte do referencial para posteriormente poder abordar as especificidades de cada país. Essa delimitação de pesquisa permitirá compreender se há a conformidade do judiciário a sua normativa nacional quando em atividade de audiência por videoconferência.

Estabelecido o ponto acima referenciado cria-se, então, a conexão com os demais capítulos do trabalho, direcionando-se, na sequência, para o arcabouço normativo de cada país. Dessa forma, a Itália será analisada sobre o aspecto da sua conformidade com o regulamento europeu, assim como o Brasil será analisado a partir da sua conformidade com a legislação brasileira sobre a matéria de proteção de dados durante a realização de audiências remotas.

Considerando que a União Europeia é composta por vários países, importante destacar que a escolha da Itália, dentre os demais, se dá, primeiro, pelo fato desse ser um país pertencente à Organização. Com isso, permite-se compreender se há o cumprimento das exigências prescritas no regulamento, bem como analisa-se o atendimento às leis nacionais. Depois, pelo fato de haver semelhança entre os sistemas jurídicos.

Além disso, importante frisar que a Itália é a origem, o berço do direito processual, e serviu de espelho para as regras processuais brasileiras. E, por último, outro destaque é que a Itália se antecedeu ao regulamento europeu, quando formulou o Código de proteção de dados, que será abordado no capítulo seguinte.

Dessa forma se justifica analisar o destaque da organização europeia, aqui denominada de *Modeladora de Normas* (em inglês, *Norm-Shaper*), tanto em relação ao aspecto normativo, como o principiológico. Trata-se de um posicionamento que se replica em outras nações principalmente considerando o modelo de sociedade atual, o da informação. É isso que se quer dizer quando se intitula *Modeladora de Normas* ou *Norm-Shaper*, tornando-se tendência ou modelo a ser seguido em outros países do globo.

Nesse entendimento, é notório o papel da União Europeia em diversas matérias, tais como economia, política, proteção ambiental², dentre outras. Importa afirmar que a União ocupa um papel significativo a nível global sendo modelo normativo para outras nações, que ao elaborarem suas normativas internas, em muitas ocasiões utilizam regulamentos europeus e outras produções normativas desse grupo como fontes inspiradoras para seus textos.

A professora Tarim explica o protagonismo da UE em matéria climática, definindo-a como *Norm-Shaper*:

Diante da atual emergência climática e de tantos outros problemas oriundos da nova Era do Antropoceno, a União Europeia (UE) tem despontado como uma influenciadora mundial de decisões, uma norm shaper, tanto no seio da União quanto

² MONT'ALVERNE, Tarin Cristino Frota; LIMA, Maria Cecília Girão Veras. The European Union as a Norm Shaper on Biodiversity Protection. **Vereadas do Direito**, v. 20, p. e202569, 2023.

no cenário internacional. Trata-se de um fenômeno que se repete nas mais diversas áreas, como o comércio internacional, porém ganha especial destaque na seara ambiental com seus desafios transfronteiriços³.

Vogler e Stephan, citados por Lima e Matias, sinalizam o mesmo entendimento sobre o protagonismo Norm-Shaper:

Existe uma base estrutural para a influência da UE como uma norm shaper, a qual pode ser vista com sua participação ativa no sistema internacional. Essa capacidade de estar presente nas mais diversas searas exerce atração sobre estrangeiros, em particular seus parceiros comerciais, criando expectativas sobre como a UE irá se posicionar, como agir, reforçando que as posições do bloco em fóruns multilaterais sejam seguidas por outros Estados⁴.

Nesse mesmo diapasão e observando a diversidade de influências europeias espelhadas pelo mundo, a UE não se comporta diferente no que diz respeito ao tema de proteção de dados e privacidade. Trata-se de tema que a Europa tem reconhecimento, pois trouxe debates que foram e são relevantes, propagando-se em outros Estados, inclusive em negociações internacionais.

O estudo sobre o GDPR e seu protagonismo fundamentará o restante do trabalho que tem como escopo responder o questionamento sobre adequação da Itália e o Brasil às suas respectivas regulamentações sobre proteção de dados no que tange a realização de audiência por videoconferência.

Relacionado a esse contexto, é importante mencionar que existe o intuito ou interesse de se estabelecer um padrão global de privacidade de dados e o GDPR, de fato, criou uma espécie de padrão a partir de 25 de maio de 2018, quando entrou em vigor. E, nessa linha, mencione-se a Convenção 108 e a Convenção 108+ que foram moldadas a partir dos padrões europeus e recebem adesão dos países (não membros da UE) que estiverem em conformidade com o modelo de privacidade que se almeja na convenção⁵. Trata-se de mais um exemplo de liderança europeia frente ao cenário mundial.

³ IBIDEM.

⁴ VOGLER, John; STEPHAN, Hannes R. The European Union in global environmental governance: leadership in the making?. *International Environmental Agreements: Politics, Law and Economics*, [Utrecht, The Netherlands], v. 7, n. 4, p. 389-413, 2007, APUD LIMA, Maria Cecília Girão Veras; MATIAS, João Luís Nogueira. Os efeitos extraterritoriais do regulamento antidesmatamento da União Europeia no Brasil. **Revista CEJ, Brasília, Ano XXVII**, n. 85, p. 47-54, 2023. Disponível em: <file:///C:/Users/Aline/Downloads/2791-Texto%20do%20artigo-7770-1-10-20231116.pdf>. Acesso em: 14 out 2024.

⁵ GREENLEAF, Graham. Global Data Privacy Laws 2023: International standards stall, but UK disruptst. 2023. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4530145, acesso em 14 mar 2024.

Observe-se que os países que fazem o 108+ (atualmente são 55 países⁶) estão seguindo um mesmo raciocínio quanto ao tema de proteção de dados. Nesse sentido, trata-se de uma tentativa de convencionar o padrão mundial em matéria de privacidade e proteção de dados que está associado ao Regulamento Europeu. Porém, ainda inicial, haja vista o número de países signatários.

Para exemplificar as influências das regras europeias como modelos a serem seguidos, pode-se dizer que o Japão e Coreia são países, que ao elaborarem suas normativas, utilizaram como exemplo o regulatório europeu como referência. Entende-se que seguir o padrão europeu traz o benefício de proporcionar boas relações internacionais entre países pertencentes e não pertencentes a UE, pois são nações que demonstram corroborar com o mesmo entendimento sobre a matéria de privacidade⁷.

Pode-se aduzir, portanto, que o país que demonstra compreender a matéria utilizando os mesmos princípios e apresentando leis semelhantes ao GDPR, comprovam afinidade no que tange a preocupação com a segurança e circulação de dados, podendo proporcionar, desse modo, as boas relações internacionais. Essa consonância de entendimento reflete em vários âmbitos, como as negociações comerciais, pois para essa prática há a necessidade de conformidade legislativa e afinidade normativa para viabilizar as transações⁸. Do contrário, se torna difícil que países com compreensões diferentes possam estabelecer negociações comerciais, por exemplo.

Mesmo reconhecendo e afirmando o importante papel exercido pela União Europeia quanto a propagação dos ideais de privacidade e proteção de dados, é importante mencionar que, como explicam Bioni e Rielli⁹, os Estados Unidos foram os pioneiros quanto a criação principiológica de proteção de dados, que serviu de base para tudo que se tem hoje no que diz respeito às leis de proteção de dados pelo mundo. Entretanto, não alcançaram a propagação que a UE abrangeu quanto a influências para outras culturas.

⁶ COUNCIL OF EUROPE. Data Protection. Parties. Disponível em: <https://www.coe.int/en/web/data-protection/convention108/parties>. Acesso em 24 jun 2024.

⁷ GREENLEAF, Graham. Global Data Privacy Laws 2023: International standards stall, but UK disrupt. 2023. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4530145, acesso em 14 mar 2024.

⁸ GREENLEAF, Graham. Global Data Privacy Laws 2023: International standards stall, but UK disrupt. 2023. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4530145, acesso em 14 mar 2024.

⁹ BIONI, Bruno Ricardo. RIELLI, Mariana. Data Privacy Brasil. Comissão Mista da Medida Provisória nº. 869, de 2018 Segunda Audiência Pública. Tema: Tratamento de dados pela Administração Pública e Proteção de Dados relativos à defesa e segurança pública. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento/download/01cdc9cc-4e64-4a40-a32b-cbad84777b05>, acesso em 14 mar 2024.

Os EUA deram início ao entendimento sobre o que seria privacidade, dando a conotação de ser “o direito de ser deixado só”. Uma compreensão ainda em seu princípio, pois ao longo do tempo foi-se ampliando o que se entende por privacidade, que vai além do “deixar só”. Por esse motivo, cita-se essa reconhecida expressão criada nos EUA.

Entretanto, fundamentando o que se vem falando nesse trabalho de pesquisa, ambos professores afirmam que a propagação transnacional se deu a partir da Organização Europeia para Desenvolvimento Socioeconômico. A partir de então, o Conselho da Europa criou regras considerando os princípios formulados pelos Estados Unidos, todavia formulando seu próprio regramento sobre proteção de dados.

Nesse mesmo interim, não se pode deixar de falar sobre a Alemanha, que também na década de 70, preocupada com a proteção dos dados dos seus cidadãos, após o que se vivenciou no período nazista, bem como atenta aos avanços da computação, criou as primeiras normas regulatórias, dando origem a norma em 1978¹⁰.

De toda maneira, a respeito da posição Europeia como modelo normativo para demais nações, Bradford explica o *The Brussels Effect*. O sentido do trabalho desenvolvido por ela é de mostrar o poder unilateral da Europa para regular os mercados globais. Em seu estudo, explica a busca por uma globalização regulatória política, assim entendida como cooperativa em vez de globalização regulatória unilateral, nesse último sendo por impulso de mercado.

Contrary to this prevalent perception, this Article highlights a deeply underestimated aspect of European power that the discussion on globalization and power politics overlooks: Europe's unilateral power to regulate global markets. The European Union sets the global rules across a range of areas, such as food, chemicals, competition, and the protection of privacy.

This Article has highlighted the unprecedented global power that the EU is exercising through its legal institutions and standards that it successfully exports to the rest of the world via the Brussels Effect. Without resorting to international institutions or seeking other nations' cooperation, the EU is able to promulgate regulations that become entrenched in the legal frameworks of developed and developing markets alike, leading to the “Europeanization” of important aspects of global commerce¹¹¹².

¹⁰ LGPD/DF. Disponível em: <https://lgpd.df.gov.br/historico/>. Acesso em 16 mar 2024.

¹¹ BRADFORD, Anu. *The Brussels Effect*, Northwestern University Law Review, Vol. 107, p. 1, 2012; Columbia Law & Economics Working Paper No. 533 (2012). Available at: https://scholarship.law.columbia.edu/faculty_scholarship/1966. Acesso em: 24 jun 2024.

¹² Tradução livre: Contrariamente a esta percepção predominante, este artigo destaca um aspecto profundamente subestimado do poder europeu que a discussão sobre a globalização e a política de poder ignora: o poder unilateral da Europa para regular os mercados globais. A União Europeia estabelece as regras globais numa série de áreas, como a alimentação, os produtos químicos, a concorrência e a proteção da privacidade.

Este artigo destacou o poder global sem precedentes que a UE está a exercer através das suas instituições e normas jurídicas que exporta com sucesso para o resto do mundo através do Efeito Bruxelas. Sem recorrer a instituições internacionais ou procurar a cooperação de outras nações, a UE é capaz de promulgar regulamentos que se enraízam nos quadros jurídicos dos mercados desenvolvidos e em desenvolvimento, conduzindo à “europeização” de aspectos importantes do comércio global.

Importante salientar que o aspecto econômico é um elemento significativo no cenário global e entre as nações. Nesse sentido, o Regulamento da UE acaba sendo uma condicional implícita a ser cumprida pelos entes envolvidos nas negociações internacionais. Bradford explica:

Strict domestic regulations can operate as global standards only if such strict regulations cannot be circumvented by moving the regulatory targets to another jurisdiction. In other words, a state's ability to override another state's preference for lenient standards is compromised if the target can escape the strict regulation by simply relocating. This is the dynamic that triggers races to the bottom as producers seek less constraining regulatory environments. The EU avoids this circumvention of its standards by primarily regulating consumer markets, such as product or food safety. Unlike a regulatory target such as capital, which is more mobile, consumers rarely move to another jurisdiction in response to strict regulatory standards. Thus, as long as a firm willing to trade within the EU wants access to its 500 million consumers, it needs to comply with the EU's consumer protection regulations. These consumers cannot be moved to a jurisdiction where lesser protections govern what products can be sold to them¹³.

Entretanto, mesmo considerando a relevância da economia internacional, o olhar mais adequado para o tema de proteção de dados é o que compreende como interesse global. Visto que dados circulam de forma extraterritorial. Ante a incessante troca de informações entre indivíduos, Estados, empresas etc., falar sobre dados pessoais e seus desdobramentos é falar sobre direitos fundamentais e proteção da dignidade da pessoa humana.

Dados são informações que proporcionam conhecimento e riqueza a quem tiver acesso a eles. O que se quer dizer é que uma vez colocados em rede de internet, os dados estão passíveis de serem explorados e consumidos por quem tiver interesse em construir algo a partir da informação de terceiros. Nesse sentido, Lévy fala sobre o ato praticado por um indivíduo produz informação, e, assim, é informação, seja ele um ato efetivo ou virtual. Dessa forma, torna-se riqueza em uma economia da informação. Considerando que o ciberespaço é um meio onde os atos podem ser registrados e explorados ou exploráveis, o consumidor se torna, ao mesmo tempo, coprodutor dos atos de forma cooperativa.

Todo ato registrável cria efetivamente ou virtualmente informação, ou seja, numa economia da informação, riqueza. Ora, o ciberespaço é por excelência o meio em que os atos podem ser registrados e transformados em dados exploráveis. Por isso o consumidor da informação, de transação ou de dispositivos de comunicação não cessa, ao mesmo tempo, de produzir uma informação virtualmente cheia de valor. O consumidor não apenas se torna coprodutor de informação que consome, mas é também produtor cooperativo dos “mundos virtuais” nos quais evolui, nem como

¹³BRADFORD, Anu. The Brussels Effect, *Northwestern University Law Review*, Vol. 107, p. 1, 2012; Columbia Law & Economics Working Paper No. 533 (2012). Available at: https://scholarship.law.columbia.edu/faculty_scholarship/1966

agente de visibilidade do mercado para os que exploram os vestígios de seus atos no ciberespaço¹⁴.

Refletindo sobre as palavras de Lévy, pode-se ter uma noção de como ocorre o funcionamento da sociedade atual no que diz respeito a comunicação e sobre os efeitos da disponibilização dos dados no ciberespaço. Seguindo esse raciocínio, as negociações internacionais comerciais consequentemente envolvem o compartilhamento de dados e dentre eles, os dados pessoais, o que gera a preocupação sobre esse mecanismo de atuação a nível mundial.

Assim, a União Europeia, ao firmar negociações comerciais com outros países, preconiza a utilização do Regulamento Europeu como parâmetro, sempre que entre os dados processados estejam os de cidadãos europeus. Não há aplicação do GDPR, mas sim um consenso em que se garanta o mínimo de proteção, como é demonstrada a preocupação a partir do regulamento europeu.

Isso refletiu, portanto, em acordos internacionais em que a União Europeia é signatária, pois passa colocar em pauta o debate sobre os princípios do GDPR (que é um ato vinculante apenas para os seus países membros) quando há a transferência de dados de seus cidadãos para o exterior. Dessa forma, coloca em discussão a proteção de dados, usando como referência o GDPR.

A título de exemplo, cita-se o acordo de parceria econômica entre União Europeia e Japão. Seguindo esse entendimento, Bendiek e Römer abordam os reflexos do regulamento europeu:

To ensure that individuals remain protected in an international data economy, EU legislators have created two safeguards: The *lex loci solutionis* (“Law of the place where relevant performance occurs”) requires any data processor to follow the EU’s General Data Protection Regulation (GDPR) whenever European customers’ data are processed. To give additional protection to data which are transferred abroad, GDPR principles have become enshrined into international trade agreements. Preeminent examples of the latter are the EUUS Privacy Shield, or relevant parts of the recently signed EU-Japan Economic Partnership Agreement (“Jefta,” for Japanese-European Free Trade Agreement)¹⁵¹⁶.

¹⁴ LÉVY, Pierre. *O que é virtual?* São Paulo. Ed. 34, 2ª edição, 2011, p. 63.

¹⁵ BENDIEK, Annegret; RÖMER, Magnus (2019): Externalizing Europe: the global effects of European data protection, *Digital Policy, Regulation and Governance*, ISSN 2398-5046, Emerald, Bingley, Vol. 21, Iss. 1, pp. 32-43, <https://doi.org/10.1108/DPRG-07-2018-0038>. Disponível em: <https://www.econstor.eu/bitstream/10419/210482/1/Full-text-article-Bendiek-et-al-Externalizing-Europe.pdf>. Acesso em: 15 mar 2024.

¹⁶ Tradução livre: Para garantir que os indivíduos permaneçam protegidos numa economia internacional de dados, os legisladores da UE criaram duas salvaguardas: A *lex loci Solutionis* (“Lei do local onde ocorre o desempenho relevante”) exige que qualquer processador de dados siga o Regulamento Geral de Proteção de Dados (GDPR) da UE, sempre que sejam tratados dados de clientes europeus. Para dar proteção adicional aos dados transferidos para o exterior, os princípios do GDPR foram consagrados em acordos comerciais internacionais. Exemplos proeminentes deste último são o Escudo de Privacidade

Quando há o interesse de um país em iniciar as tratativas de negociações comerciais com a União Europeia sobre proteção de dados se faz necessário um procedimento intitulado de “decisão de adequação¹⁷”. Isso porque se trata de possíveis fluxos de dados transfronteiriço.

O art. 45 do regulamento europeu afirma que a transferência de dados para terceiros países irá acontecer se a transação garante o nível adequado de proteção de dados. Nos casos em que a negociação aconteceu a comissão acompanha para saber se permanece a adequação, caso contrário, pode haver revogação¹⁸.

Além disso, a decisão leva em consideração aspectos políticos, além dos requisitos do parágrafo 2 do art. 45 entre outros requisitos. Fala-se em regras substancialmente equivalentes. Outrossim, as decisões tomadas vinculam todos os Estados membros da UE. Dessa forma, os procedimentos iniciam a partir da iniciativa do terceiro Estado que aciona a Comissão Europeia, considerando que a Comissão deve consultar o Comitê Europeu sobre Proteção de Dados e o parecer desse último é vinculante¹⁹.

Ainda sobre o aspecto negocial internacional, é mais eficiente para grandes empresas que participam do mercado global, se alinharem ao regulamento europeu. Quer dizer, de terem um entendimento, seja normativo ou institucional, no mesmo sentido que a UE entende sobre proteção de dados. Isso porque, diminui a possibilidade de divergências e, desse modo, não deixarão de atuar no âmbito da Europa, já que o GDPR é o fundamento e direcionamento para a UE também quando atua a nível global, haja vista o art. 45 do GDPR.

For global companies like Google, Facebook or Amazon, it is not an option to leave the European market. At the same time, it is an extraordinary burden to organize their business along two different sets of legal regulations. The inherent mobility of data necessitates de facto transnational regulation. For now, it is far more efficient to implement the rigid European regulations on a global scale, instead of trying to align digital markets with national borders.[3] As a result, the large providers of digital services claim to offer to the American consumer the same level of protection as they do for Europeans customers. The outcome is straight forward: although legally only aiming to safeguard EU customers who rely on foreign based services, the EU de facto extends the territorial reach of its data protection law, forcing foreign market

UE-EUA, ou partes relevantes do Acordo de Parceria Económica UE-Japão recentemente assinado (“Jefta”, para Acordo de Comércio Livre Japonês-Europeu).

¹⁷ UNIÃO EUROPEIA. General Data Protection Regulation. Art. 45. Disponível em: **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE)**. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679>. Acesso em: 20 jun 2024.

¹⁸ RUGANI, Gabriele. I FLUSSI DI DATI PERSONALI DALL’UE VERSO PAESI TERZI, TRA ESPANSIONE DEL COMMERCIO E PERSONAL DATA PROTECTION. 2022. Tese de Doutorado. 2022.

¹⁹ RUGANI, Gabriele. I FLUSSI DI DATI PERSONALI DALL’UE VERSO PAESI TERZI, TRA ESPANSIONE DEL COMMERCIO E PERSONAL DATA PROTECTION. 2022. Tese de Doutorado. 2022.

participants to obey EU law irrespective of whether they serve EU, US or any other customers. Yet from the EU's perspective, this indirect effect of European law on extraterritorial markets is not sufficient. Acknowledging the mobility of data and the importance of US digital service providers, the EU is additionally negotiating international agreements to ensure that EU customers' data is also protected when processed abroad, outside of its own jurisdiction. While not forcing third states to adopt EU legislation, adequacy agreements nevertheless aim to ensure that the third state's level of data protection is adequate, i.e. grants similar rights as EU law does²⁰.

A partir dessa compreensão que se apresenta aqui sobre a posição da Europa frente aos outros países, do ponto de vista de influência normativa, observa-se a posição liderança europeia em várias temáticas relevantes socialmente. Dessa forma, classificar a União Europeia como *Norm-Shaper* ou *Modeladora de Normas* é dizer que esta organização traz influência para vários outros Estados que não são os Estados-membros que a compõe, servindo de exemplo para a promoção de direitos em outras partes do mundo²².

Pode-se afirmar que a Comissão Europeia, que tem a função de defender interesses gerais da UE representa o papel da liderança europeia. Isso porque, ela tem competência para apresentar propostas e execuções legislativas, de políticas e do orçamento da UE. Nesse sentido, ao apresentar o Regulamento Europeu de Proteção de Dados como regramento, é dizer que exerce seu papel, conforme previsto o GPDR, e, dessa forma, fazendo a organização protagonizar no cenário mundial²³.

²⁰ BENDIEK, Annegret; RÖMER, Magnus (2019): Externalizing Europe: the global effects of European data protection, Digital Policy, Regulation and Governance, ISSN 2398-5046, Emerald, Bingley, Vol. 21, Iss. 1, pp. 32-43, <https://doi.org/10.1108/DPRG-07-2018-0038>. Disponível em: <https://www.econstor.eu/bitstream/10419/210482/1/Full-text-article-Bendiek-et-al-Externalizing-Europe.pdf>. Acesso em: 15 mar 2024.

²¹ Tradução livre: Para empresas globais como Google, Facebook ou Amazon, sair do mercado europeu não é uma opção. Ao mesmo tempo, é um fardo extraordinário organizar os seus negócios ao longo de dois conjuntos diferentes de regulamentos legais. A mobilidade inerente dos dados exige regulamentação transnacional de facto. Por enquanto, é muito mais eficiente implementar as rígidas regulamentações europeias à escala global, em vez de tentar alinhar os mercados digitais com as fronteiras nacionais.[3] Como resultado, os grandes fornecedores de serviços digitais afirmam oferecer ao consumidor americano o mesmo nível de protecção que oferecem aos clientes europeus. O resultado é simples: embora legalmente vise apenas proteger os clientes da UE que dependem de serviços baseados no estrangeiro, a UE alarga de facto o alcance territorial da sua lei de protecção de dados, forçando os participantes estrangeiros no mercado a obedecer à legislação da UE, independentemente de servirem a UE, EUA ou quaisquer outros clientes. No entanto, do ponto de vista da UE, este efeito indireto da legislação europeia nos mercados extraterritoriais não é suficiente. Reconhecendo a mobilidade dos dados e a importância dos prestadores de serviços digitais dos EUA, a UE está também a negociar acordos internacionais para garantir que os dados dos clientes da UE também sejam protegidos quando processados no estrangeiro, fora da sua própria jurisdição. Embora não obriguem os Estados terceiros a adotar legislação da UE, os acordos de adequação visam, no entanto, garantir que o nível de protecção de dados do Estado terceiro é adequado, ou seja, concede direitos semelhantes aos da legislação da UE

²² MONT'ALVERNE, Tarin Cristino Frota; LIMA, Maria Cecília Girão Veras. The European Union as a Norm Shaper on Biodiversity Protection. **Veredas do Direito**, v. 20, p. e202569, 2023.

²³ COMISSÃO EUROPEIA. Disponível em: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-commission_pt#:~:text=Tem%20a%20responsabilidade%20exclusiva%20de,e%20do%20Conselho%20da%20UE., acesso em 07/03/2024.

Como dito acima, o art. 45 do GDPR dá a competência a Comissão Europeia para análise sobre decisão de adequação. Ela faz a análise sobre o fluxo de dados transfronteiriços. A influência legislativa europeia é reconhecida pela doutrina brasileira na matéria de proteção de dados, ao se observar o trajeto para a promulgação da lei de proteção de dados brasileira.

O professor Magrini²⁴, em sua obra “Entre dados e robôs: ética e privacidade na era da hiperconectividade” ao falar sobre o caminho tomado para a construção da lei brasileira, relata a comparação com a lei europeia, demonstrando a sua influência e justifica, por isso, o porquê trabalhar com esta norma. Ele faz uma análise de similaridades entre ambas justificando a incidência europeia:

Exploraremos a fundo no tópico seguinte as previsões regulatórias específicas contidas na lei e seu contraste com a regulação europeia. A justificativa para essa comparação internacional se deve à forte influência da regulação europeia nos projetos de lei sobre dados pessoais no Brasil, assim como à maior compatibilidade e adequação entre o direito brasileiro e o direito europeu, razão pela qual não nos aprofundaremos neste trabalho nas especificidades da regulação norte-americana.

Ser reconhecida como influenciadora a nível normativo é também notável entre os próprios cidadãos europeus, especialmente aqueles que se dedicam a estudar e analisar privacidade e proteção de dados. Cataleta, em seu texto sobre os três anos de aplicação do Regulamento, afirma o reflexo do GDPR em outras nações, inclusive citando o Brasil:

Sono trascorsi tre anni da quando, il 25 maggio 2018, il Regolamento Generale sulla Protezione dei Dati Personali (**GDPR**) è divenuto applicabile e ben cinque dalla sua entrata in vigore, il 25 maggio 2016.

Da allora, l'Europa ha lasciato **un segno indelebile** in tema di regole in materia di dati personali che ha costretto diverse nazioni del mondo – e i giganti tech – ad adeguarsi implementando legislazioni simili, in grado di valorizzare e mettere al centro del nuovo ecosistema giuridico i **diritti** e le **libertà** dell'interessato.

In questi 3 anni, l'innovazione che il GDPR ha portato nel campo della protezione dei dati personali e l'impatto che ha avuto in Europa su tutti i player del settore, Big Tech comprese, ha fatto sì che il Regolamento Europeo fosse considerato **un benchmark a livello globale**, fungendo da musa ispiratrice per la creazione di altre leggi sulla protezione dei dati personali. Lo stesso Wojciech Wiewiórowski (European Data Protection Supervisor), in occasione proprio di questo terzo anniversario, ha affermato che “The GDPR has been a sensational achievement for Europe and its citizens, acting as a lighthouse for the entire global policy-making scene... It has acted as a catalyst for many jurisdictions around the world to draft and implement their own privacy and data protection legislation.”

La struttura orientata all'accountability, l'empowerment dei data subject ottenuto attraverso la previsione di un ventaglio più ampio di diritti azionabili a tutela dei propri dati, nonché la previsione di un **sistema sanzionatorio** come quello introdotto dal GDPR hanno ispirato, infatti, molte delle più recenti normative sulla privacy a livello globale, prima fra tutti la California, che con il suo **California Consumer Privacy Act** (a breve California Privacy Rights and Enforcement Act – CPRA) è diventata il primo Paese degli Stati Uniti con una normativa organica sulla privacy dei consumatori. In Brasile, la recentissima Brazilian General Data Protection Law (LGPD) è un altro esempio perfetto dell'influenza globale ottenuta dal GDPR,

²⁴ MAGRINI, Eduardo. Entre dados e robôs: ética e privacidade na era da hiperconectividade / Eduardo Magrani. — 2. ed. — Porto Alegre: Arquipélago Editorial, 2019.

essendo quasi interamente allineata con la disciplina europea. Da non dimenticare, inoltre, il Protection of Personal Information Act (POPIA) in Sudafrica ed il Personal Information Protection Act (PIPA) in Corea del Sud²⁵²⁶.

Os professores Gallo e Mula fazem referência no mesmo sentido, afirmando a transversalidade do GDPR pelo mundo:

Ma questo fenomeno contiene in sé un concetto molto più ampio, dato forse dalla eccezionale applicabilità territoriale del GDPR che non si limita alla sua portata normativa ma si estende nei principi e negli obblighi, investendo trasversalmente le legislazioni in materia di tutto il mondo²⁷²⁸.

A liderança sobre o debate a respeito de proteção de dados se deu pela União Europeia²⁹. Pinheiro afirma que o GDPR causou um “efeito dominó” pois os demais países e empresas que

²⁵ CATALETA, Anna. GDPR, um bilancio dei primi tre anni di applicazione: effetti, traguardi e prossimi step. Disponível em: <https://www.agendadigitale.eu/sicurezza/privacy/gdpr-un-bilancio-dei-primi-tre-anni-di-applicazione-effetti-traguardi-e-prossimi-step/>. 2021. Acesso em 16 mar 2024.

²⁶ Tradução livre: Passaram três anos desde que, em 25 de maio de 2018, o Regulamento Geral de Proteção de Dados (RGPD) se tornou aplicável e cinco desde a sua entrada em vigor, em 25 de maio de 2016.

Desde então, a Europa deixou uma marca indelével em termos de regras relativas aos dados pessoais, o que obrigou várias nações do mundo - e gigantes tecnológicos - a adaptarem-se através da implementação de legislação semelhante, capaz de potenciar e colocar no centro o novo ecossistema jurídico, os direitos e liberdades da parte interessada.

Nestes 3 anos, a inovação que o GDPR trouxe para o domínio da proteção de dados pessoais e o impacto que teve na Europa em todos os players do setor, incluindo as Big Tech, fez com que o Regulamento Europeu fosse considerado uma referência global, servindo de musa para a criação de outras leis de proteção de dados. O próprio Wojciech Wiewiórowski (Autoridade Europeia para a Proteção de Dados), por ocasião deste terceiro aniversário, afirmou que “O RGPD tem sido uma conquista sensacional para a Europa e os seus cidadãos, funcionando como um farol para todo o cenário político global... Tem funcionado como um catalisador para muitas jurisdições em todo o mundo elaborarem e implementarem a sua própria legislação sobre privacidade e proteção de dados.

A estrutura orientada para a responsabilização, o empoderamento dos titulares dos dados obtido através da concessão de uma gama mais ampla de direitos que podem ser aplicados para proteger os seus dados, bem como a disponibilização de um sistema de sanções como o introduzido pelo RGPD inspiraram, na verdade, muitas das regulamentações de privacidade mais recentes em nível global, em primeiro lugar na Califórnia, que com sua Lei de Privacidade do Consumidor da Califórnia (em breve Lei de Direitos e Execução de Privacidade da Califórnia - CPRA) se tornou o primeiro país nos Estados Unidos com um orgânico regulamentação sobre a privacidade dos consumidores. No Brasil, a muito recente Lei Geral de Proteção de Dados (LGPD) brasileira é outro exemplo perfeito da influência global alcançada pelo GDPR, estando quase totalmente alinhada com a regulamentação europeia. Também não devem ser esquecidas a Lei de Proteção de Informações Pessoais (POPIA) na África do Sul e a Lei de Proteção de Informações Pessoais (PIPA) na Coreia do Sul.

²⁷ GALLO, Veronica. MULA, Davide. USA, come sta cambiando l'approccio alla privacy: la grande svolta. 2021. Disponível em: <https://www.agendadigitale.eu/sicurezza/privacy/dal-diritto-alla-solitudine-alla-protezione-dei-dati-come-cambia-lapproccio-alla-privacy-negli-usa/>. Acesso em: 16 mar 2024.

²⁸ Tradução Livre: Mas este fenómeno contém em si um conceito muito mais amplo, talvez dado pela excecional aplicabilidade territorial do RGPD que não se limita ao seu âmbito regulatório mas se estende em princípios e obrigações, afetando transversalmente a legislação relevante em todo o mundo.

²⁹ PINHEIRO, Patrícia Peck. Proteção de dados pessoais. Comentários à Lei n. 13.709/2018. 4ª ed. Saraiva, 2023, p. 6.

mantivessem relações comerciais com a União Europeia deveriam ter normativa do mesmo porte.

Interessante afirmar que a UE se posiciona como sendo padrão ouro no que diz respeito a proteção de dados:

The EU's data protection laws have long been regarded as a gold standard all over the world. Over the last 25 years, technology has transformed our lives in ways nobody could have imagined so a review of the rules was needed³⁰.

No que diz respeito a proteção de dados é importante mencionar que o protagonismo europeu não começa pelo GDPR. Sua posição de regulamentação sobre dados pessoais, no cenário mundial, se deu com a Diretiva³¹ que antecedeu o Regulamento, que já tinha o condão de modelo para outros países:

il livello di tutela assicurato ai titolari dei dati dalla direttiva del 1995 era già stato considerato un esempio da seguire spontaneamente. Il nuovo regolamento, attuando la previsione del Trattato che fa della protezione dei dati personali un diritto fondamentale, per queste ed altre ragioni, è destinato – nelle intenzioni delle istituzioni comunitarie – a divenire un «global standard»³²³³.

Aqui é importante abrir uma observação sobre a diferença entre Regulamento e Diretiva. Isso poderia gerar um questionamento sobre o porquê houve a necessidade de elaborar um Regulamento, tendo em vista que já existia uma diretiva sobre a matéria.

Trata-se de estrutura normativa do ordenamento europeu. O funcionamento e a incidências dessas normas nos Estados-membros são diferentes. A diretiva é de abrangência para todos os Estados, entretanto, ela não incide diretamente, se faz necessário que cada país elabore uma norma específica adequada ao que a diretiva exige. Já o Regulamento tem aplicação imediata, não sendo necessário que haja uma norma adaptativa de cada Estado para que seja aplicada.

³⁰ EUROPEAN DATA PROTECTION SUPERVISOR. The History of The General Data Protection Regulation. Disponível em: https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en. Acesso em: 17 mar 2024.

³¹ UNIÃO EUROPEIA. Diretiva 95/46/EC do Parlamento Europeu e Conselho, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>. Acesso em 28 mar 2024.

³² AIELLO, Giuseppe Francesco. La protezione dei dati personali dopo il trattato di Lisbona: natura e limiti di un diritto fondamentale <disomogeneo> alla luce della nuova proposta di General Data Protection Regulation. Disponível em: <https://www.rivisteweb.it/doi/10.4478/81757>. Acesso em 25 mar 2024.

³³ Tradução livre: o nível de protecção garantido aos titulares dos dados pela directiva de 1995 já tinha sido considerado um exemplo a seguir espontaneamente. O novo regulamento, que implementa a disposição do Tratado que torna a protecção dos dados pessoais um direito fundamental, por estas e outras razões, está destinado - nas intenções das instituições comunitárias - a tornar-se uma "norma global".

O Regulamento é de incidência obrigatória de imediato para todos os países que fazem parte da União Europeia. Em todos os casos, são de cumprimento obrigatório, entretanto, a forma como são aplicados é que os diferencia. Além disso, o GDPR inovou a respeito da matéria de proteção de dados em relação a diretiva, pois trouxe mais detalhes sobre regramento. A diretiva traz objetivos a serem alcançados, o regulamento traz normas diretamente aplicáveis. A diretiva tem flexibilidade alta e uniformidade baixa, já o regulamento tem flexibilidade baixa e uniformidade alta.

Dessa forma, a influência europeia sobre atenção na proteção sobre os dados pessoais se torna cada vez mais importante no cenário do comércio internacional. Isto porque não existe uma regulamentação específica sobre a matéria de abrangência mundial, exceto a convenção 108+ que ainda é introdutório. A União Europeia é a organização que mais demonstra exigir um olhar adequado quanto aos dados no contexto de acordos internacionais. Daí o seu protagonismo.

No Comunicado emitido pelo Parlamento Europeu sobre proteção de dados e globalização também foi enfatizado o papel da União Europeia no cenário mundial no que diz respeito a regulação dos dados:

The demand for protection of personal data is however not limited to Europe. Consumers around the world increasingly cherish and value their privacy. In turn, companies recognise that strong privacy protections give them a competitive advantage as confidence in their services increases. Many, especially those with global reach, are aligning their privacy policies with the GDPR, both because they want to do business in the EU, and because they see it as a model to follow³⁴³⁵.

Nesse sentido, no estudo do perfil *Modelador de Normas* e do GDPR, a influência europeia na atenção à proteção dos dados pessoais torna-se cada vez mais importante no contexto do comércio internacional. Isso ocorre porque não existe uma regulamentação específica consolidada sobre o assunto em nível global e os países não consideravam a referida área uma prioridade. A União Europeia é a organização que mais enfatiza a importância de dar

³⁴ EUROPIAN COMISSION. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Exchanging and Protecting Personal Data in a Globalised World. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN>. Acesso em 28 mar 2024.

³⁵ Tradução livre: A procura de protecção de dados pessoais não se limita, contudo, à Europa. Os consumidores em todo o mundo prezam e valorizam cada vez mais a sua privacidade. Por sua vez, as empresas reconhecem que fortes proteções à privacidade lhes proporcionam uma vantagem competitiva à medida que aumenta a confiança nos seus serviços. Muitos, especialmente aqueles com alcance global, estão a alinhar as suas políticas de privacidade com o RGPD, tanto porque querem fazer negócios na UE, como porque o veem como um modelo a seguir.

a devida atenção aos dados no contexto dos acordos internacionais, o que confere destaque ao seu protagonismo³⁶.

O que se pode afirmar, até então, é sobre a existência da convenção 108+³⁷ do Conselho Europeu que tem como objetivo a proteção das pessoas singulares no que diz respeito ao tratamento de dados automatizados. Ainda preambular, tal convenção é de 1981 e foi o primeiro instrumento internacional juridicamente vinculativo sobre proteção de dados.

Importante salientar que no quesito de avanços tecnológicos, o Parlamento Europeu acaba de regulamentar o uso de Inteligência artificial³⁸. Em 1º de agosto entrou em vigor o AI Act, a lei de inteligência artificial da União Europeia que tem como objetivo regulamentar sistemas de inteligência artificial. Trata-se de norma da UE com efeitos extraterritoriais, pois é aplicada a qualquer sistema que venha impactar no mercado ou nos cidadãos europeus mesmo que não tenha operação no território da UE. Tozzini Freire advogados afirma que é necessária uma abordagem coordenada e global sobre como lidar com IA complementando que a EU Act servirá de inspiração para outras regulamentações, incluindo o Brasil³⁹.

O intuito é de proteger os direitos fundamentais, democracia, o Estado de Direito e sustentabilidade ambiental. O regulamento sobre a IA traz alguns regramentos para proteger contra potenciais riscos e nível de impacto. Esse regulamento sobre IA tem forte tendência de influenciar outros países, principalmente companhias do mundo. Lucas Reis faz algumas observações sobre o aspecto do marketing, mas que pode trazer reflexões sobre outras áreas quanto a influência desse novo regulamento. Ele afirma sobre a falada influência sobre empresas e profissionais que não estão na Europa. Isso reafirma o protagonismo europeu em mais uma área da ciência social⁴⁰.

³⁶ FEDRECHESKI, Geovane. Entenda como a GDPR, a LGPD e NIST ajudam na proteção de dados pessoais. 05/07/2023. Disponível em: <https://www.alura.com.br/artigos/gdpr-lgpd-nist-ajudam-protecao-dados-pessoais>. Acesso em: 21 jun 2024.

³⁷ UNIÃO EUROPEIA. Council of Europe. Convenção 108+. Disponível em: <https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2>. Acesso em: 06 jul 2024.

³⁸ UNIÃO EUROPEIA. Regulamento Inteligência Artificial: Parlamento aprova legislação histórica. Disponível em: <https://www.europarl.europa.eu/news/pt/press-room/20240308IPR19015/regulamento-inteligencia-artificial-parlamento-aprova-legislacao-historica>. Acesso em: 01 abril 2024.

³⁹ Lei de Inteligência Artificial da União Europeia entra em vigor. Publicado em 06 de agosto de 2024. Disponível em: <https://www.tozzinifreire.com.br/boletins/lei-de-inteligencia-artificial-da-uniao-europeia-entra-em-vigor>. Acesso em: 15 out 2024.

⁴⁰ REIS, Lucas. Regulamentação Europeia sobre Inteligência Artificial: o que uma liderança de marketing precisa saber. A versão final da regulamentação possui 272 páginas e ele influenciará a atuação da maior parte das companhias do mundo. Disponível em:

Isto posto, pode-se observar no cenário global o papel considerável de *Modelador de Normas* da União Europeia com alcance normativo que se estende cada vez mais a países terceiros. O protagonismo e o pioneirismo são características que tem se destacado na Organização, especialmente no que tange as regulamentações frente aos avanços tecnológicos.

Assim, é relevante para a pesquisa estudar a origem e desenvolvimento sobre proteção de dados na UE, pois compreender todo o mecanismo construído em seu regulamento traz mais propriedade para discutir e disseminar aprimoramentos. Essa análise permite concluir que há intenção de tornar sólida a preocupação sobre os direitos fundamentais, a democracia e o uso adequado da tecnologia. Dessa forma, a UE ocupa um posto de responsabilidade global, pois os seus passos legislativos seguem como tendência para os países terceiros.

Desenvolvimento cronológico do General Data Protection Regulation – GDPR e algumas considerações sobre este Regulamento

Antes de adentrar na abordagem regulatória protetiva dos dados aqui proposta, é substancial explicar de forma sucinta a estrutura que constitui a União Europeia para que se possa compreender a própria formação do regulamento e como funcionam as normativas a nível europeu. Importante frisar que a necessidade da integração entre os países europeus se deu no Pós-Guerra, com intenção de fortalecimento e desenvolvimento formando o Mercado comum, além da busca pela paz.

A partir de então, o ordenamento europeu teve início a partir de três organizações internacionais com objetivo de integração econômica entre os estados membros. Ocorreram as negociações entre Comunidade Europeia do Carvão e do aço (CECA), Comunidade Econômica europeia (CEE), Comunidade Europeia para energia atômica (CEEa ou Euratom). As organizações CECA e CEEa tinham objetivo de estabilidade na área de carvão, aço e energia atômica. Já a CEE almejava integração econômica e social. Tais anseios por estabilidade tiveram força no Pós Guerra com o ideal internacionalista.

As intenções se limitavam aos vieses econômico e social, não abrangia o viés político pelo receio de haver rejeição por parte dos países membros à proposta de integração, podendo comprometer esse processo. O tratado se baseava na filosofia da integração europeia, levando

o nome de *funzionalismo*. O *funzionalismo* traz a proposta de integração entre os Estados da Europa no que tange a economia e a parte social, para, gradualmente chegar à parte política.

Nesse sentido, tais tratados foram evoluindo, sendo aprimorados e aperfeiçoados os objetivos e fazendo surgir a Comunidade Europeia com a proposta de integração. As três comunidades prosperaram e a União Europeia sucedeu a Comunidade Europeia. Obteve-se o Tratado da União Europeia, Maastricht, em 1993 que institui a União Europeia que não tinha proposta de desconstituir a Comunidade original. Havia a intenção de acrescentar a forma de cooperação na área jurídica, política externa e segurança comum. Tudo isso aconteceu em um primeiro momento.

No segundo momento houve a condução para o Tratado de Nice⁴¹ que foi elaborado em 26 de fevereiro de 2001 e assinado em 1 de fevereiro de 2003. Alterou o Tratado da União Europeia, os tratados que instituem as Comunidades Europeias e alguns atos relativos a esses tratados. O tratado de Nice teve como objetivo reformar a estrutura institucional da União Europeia abrindo para ampliação e adesão de novos membros.

Posteriormente, realizou-se a redação do Tratado de Lisboa^{42,43} que foi assinado em 2007 e entrou em vigor em 2009. O que antes era entendido como Comunidade Europeia (nos tratados negociados anteriormente), traz muitas modificações no que tange a competências, estrutura e processos de decisões, por exemplo, moldando a então União Europeia. O tratado de Lisboa tem tentado racionalizar o complexo sistema jurídico da integração europeia.

Hoje, a União Europeia tem como regras fundamentais o Tratado da União Europeia (TUE) e as regras de funcionamento que estão previstas no Tratado de funcionamento da União Europeia (TFUE), ambos com iguais valores jurídicos perante a União Europeia. Além disso, o tratado de Lisboa confere valor vinculante à Carta de Direitos Fundamentais⁴⁴.

Especificamente sobre proteção de dados, o Tratado sobre Funcionamento da União Europeia, em seu art. 16 aborda a temática. Nele prevê que o Parlamento e o Conselho

⁴¹ UNIÃO EUROPEIA. **Tratado que institui a Comunidade Europeia (Versão consolidada 2002)**. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:12002E/TXT>. Acesso em 21 jun 2024.

⁴² TRATADO DE LISBOA. Disponível em: <https://www.parlamento.pt/europa/Paginas/TratadodeLisboa.aspx>, acesso em 02/03/2024.

⁴³ UNIÃO EUROPEIA. Tratado de Nice. EUR-Lex. Access to European Union Law. Tratado de Nice. Síntese do Tratado de Nice. Disponível em: <https://eur-lex.europa.eu/PT/legal-content/summary/treaty-of-nice.html>. Acesso em: 21 jun 2024.

⁴⁴ CANNIZZARO, Enzo. Il diritto dell'integrazione europea: l'ordinamento dell'Unione. 2ª ed, Giappichelli, Torino 2017, p. 1-4.

estabeleçam normas protetivas para as pessoas singulares, no que tange a tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros nos exercícios das atividades relacionadas com a União. Tudo isso quando estiver relacionado a circulação de dados⁴⁵.

As breves considerações sobre formação da União Europeia são fundamentais tendo em vista que, tal como é constituída hoje, traz os pilares que são referenciados como norteadores para a organização. Desse modo, a elaboração do Regulamento Europeu utilizou-se de princípios e garantias neles contidos para, então, desenvolver a estrutura adequada de norma de proteção de dados.

Ao analisar a construção normativa da União Europeia sobre direitos fundamentais, é importante salientar que a Declaração Universal sobre os direitos do homem foi um dos pontos iniciais⁴⁶. Um documento universal que direciona várias nações para o objetivo comum, o de proteger os direitos fundamentais de todas as pessoas. Essa visão sobre a Declaração Universal sobre os direitos do homem remete a dignidade da pessoa humana. Dessa forma, a proteção dos dados pessoais está ligada aos direitos da personalidade⁴⁷.

Considerando que a Carta de direitos fundamentais é base jurídica sobre proteção de dados pela União Europeia^{48,49}, é importante enfatizar que o referido documento estabelece que a União respeita os direitos, liberdades e princípios, iniciando seu texto com dignidade do ser humano. Desse modo, afirma ser inviolável a dignidade e deve ser respeitada e protegida. O direito a proteção dos dados pessoais é um direito fundamental e de acordo com o art. 12⁵⁰ da Declaração Universal ninguém deve ter interferências arbitrárias em sua privacidade: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to

⁴⁵ TRATADO SOBRE O FUNCIONAMENTO DA UNIÃO EUROPEIA. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF, acesso em 02/03/2024.

⁴⁶ DECLARAÇÃO UNIVERSAL SOBRE OS DIREITOS DO HOMEM. Disponível em: <https://brasil.un.org/pt-br/91601-declara%C3%A7%C3%A3o-universal-dos-direitos-humanos>, acesso em 02/03/2024.

⁴⁷ UNIÃO EUROPEIA. EUROPEAN DATA PROTECTION SUPERVISOR. DATA PROTECTION. Disponível em: [HTTPS://WWW.EDPS.EUROPA.EU/DATA-PROTECTION/DATA-PROTECTION_EN](https://www.edps.europa.eu/data-protection/data-protection_en). Acesso em: 21 JUN 2024.

⁴⁸ UNIÃO EUROPEIA. Parlamento Europeu. Proteção de dados. Disponível em: https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf. Acesso em: 06 jul 2024.

⁴⁹ UNIÃO EUROPEIA. Carta de Direitos Fundamentais. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 06 jul 2024.

⁵⁰ UNITED NATIONS. Universal Declaration of Human Rights. Disponível em: <https://www.un.org/en/about-us/universal-declaration-of-human-rights>. Acesso em: 21 jun 2024.

attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks⁵¹.

A partir disso, surgiu a Convenção Europeia sobre Direitos Humanos⁵², em 1950, baseada na Declaração Universal sobre os direitos do homem. É significativo salientar que em seu art. 8º afirma o respeito à vida privada e familiar, uma previsão relacionada com a privacidade. Essa garantia de respeito à vida e a família já é a sinalização necessária para a regulamentação dos direitos delas decorrentes, como seria o exemplo dos dados pessoais.

No contexto de privacidade, uma análise de considerável importância sobre as normas atinentes a proteção de dados, agora no âmbito internacional, diz respeito a Convenção 108 de 1981 do Conselho Europeu, já citada acima. Esse documento se propõe a abordar a proteção de dados pessoais. Observa-se no texto a preocupação sobre o objetivo de alcançar a unidade dos Estados-Membros, considerando a dignidade da pessoa humana, a proteção dos direitos humanos e das liberdades fundamentais, dentre outros⁵³.

Esse documento é tido como um dos mais relevantes instrumentos que aborda o tema de forma global. Como dizem Fachinetti e Camargo em artigo de opinião:

A convenção, introduzida pelo Conselho da Europa, é uma regulação transversal que estipula um regime de governança para questões de proteção de dados pessoais, consistindo em um marco internacional que começou a pavimentar potencial estrutura global de proteção de dados⁵⁴.

Eles esperam que a partir de tal convenção, se possível, sejam adotados padrões e estruturas globais que tragam essas proteções, aumentem a segurança jurídica, aprimorem a aplicação transfronteiriça de normativos, fortaleçam inovações e promovam o crescimento econômico entre as nações⁵⁵.

⁵¹ Tradução livre: Ninguém será sujeito a intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem a ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques.

⁵² EUROPEAN CONVENTION ON HUMAN RIGHTS. Disponível em: <https://www.coe.int/en/web/human-rights-convention>, acesso em 02/03/2024.

⁵³ CONVENÇÃO 108/1981. Disponível em: <https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2>, acesso em 01/03/2024.

⁵⁴ FACHINETTI, Aline Fuke. CAMARGO, Guilherme. Convenção 108 +: o tratado de proteção de dados e a relevância do tema para o Brasil. 04/07/2021. Disponível em: <https://www.conjur.com.br/2021-jul-04/opiniao-convencao-108-relevancia-protecao-dados/>. Acesso em: 23 jun 2024.

⁵⁵ FACHINETTI, Aline Fuke. CAMARGO, Guilherme. Convenção 108 +: o tratado de proteção de dados e a relevância do tema para o Brasil. 04/07/2021. Disponível em: <https://www.conjur.com.br/2021-jul-04/opiniao-convencao-108-relevancia-protecao-dados/>. Acesso em: 23 jun 2024.

No mesmo texto, fala-se sobre a necessidade de incluir na proteção os dados pessoais, considerando o papel na sociedade e a conciliação com outros direitos. Afirma a necessidade de promover, a nível mundial, os valores fundamentais do respeito pela primazia e pela proteção dos dados pessoais, e demonstrando o interesse na livre circulação de informação entre as pessoas⁵⁶.

Nesse sentido, os autores explicam que a Convenção 108 surgiu com o propósito apresentar princípios basilares sobre proteção de dados⁵⁷. A sua modernização tem dois objetivos principais:

Embora os princípios fundamentais contidos na Convenção n.º 108 de 1981 tenham resistido ao teste do tempo e a sua abordagem generalista e tecnologicamente neutra constitua uma força inegável, o Conselho da Europa considerou necessário modernizar o seu instrumento de referência. A modernização da Convenção n.º 108 visa dois objetivos principais: enfrentar os desafios decorrentes da utilização das novas tecnologias da informação e da comunicação e reforçar a aplicação efetiva da Convenção⁵⁸.

É ainda substancial mencionar, que antes do surgimento do GDPR havia a diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 1995, que abordava a proteção das pessoas singulares no que diz respeito a tratamento de dados pessoais e a livre circulação desses dados. Após a vigência do GDPR, ficou revogada tal Diretiva 95/46/CE⁵⁹ que era a norma que tratava sobre o assunto de proteção de dados das pessoas singulares. O Regulamento Europeu, que entrou em vigor, trata o tema de forma mais detalhada, mas deve-se considerar a importância da Diretiva no contexto normativo.

Dando sequência sobre as normas assecuratórias de direitos sobre proteção de dados, é necessário falar sobre a Carta de Direitos Fundamentais da União Europeia⁶⁰. Datada do ano de 2000, aborda direitos, liberdades e princípios que formaram a base da União Europeia. Em seu

⁵⁶ CONVENÇÃO 108/1981. Disponível em: <https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2>, acesso em 01/03/2024.

⁵⁷ FACHINETTI, Aline Fuke. CAMARGO, Guilherme. Convenção 108 +: o tratado de proteção de dados e a relevância do tema para o Brasil. 04/07/2021. Disponível em: <https://www.conjur.com.br/2021-jul-04/opinioao-convencao-108-relevancia-protecao-dados/>. Acesso em: 23 jun 2024.

⁵⁸ CONVENÇÃO 108+. Convenção para a proteção das pessoas relativamente ao tratamento de dados de carácter pessoal. Disponível em: <https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2#:~:text=A%20presente%20Conven%C3%A7%C3%A3o%20tem%20por,do%20direito%20%C3%A0%20vida%20privada>. Acesso em: 23 jun 2024.

⁵⁹ UNIÃO EUROPEIA. Departamento temático dos Direitos dos Cidadãos e dos Assuntos Constitucionais do Parlamento Europeu. Proteção de dados pessoais. Disponível em: <https://www.europarl.europa.eu/factsheets/pt/sheet/157/protecao-dos-dados-pessoais>. Acesso em 22 mar 2024.

⁶⁰ CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf, acesso em 02/03/2024.

art. 7º estão previstos o respeito à vida privada e familiar (aparentemente seguindo o texto da Declaração Universal dos Direitos do Homem). E, em seu art. 8º, prega a proteção dos dados pessoais, garantindo o tratamento para fins específicos e com o consentimento da pessoa ou por outro fundamento legítimo. Além disso, autoriza a fiscalização por órgão competente⁶¹.

O Regulamento europeu faz referência a Carta de Direitos fundamentais e a Convenção Europeia para proteção dos direitos do homem e das liberdades fundamentais. Em suas considerações, nº. 73, faz referência a tais documentos, indicando que deverão ser respeitados os ditames da Carta e Convenção quanto às restrições a princípios específicos e direitos a informação etc. Segue o texto do nº. 73 do Regulamento Europeu:

(73) O direito da União ou dos Estados-Membros podem impor restrições relativas a princípios específicos e aos direitos de informação, acesso e retificação ou apagamento de dados pessoais e ao direito à portabilidade dos dados, ao direito de oposição, às decisões baseadas na definição de perfis, bem como à comunicação de uma violação de dados pessoais ao titular dos dados, e a determinadas obrigações conexas dos responsáveis pelo tratamento, na medida em que sejam necessárias e proporcionadas numa sociedade democrática para garantir a segurança pública, incluindo a proteção da vida humana, especialmente em resposta a catástrofes naturais ou provocadas pelo homem, para a prevenção, a investigação e a repressão de infrações penais ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública ou violações da deontologia de profissões regulamentadas, para outros objetivos importantes de interesse público geral da União ou de um Estado-Membro, nomeadamente um interesse económico ou financeiro importante da União ou de um Estado-Membro, para a conservação de registos públicos por motivos de interesse público geral, para posterior tratamento de dados pessoais arquivados para a prestação de informações específicas relacionadas com o comportamento político no âmbito de antigos regimes totalitários ou para efeitos de defesa do titular dos dados ou dos direitos e liberdades de terceiros, incluindo a proteção social, a saúde pública e os fins humanitários. Essas restrições deverão respeitar as exigências estabelecidas na Carta e na Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais⁶².

Assim, com o cenário de hiperconectividade alavancado pelo uso da internet em maior escala, o modelo de sociedade se transforma através do grande fluxo de informações. O movimento regido nesse sentido, torna a discussão sobre proteção de dados pessoais um trabalho significativo para a construção de um espaço, físico ou virtual, justo, igualitário e

⁶¹ CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf, acesso em 02/03/2024.

⁶² UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>. Acesso em: 21 jun 2024.

seguro. Trata-se também de uma preocupação da Organização das Nações Unidas que já elabora o Pacto Digital Global⁶³.

É pertinente mencionar que ao abordar o assunto sociedade hiperconectada há de se fazer correlação com proteção de dados porque ao se inserir tais informações no ambiente virtual, passam a estar no espaço virtual. Além disso, o acesso é normalmente realizado a partir de uma simples conexão à internet e, a depender do nível de proteção de camadas em que se encontrem, podem estar mais ou menos vulneráveis do ponto de vista da segurança da informação.

Uma sociedade hiperconectada é dizer que os indivíduos estão conectados a todo tempo por meio das ferramentas tecnológicas e internet. Isso permite dizer que as informações circulam em uma velocidade infinitamente maior do que seria se não houvesse internet. Tanto o acesso quanto a disponibilidade de informações se tornam rápidos e acessíveis pelo uso de um smartfone ou de um computador, conectados à internet.

Isso quer dizer instantaneidade ao acesso à informação. Dessa forma, os dados quando postos em rede de internet, tornam-se disponíveis. Assim, falar em dados pessoais é pensar também em um contexto hiperconectado, pois quando os dados são coletados de forma digital, já se encontram no espaço virtual e sujeitos a essa dinâmica de comunicação e acesso. E, nesse sentido, considerando a temática central do capítulo, qual seja, a União Europeia como *Modeladora de Normas* em matéria de proteção de dados, cabe tecer reflexões sobre o Regulamento Europeu que é o principal objeto de análise nesse contexto de protagonismo, não desconsiderando as demais normativas sobre o mesmo tema.

Após a análise de importante significância sobre o histórico normativo a respeito da evolução da União Europeia e sobre privacidade e proteção de dados, que fundamentam a compreensão europeia sobre o tema, dá-se sequência com a abordagem do General Data Protection Regulation - GDPR. Isso porque, foi o General Data Protection Regulation – GDPR que marcou a liderança regulatória especificamente sobre proteção de dados que se espalhou como exemplo pelo mundo como já discutido no início do capítulo.

Nesse diapasão, analisando as normativas da UE, dentre as que abordam a matéria de proteção de dados e seus desdobramentos, observa-se o Tratado de Lisboa, que discorre sobre defesa dos dados para que aconteça de forma clara e eficaz (aqui inclui o TFUE e as

⁶³ ONU Brasil. Rede Brasil do Pacto Global quer mais empresas alinhadas aos objetivos globais. Disponível em: <https://brasil.un.org/pt-br/83698-rede-brasil-do-pacto-global-quer-mais-empresas-alinhadas-aos-objetivos-globais>. Acesso em: 30 mar 2024.

competências para regulamentação). Dessa maneira, é conveniente mencionar, em meio a análise, apesar de não ser referente a normativa da União Europeia, que a Itália já tinha um Decreto Legislativo 196/2003 (como mencionado anteriormente), o chamado Código de Proteção de Dados Pessoais que antecedeu o Regulamento Europeu com texto também detalhado sobre a matéria⁶⁴.

Fazendo um panorama temático normativo sobre proteção de dados, no contexto europeu, observa-se a preocupação voltada para o respeito à vida privada, todos entendidos como direitos fundamentais. Nesse sentido, o Parlamento Europeu compreende que garantir a proteção de tais direitos está associado a proteger os direitos humanos. Assim, tem-se como uma das bases jurídicas o Tratado sobre funcionamento da União Europeia, já abordado acima, que em seu artigo 16 e art. 7º e 8º da Carta de Direitos fundamentais são as diretrizes basilares da União Europeia.

Atualmente, os instrumentos normativos indicados como protetivos de dados pessoais pelo Parlamento Europeu são o Regulamento Geral de Proteção de Dados (em inglês a sigla é GDPR) e Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho. Esta que aborda a aplicação da lei quanto ao tratamento de dados pessoais quando estes forem utilizados pelas autoridades responsáveis pela aplicação da lei (aborda proteção de dados de vítimas, testemunhas se suspeitos de crimes, cabendo cooperação transfronteiriça quanto à luta contra a criminalidade e terrorismo)⁶⁵.

Essas observações conduzem a compreensão de um posicionamento europeu voltado para proteção de dados. O regulamento sobre o tema traz significativos posicionamentos que demonstram a especificidade a que ele se propôs normatizar com base em sua visão de direito

⁶⁴ ITÁLIA. Decreto Legislativo de 30 de giugno 2003, n. 196. Codice in Materia di Protezione dei Dati Personali. Disponível em: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2003-07-29&atto.codiceRedazionale=003G0218. Acesso em 25 mar 2024.

⁶⁵ Na análise, inclui-se a existência das Diretivas sobre privacidade e comunicações eletrônicas, a Diretiva 2002/58 que foi alterada pela Diretiva 2009/136, artigos sobre proteção de dados em atos legislativos setoriais, além das disposições internacionais sobre proteção de dados (transferência de dados comerciais associadas a adequação nas negociações, acordos com outros países, incluindo o Acordo Global UE-EUA, dentre outros).

Aqui é importante citar a recente notícia a respeito de proteção de dados e a vigilância dos EUA no estrangeiro. Em abril, o presidente dos EUA, Joe Biden, renovou uma seção do quadro de vigilância dos EUA, prolongando por dois anos a autorização para monitorizar e recolher dados sem mandatos de não americanos em todo o mundo, incluindo europeus. EURONEWS. O que significa uma lei de vigilância dos EUA para a privacidade dos dados europeus. 01/06/2024. Disponível em: <https://pt.euronews.com/next/2024/06/01/o-que-significa-uma-lei-de-vigilancia-dos-eua-para-a-privacidade-dos-dados-europeus>. Acesso em: 23 jun 2024.

fundamentais. Nesse sentido, passa-se a análise sobre o regulamento europeu acerca da proteção de dados.

O GDPR inaugura o texto do documento remetendo à proteção das pessoas singulares, fazendo referência aos dados como direitos fundamentais, pontuando a Carta de Direitos Fundamentais da União Europeia, tratado sobre funcionamento da UE, além de reafirmar a existência da Convenção Europeia para proteção dos direitos do Homem e Liberdades Fundamentais. Observa-se, nesse sentido, o elevado grau de importância que é dado aos dados pessoais, privacidade e direitos fundamentais⁶⁶.

A respeito da relevância do Regulamento, Spagnolo ressalta a afirmativa sobre direito fundamental ao abordar a norma:

Il presupposti del Regolamento sono contenuti nei 173 considerando che precedono l'enunciazione dei 99 articoli ed han no una forte rilevanza dal punto di vista etico-giuridico. Il diritto della persona alla protezione dei dati di carattere personale che la riguardano è considerato un "diritto fondamentale", richiamato dalla Carta dei diritti fondamentali dell'Unione europea e dal Trattato sul funzionamento dell'Unione europea, e il trattamento dei dati personali viene configurato come al servizio dell'uomo^{67,68}.

No considerando nº. 3 da parte introdutória do GDPR há a abordagem sobre a regulamentação através da Diretiva de 2016/680, sobre proteger os referidos dados no âmbito da cooperação judiciária em matéria de âmbito penal e policial. Esta Diretiva estabelece regra para o tratamento e circulação dos dados na condição de cooperação judiciária específica. A regra posta nesta Diretiva demonstra a preocupação em assegurar a proteção de dados ao mesmo tempo que reconhece o interesse público, haja vista ser processo que trata de segurança pública. Mesmo sendo coletados os dados para fins de interesse público, o texto traz a preocupação em como serão tratados os dados nesse contexto.

⁶⁶ UNIÃO EUROPEIA. Proteção de dados e respeito a vida privada são Direitos fundamentais. Presente no texto sobre Proteção de dados da União Europeia. Proteção de dados pessoais. Disponível em: <https://www.europarl.europa.eu/factsheets/pt/sheet/157/protecao-dos-dados-pessoais>. Acesso em 30 mar 2024.

⁶⁷ SPAGNOLO, Antonio G. Il Regolamento Europeo sulla protezione dei dati personale: implicazioni pela ricerca scientifica. Medicina e Morale, 2018, Vol.67 (2), p.151-157. Disponível em: <https://web.p.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=0&sid=db0cf330-f25f-486d-b286-7a6475feec75%40redis>. Acervo da Biblioteca da UNIFI. Acesso em 25 mar 2024.

⁶⁸ Tradução livre: Os pressupostos do Regulamento estão contidos nos 173 considerando que antecedem o enunciado dos 99 artigos e têm forte relevância do ponto de vista ético-jurídico. O direito da pessoa à proteção dos dados pessoais que lhe digam respeito é considerado um "direito fundamental", referido na Carta dos Direitos Fundamentais da União Europeia e no Tratado sobre o Funcionamento da União Europeia, e o tratamento de dados pessoais configura-se como se estivesse a serviço do homem

O considerando nº. 5 traz uma afirmação mais específica sobre a proteção dos dados e a livre circulação. Mostra a necessidade de harmonização das regras do regulamento quando da utilização no setor público pelos Estados-membros. Enfatiza que devem ser seguidos os princípios do Regulamento 2016/679⁶⁹. Trata-se de uma interpretação homogênea. Mais uma vez faz referência ao setor público, reafirmando que o cuidado com os dados abrange todos os âmbitos.

Há de se ressaltar o considerando nº. 10 o qual afirma que o nível de proteção dos direitos e liberdades das pessoas singulares relativamente ao tratamento desses dados deverá ser equivalente em todos os Estados-membros. No texto, há a demonstração da necessidade de aplicação coerente e homogênea das regras de defesa dos direitos e das liberdades fundamentais das pessoas no que tange a tratamento de dados pessoais.

Um dado importante que o regulamento europeu traz é que a coleta de dados deve ser precedida de informações a serem dadas ao titular. Isso inclui quando ocorrerem compartilhamento ou tiverem sido obtidos a partir de outras fontes. Além disso, o responsável pelo tratamento de dados é obrigado a executar medidas que forem adequadas e eficazes para as atividades e ainda estarem de acordo com o Regulamento.

O que se observa é que o GDPR traz uma fundamentação sólida e bastante detalhada de como promover a segurança dos dados pessoais das pessoas e o porquê. Inclui a descrição de quais instituições devem cumprir e como devem fazer para respeitar esse direito fundamental. O regulamento ressalta, ainda, os riscos que tornam o titular vulnerável, podendo sofrer danos, como fraudes, uso indevido ou venda de dados etc., a partir dessa referida operação.

O texto elenca os danos que os titulares podem sofrer. O considerando nº. 46 apresenta diversos exemplos possíveis, como discriminação, usurpação ou roubo de identidade, perda da confidencialidade dos dados, entre outros. Tais riscos afetam os direitos e liberdades da pessoa singular e devem ser considerados para mensurar a vulnerabilidade da pessoa. Para isso, o regulamento exige que medidas técnicas e organizativas adequadas para atender o regulamento europeu.

⁶⁹ Este regulamento constitui uma medida essencial para reforçar os direitos fundamentais das pessoas na era digital e facilitar a atividade comercial, mediante a clarificação das normas aplicáveis às empresas e aos organismos públicos no mercado único digital. Proteção de Dados na UE. Disponível em: [https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_pt#:~:text=Regulamento%20\(UE\)%202016%2F679,23%20de%20maio%20de%202018](https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_pt#:~:text=Regulamento%20(UE)%202016%2F679,23%20de%20maio%20de%202018). Acesso em: 22 mar 2024.

O Considerando n.º 63, bem como o art. 94 abordam a possibilidade de transferência de dados das instituições e órgãos da União para países terceiros ou para organizações internacionais. Como as demais formas de compartilhamento de dados, esse ponto exige também o cumprimento do regulamento, devendo ser garantido o nível de proteção das pessoas singulares assegurado na União pelo presente regulamento. Ademais, o GDPR ainda prevê sobre transferência para terceiros, admitindo a possibilidade de a Comissão decidir que o país, território ou setor específico de um país ou organização internacional assegurem o nível de proteção de dados. Desse modo, não haverá necessidade de autorização para transferência⁷⁰.

Porém, a respeito de proteção de dados, não poderá a Autoridade Europeia exercer competência, quando o Tribunal estiver no exercício das suas funções jurisdicionais. O Tribunal seguirá o art. 8.º, n.º 3⁷² a título de exemplo, que significa dizer que o cumprimento das regras de proteção de dados ficará sujeito a fiscalização de autoridade independente, e o Tribunal segue um mecanismo interno (ponto 74)⁷³.

Ao abordar o GDPR, importante conectar o trabalho de pesquisa com o cerne que gerou toda a regulamentação que se desenvolveu na União Europeia. Nesse sentido, se faz necessário observar o art. 1.º quanto aos objetivos e objeto e suas considerações:

(1)A proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais, é um direito fundamental. O artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia («Carta») e o artigo 16.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. Este direito é igualmente garantido pelo artigo 8.º da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais.

Nessa primeira consideração refrisa-se um dos maiores valores da União Europeia, pois cita a Carta de Direitos fundamentais da União Europeia, o Tratado sobre funcionamento da União Europeia, todos voltados para a interpretação direcionada à Proteção de dados da pessoa

⁷⁰ Importante ressaltar que os tópicos e fundamentos são todos extraídos do Regulamento, exceto aqueles que são referenciados de outras fontes.

⁷¹ UNIÃO EUROPEIA. Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho relativo a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32018R1725>. Acesso em: 23 mar 2024.

⁷² UNIÃO EUROPEIA. Carta dos Direitos Fundamentais da União Europeia. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em 23 mar 2024.

⁷³ UNIÃO EUROPEIA. Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho relativo a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32018R1725>. Acesso em: 23 mar 2024.

singular. Além disso, afirma a quem é direcionada à aplicação do regulamento, o que se torna importante mencionar que abrange todas as pessoas, independente da nacionalidade, protegendo todas as pessoas que tenham dados pessoais objeto de tratamento.

O GDPR⁷⁴ menciona as transformações tecnológicas. Nas considerações de nº. 16 há a abordagem sobre o desenvolvimento tecnológico, globalização e o compartilhamento de dados nesse novo cenário. E, em vários artigos, o regulamento apresenta a possibilidade dos meios tecnológicos como incidentes de tratamento de dados, demonstrando ser uma normativa adequada a realidade social. Cite-se, como exemplo, o art. 39.

O referido artigo aborda a avaliação de impacto relativa à proteção de dados. Expressa que em sendo realizado o tratamento de dados pessoais realizado por nova tecnologia, antes de o fazer, o responsável deverá realizar uma avaliação do impacto das operações. Além disso, o responsável deve solicitar parecer do encarregado de dados.

Nesse diapasão, importante enfatizar o posicionamento da UE sobre direito ao esquecimento. O considerando nº. 39 relata o direito ao apagamento a ser solicitado pelo interessado e direcionado a quem tornou pública a informação. Nesse quesito, não prevaleceu a mesma interpretação no ordenamento brasileiro, pois a jurisprudência entende que não é compatível com a Constituição de 1988 da República Federativa do Brasil⁷⁵.

Assim, é essencial ressaltar os valores e princípios que regem o regulamento europeu: licitude, transparência, finalidade, adequação, exatidão, limitação da conservação, integridade e confidencialidade e responsabilização. Os valores são privacidade, autonomia, transparência, segurança. Todos esses elementos revelam a robustez desse marco regulatório, e, uma vez que o tratamento dos dados seja realizado seguindo os referidos princípios e valores, atenderá a ética e a legalidade e protegendo os direitos dos indivíduos.

⁷⁴UNIÃO EUROPEIA. Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho relativo a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32018R1725>. Acesso em: 23 mar 2024.

⁷⁵ BRASIL. Superior Tribunal de Justiça. **Direito ao esquecimento não justifica obrigação de excluir notícia de site, decide Terceira Turma**. Disponível em: <https://www.stj.jus.br/sites/portalt/Paginas/Comunicacao/Noticias/08032022-Direito-ao-esquecimento-nao-justifica-obrigacao-de-excluir-noticia-de-site-decide-Terceira-Turma.aspx#:~:text=Direito%20ao%20esquecimento%20incompat%C3%ADvel%20com%20a%20Constitui%C3%A7%C3%A3o&text=Todavia%2C%20a%20ministra%20observou%20que,o%20entendimento%20firmado%20pelo%20STJ..> Acesso em: 15 out 2024.

Portanto, a partir de uma análise sobre o Regulamento Europeu, pode-se compreender o intuito claro sobre objeto tutela da norma, qual seja, o de proteção de dados pessoais da pessoa singular, que encontra fundamento no princípio da dignidade da pessoa humana, nos direitos fundamentais e na liberdade das pessoas. Ressalte-se que o regramento que é direcionado aos Estados-membros da União Europeia, mas como já estudado nessa pesquisa, o regulamento se porta como modelador de normas e assim, tomou proporções influenciando outros países terceiros a UE a regularem o assunto utilizando como parâmetro o GDPR.

Princípio da privacidade e transparência: visão da União Europeia

Para contextualizar o presente tópico na discussão sobre a proposta de pesquisa aqui desenvolvida a respeito da proteção de dados pessoais, se faz necessário compreender como são definidos os princípios de privacidade e transparência como instrumentos basilares para a formulação das normativas referentes ao tema sob a perspectiva da União Europeia.

Foram eleitos especialmente os referidos princípios tanto por serem o cerne da problemática em sociedade sobre proteção dos dados, quanto pelo ponto específico do trabalho que fala sobre processo judicial. Isso porque, deve-se considerar que tais princípios também são relevantes na discussão a respeito do que é público e do que é privativo, transparência e privacidade no curso de um processo judicial.

Aqui os princípios necessitam ser analisados a luz da virtualização dos atos e da realização de audiências por videoconferência nos processos judiciais, ponto central dessa pesquisa. A coexistência dos dois princípios deve acontecer de forma equilibrada, isso porque caso haja a prevalência absoluta de um tem-se a violação do outro. Portanto, o desafio é a ponderação deles, considerando que ambos são importantes para um sistema equânime.

Para isso, é feita uma análise no viés processual, em que há o princípio da publicidade dos atos, sendo esta a regra no âmbito processual, corroborando com o acesso à informação. Já a privacidade é um direito do indivíduo, fundamentado na dignidade da pessoa humana. Desse modo, encontram-se duas regras com aparências antagônicas, o direito à privacidade e o direito à publicidade, quando se discute a disponibilidade dos dados pessoais na realização de audiências remotas. Isso porque, mesmo que os atos sejam públicos, deve-se atentar para segurança da privacidade das informações disponibilizadas em audiências remotas. Isto é, ainda que as audiências devam atender a publicidade, exige-se o rigor legal no tratamento dos dados pessoais coletados em audiência.

Assim, seguindo o raciocínio proposto acerca da visão europeia sobre esses princípios, deve-se considerar que a União Europeia, ao formular as regulamentações, teve como fundamentação principal a dignidade da pessoa humana e os direitos fundamentais do homem. A compreensão sobre o que é privacidade e a importância da proteção a esse direito traz um amplo panorama normativo, condicionando interpretação mais adequada sobre a normativa europeia. Nesse sentido, a doutrina de Cannizzaro⁷⁶ afirma: L'Unione si è dotata di un proprio sistema de interessi e valore fondamentali, fra i quali quelli attinente alla tutela delle libertà e dei diritti individuali⁷⁷. Assim, a União tem seus próprios valores que fundamentam as suas normativas regulatórias.

Para elucidar melhor o significado da privacidade e a correlação com proteção de dados, vale mencionar a fala de Fabrício Mota⁷⁸ que diz: proteção de dados pessoais é a evolução da privacidade. Daí a importância de compreender como a União Europeia interpreta o que é privacidade, pois é fundamento para regulamentação da proteção dos dados. Como o autor Mota afirma, foi só o início sobre valor social que precisava de proteção, criando-se o direito à privacidade.

Ao passo que se fala sobre as primeiras notas do que é privacidade, vale trazer o histórico sobre o seu surgimento. Afirma-se que vem a partir da teoria de juristas americanos Warren e Brandeis em 1891, que criaram a ideia do “direito de ser deixado em paz”. Em suma, na época tratava-se de um direito a ser protegido contra as intrusões sobre a vida pessoal divulgada por jornalistas:

Un altro diritto da prendere sul serio, nel costituzionalismo della società tecnologica, è quello della privacy. Un diritto che nasce come una nuova esigenza di libertà personale. È nota male la pena ricordare l'origine del right to privacy, che venne teorizzato, per la prima volta, in un articolo, così intitolato, scritto da due giuristi statunitensi, Samuel D. Warren e Louis D. Brandeis, e pubblicato sulla Harvard Law Review nel 1891. Si invocava « il diritto di godere della vita, ovvero il diritto di starsene soli (right to be let alone) »: un diritto individuale di libertà da esercitare e tutelare specialmente nei confronti delle intrusioni, allora, della stampa nel riportare al pubblico fatti o elementi strettamente personali, la cui conoscenza avrebbe comportato disdoro e imbarazzo nella persona interessata. “Diritto a essere lasciati soli”, che si riteneva essere stato violato dalla stampa dell'epoca nel dare notizia, con dovizia di particolari, delle sontuose feste che si tenevano nella villa bostoniana di Warren. Non si chiedeva però di esaltare la difesa della solitudine fisica, ma piuttosto di ricondurre la privacy alla tutela dei valori di autonomia e dignità dell'individuo,

⁷⁶ CANNIZZARO, Enzo. Il diritto dell'integrazione europea: l'ordinamento dell'Unione. 2ª ed, Giappichelli, Torino, 2017, p.2.

⁷⁷ Tradução livre: A União dotou-se do seu próprio sistema de interesses e valores fundamentais, incluindo os relativos à proteção das liberdades e dos direitos individuais.

⁷⁸ MOTA, Fabrício. Proteção de dados é a evolução de privacidade. Disponível em: <https://www.serpro.gov.br/lgpd/noticias/protecao-dados-evolucao-privacidade>. Acesso em 17 mar 2024.

che comprendono anche la protezione della sua cerchia familiare e persino di quella societaria, in cui egli ha scelto di collocarsi.

La concezione della privacy si è evoluta nel tempo, non più e non tanto come “diritto a essere lasciati soli”, e quindi una forma passiva di tutela, ma piuttosto anche come “diritto a disporre dei propri dati”, assumendo pertanto una forma attiva di partecipazione informativa⁷⁹⁸⁰.

Ainda sobre o histórico do desenvolvimento da privacidade, vale tecer algumas notas de Rodotà que em sua obra *Tecnologie e Diritti* faz um apanhado do que era o entendimento de ser privativo, e não ser coletivo. Ele diz que para compreender o que é, não se atendo apenas a questões biológicas do direito em uma esfera reservada, é fundamental entender o contexto socioeconômico em que se desenvolveu e amadureceu a privacidade:

Per comprendere questa vicenda, più che insistere sui dati naturalistici relativi alla necessità biologica di una sfera riservata, è opportuno ricordare il contesto socio-economico in cui sono maturate le condizioni che hanno poi consentito l’affermarsi della privacy come esigenza bisognosa di autonoma tutela⁸¹⁸².

Ele explica que a privacidade começou na era medieval, quando se iniciou a desenvolver o senso de intimidade. O isolamento era um privilégio de poucos, como o de monges, pastores, de acordo com as palavras do professor. Por isso, estabelecer a intimidade, naquela época, havia

⁷⁹ FROSINI, Tommaso Edoardo et al. Il costituzionalismo nella società tecnologica. **Giurcost. org, Liber Amicorum per Pasquale Costanzo**, v. 25, 2020. Il costituzionalismo nella società tecnologica. Disponível em: <https://dirittodiinternet.it/wp-content/uploads/2021/12/afro.pdf>. Acesso em 17 mar 2024.

⁸⁰ Tradução livre: Outro direito a ser levado a sério, no constitucionalismo da sociedade tecnológica, é o da privacidade. Um direito que nasceu como uma nova necessidade de liberdade pessoal. É bem conhecido, mas vale a pena lembrar a origem do direito à privacidade, que foi teorizado pela primeira vez num artigo, assim intitulado, escrito por dois juristas americanos, Samuel D. Warren e Louis D. Brandeis, e publicado em Harvard Law Review em 1891. Invocou "o direito de aproveitar a vida, ou o direito de ser deixado em paz": um direito individual de liberdade a ser exercido e protegido especialmente contra as intrusões, então, da imprensa em reportar ao público estritamente factos ou elementos pessoais cujo conhecimento teria trazido vergonha e constrangimento ao interessado.

“Direito de ser deixado em paz”, que se acreditava ter sido violado pela imprensa da época ao relatar, detalhadamente, as suntuosas festas realizadas na villa de Warren em Boston. No entanto, não pedíamos para exaltar a defesa da solidão física, mas sim para devolver a privacidade à protecção dos valores da autonomia e da dignidade do indivíduo, que incluem também a protecção do seu círculo familiar e mesmo da sociedade. , em que ele escolheu colocar.

O conceito de privacidade evoluiu ao longo do tempo, já não e tanto como o “direito de ser deixado em paz”, e portanto uma forma passiva de protecção, mas também como o “direito de dispor dos próprios dados”, assumindo assim uma forma ativa de participação informativa

⁸¹ RODOTÀ, Stefano. *Tecnologie e diritti*, Bologna, Il Mulino, 2021(ed. digit.: 2021, doi: 10.978.8815/367778, Capítulo primo: La privacy tra individuo e collettività, pp. 23-41, doi capitolo: 10.1401/9788815367778/c1). Disponível em: <https://www.darwinbooks.it/doi/10.978.8815/367778/page/28>. Acervo Biblioteca UNIPI. Acesso em: 26 mar 2024

⁸² Tradução livre: Para compreender esta história, em vez de insistir nos dados naturalistas relativos à necessidade biológica de uma esfera privada, é apropriado lembrar o contexto socioeconômico em que se desenvolveram as condições que permitiram então a emergência da privacidade como uma necessidade que necessita de protecção autónoma.

relação com as condições materiais que pudessem proporcionar esse limite. Ele explica, desse modo, que o direito à privacidade não surge como um direito “natural”, era um privilégio. Inclusive ele diz que estabelecer o “direito de ser deixado em paz” para os trabalhadores pode ter aspecto negativo, pois implicaria abandono dos mais fracos.

O estudioso relata ainda que é importante considerar a cultura global de cada grupo de burguesia. Ao referir-se a Warren e Brandeis (os quais ele denomina “pais fundadores”), ele explica que ambos tinham posicionamentos diferentes. O primeiro direcionado a proteger os interesses da burguesia, o segundo, mesmo que preocupado com a classe burguesa também demonstrava inquietação com as minorias, pois elas poderiam ocasionar impopularidade. Ele afirma, inclusive, que tal característica pode ser encontrada atualmente.

É importante trazer a seguinte observação do referido professor:

(...)pubblicità e controllo non sono termini contraddittori, come pubblicità e segreto. Proprio là dove si ammette la massima circolazione delle informazioni a contenuto economico, si deve consentire agli interessati di esercitare un reale potere di controllo sulla esattezza di tali informazioni, sui soggetti che le adoperano, sulle modalità della loro utilizzazione⁸³⁸⁴.

Em sua obra *Riservatezza*, diz que essa expressão, que dá nome ao livro, entra no vocabulário jurídico, primeiro com os estudiosos e depois com a jurisprudência. Na legislação, ele faz referência ao direito do trabalhador e sobre o âmbito penal. Aborda a vida privada que tem o sentido de *Riservatezza*. Mas o reconhecimento legislativo se dá com o estatuto dos trabalhadores, que vetava perguntas sobre opiniões políticas, religiosas e sindicais.

La norma più significativa, tuttavia, è contenuta nell’art. 8, che vieta le indagini sulle opinioni politiche, religiose e sindacali dei lavoratori, individuando così una categoria di dati personali che, insieme ad Altri, saranno poi qualificati “sensibili”(…) ⁸⁵⁸⁶

Interessante quando o professor Rodotà aborda o novo conceito de privacidade. Ele explica que não se refere mais ao direito de ser deixado só. Ele explica que se vive a Sociedade

⁸³ RODOTÀ, Stefano. *Tecnologie e diritti*, Bologna, Il Mulino, 2021(ed. digit.: 2021, doi: 10.978.8815/367778, Capitolo primo: La privacy tra individuo e collettività, pp. 23-41, doi capitolo: 10.1401/9788815367778/c1). Disponível em: <https://www.darwinbooks.it/doi/10.978.8815/367778/page/28>. Acervo Biblioteca UNIPI. Acesso em: 26 mar 2024, p. 36.

⁸⁴ Tradução livre: publicidade e controle não são termos contraditórios, como publicidade e sigilo. Precisamente onde é permitida a circulação máxima de informação com conteúdo econômico, os interessados devem poder exercer um poder real de controle sobre a veracidade dessa informação, sobre os sujeitos que a utilizam, sobre os métodos da sua utilização.

⁸⁵ RODOTÀ, Stefano. *Riservatezza*. 10ª edição. Treccani, 2023, p. 69-70.

⁸⁶ Tradução livre: A regra mais significativa, porém, está contida no art. 8º, que proíbe a investigação de opiniões políticas, religiosas e sindicais dos trabalhadores, identificando assim uma categoria de dados pessoais que, juntamente com Outros, serão então classificados como “sensíveis”(…)

da Informação e falar sobre privacidade é dizer que a pessoa conhece, controla, interrompe o fluxo de seus dados. O conceito está mais próximo do direito de manter controle sobre suas próprias informações.

Nella società dell'informazione tendono a prevalere modi, fanno riferimento alla possibilità di un soggetto di conoscere, controllare, indirizzare, interrompere il flusso delle informazioni che lo riguardano. La privacy, quindi, può essere più precisamente definita, in una prima approssimazione, come il diritto di mantenere il controllo sulle proprie informazioni⁸⁷⁸⁸.

Interessante posicionamento do professor Rodotà quando, em seu livro, aborda a privacidade versus publicidade. Ele afirma que a privacidade é um direito fundamental, direito de autodeterminação informativa. Ele compreende que a era tecnológica transformou as relações, mas afirma que se trata de cidadania e que não pode se resumir a regulamentação e questões contratuais.

Così cambia profondamente la funzione sociopolitica della privacy, che si proietta ben al di là della sfera privata, per divenire elemento costitutivo della cittadinanza. Ma a questo significa purè che la misura sociale della privacy non può essere determinata con riferimento a criteri settoriali, come quelli tratti, per esempio, dall'universo del consumo. La privacy, allora, s'impone come diritto fondamentale; si especifica come diritto all'autodeterminazione informativa e, più precisamente, come diritto a determinar le modalità di costruzione della sfera privata nella loro totalità; si presenta, infine, come preconditione della cittadinanza dell'età elettronica e, in quanto tale, non può essere affidata unicamente alla logica dell'autoregolamentazione o ai rapporti contrattuali⁸⁹⁹⁰.

No mesmo sentido Doneda⁹¹ estabelece que foi modificado o entendimento do que é privacidade. O que antes era o “direito de ser deixado só”, hoje, privacidade tem um perfil de outra ordem, relacionada a informação pessoal e condicionada a tecnologia. O conceituado jurista afirma também que proteção de dados, ainda que vinculado a privacidade, se sofisticou e tem características próprias. A partir de seu pensamento, pode-se compreender que

⁸⁷ RODOTÀ, Stefano. *Riservatezza*. 10ª edição. Treccani, 2023, p. 69-70.

⁸⁸ Tradução livre: Na sociedade da informação os modos tendem a prevalecer, referem-se à possibilidade de um sujeito conhecer, controlar, dirigir, interromper o fluxo de informações que lhe dizem respeito. A privacidade, portanto, pode ser definida com mais precisão, numa primeira aproximação, como o direito de manter o controle sobre as próprias informações.

⁸⁹ RODOTÀ, Stefano. *Riservatezza*. 10ª edição. Treccani, 2023, p. 101.

⁹⁰ Tradução livre: Assim, a função sociopolítica da privacidade muda profundamente, estendendo-se para além da esfera privada para se tornar um elemento constitutivo da cidadania. Mas isto também significa que a medida social da privacidade não pode ser determinada com referência a critérios sectoriais, como os extraídos, por exemplo, do universo de consumo. A privacidade, então, impõe-se como direito fundamental; especifica-se como o direito à autodeterminação informativa e, mais precisamente, como o direito de determinar os métodos de construção da esfera privada na sua totalidade; por último, apresenta-se como uma condição prévia da cidadania da era electrónica e, como tal, não pode ser confiada apenas à lógica da auto-regulação ou das relações contratuais.

⁹¹ DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*. 3ª edição. Revista dos Tribunais, 2021, p. 23-24.

privacidade é algo maior e que, além de estar voltada para um momento diverso de quando foi criada, tem desdobramentos importantes. Está associada a liberdade de escolha entre outros direitos. Assim, compreender privacidade permite uma interpretação mais adequada sobre proteção de dados.

Uma questão de relevância sobre privacidade e publicidade é o direito ao esquecimento, comentado no tópico anterior quando falado sobre o teor do GDPR. Trata-se de um desdobramento do direito à privacidade. Antonello Soro faz uma boa reflexão sobre a necessidade da publicidade, quando é informação, e a desvinculação de dados em relação à pessoa e o respeito à dignidade. Ele faz ponderações a respeito do direito do esquecimento. Há sim uma revolução da privacidade, mas cita os limites, transparência, navegação on-line e inteligência artificial⁹².

Nesse sentido, o cerne do que é privacidade foi mantido. Isso quer dizer que a União Europeia aborda esse direito sob a ótica de direito fundamental. Observando que a Carta dos Direitos Fundamentais da União Europeia elenca, em seu art. 7º, o respeito à vida privada e familiar, pode-se aduzir que os documentos seguintes têm o sentido de proteção com base no direito fundamental. Esse direito abrange o domicílio e às comunicações. Além disso, a Carta fala também sobre proteção de dados.

A respeito do posicionamento do Parlamento Europeu quando foi elaborada a Diretiva 2002/58/CE que discorreu sobre o tratamento dos dados pessoais e a tutela da vida privada na área de comunicação eletrônica. Tal diretiva deixa expresso que adere aos princípios reconhecidos pela Carta dos Direitos Fundamentais da União Europeia, especificando os artigos 7º e 8º do documento:

(2) La presente direttiva mira a rispettare i diritti fondamentali e si attiene ai principi riconosciuti in particolare dalla Carta dei diritti fondamentali dell'Unione europea. In particolare, la presente direttiva mira a garantire il pieno rispetto dei diritti di cui agli articoli 7 e 8 di tale Carta⁹³⁹⁴.

⁹² SORO, Antonello. *Là libertà e il suo limite. Una riflessione sul diritto alla privacy a partire dalla sentenza Roe v. Wade*. Disponível em: <https://www.giustiziainsieme.it/it/diritto-e-innovazione/2396-la-liberta-e-il-suo-limite-una-riflessione-sul-diritto-alla-privacy-a-partire-dalla-sentenza-roe-v-wade>. Acesso em: 30 mar 2024.

⁹³ UNIÃO EUROPEIA. **Diretiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)**. Disponível em: <https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A32002L0058>. Acesso em: 06 jul 2024.

⁹⁴ Tradução livre: (2) A presente diretiva visa respeitar os direitos fundamentais e obedece aos princípios reconhecidos, nomeadamente, pela Carta dos Direitos Fundamentais da União Europeia. Em particular, a presente diretiva visa garantir o pleno respeito pelos direitos referidos nos artigos 7.º e 8.º da referida Carta

Outro importante documento, já mencionado, mas que precisa ser reafirmado nesse tópico, agora tratando sobre a temática do que é privacidade, é a Convenção 108 e que se tornou 108+⁹⁵, que também traz esse assunto como um de seus princípios. Nesse ponto, expõe sobre a privacidade no espaço digital. Assim, retrata sobre proteção de todas as pessoas, independente da nacionalidade ou residência, no que concerne aos dados pessoais, respeitando assim os direitos humanos e liberdades fundamentais e a vida privada.

Sobre o entendimento acerca de privacidade, a jurisprudência do Tribunal Europeu referiu-se ao conceito de dados pessoais usado na Convenção nº. 108. A partir do *informativo/ficha temática*, pode-se observar exemplos de medidas dos Estados membros quando da execução de sentenças em várias situações que envolvem tratamento de dados pessoais. O Conselho Geral do Judiciário, em relatório, sinalizou que os tribunais domésticos têm obrigação de equilibrar adequadamente os direitos e interesses constitucionais das partes envolvidas, de um lado as garantias processuais e do outro a privacidade. Como consta no *informativo/ficha temático*:

In 2019, the Court's judgment was analysed by the General Judiciary Council in a report underlining that domestic courts have the obligation to adequately balance the constitutional rights and interests of the parties concerned (on the one hand, the right to judicial protection and defence, procedural safeguards linked to the principle of transparency and the need to reason decisions and resolutions and, on the other hand, the right to privacy and the protection of personal data (requiring that the inclusion of identifying data (or their anonymization) be reasoned with regard to its legal purpose and proportionality.) Specific training sessions in this respect were organised at the Academy of Judicial Training⁹⁶⁹⁷.

Nesse trecho fica evidenciada a necessidade de haver o equilíbrio entre a transparência, conforme fundamentação das decisões e o respeito à privacidade e à proteção de dados pessoais. Além disso, informa que sessões de treinamento específicas sobre esse assunto foram

⁹⁵ Convenção 108+. Disponível em: <https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2>. Acesso em 17 mar 2024.

⁹⁶ UNIÃO EUROPEIA. Council of Europe. Department for the Execution of judgments of the European Court of Human Rights. DG1. Thematic Factsheet. September 2022. Disponível em: <https://rm.coe.int/tfs-personal-data-protection-eng/1680a811ea>. Acesso em: 08 jul 2024.

⁹⁷ Tradução livre: Em 2019, o acórdão do Tribunal foi analisado pelo Conselho Geral da Magistratura num relatório que sublinha que os tribunais nacionais têm a obrigação de equilibrar adequadamente os direitos e interesses constitucionais das partes envolvidas (por um lado, o direito à protecção e defesa judicial, direitos processuais salvaguardas ligadas ao princípio da transparência e à necessidade de fundamentar decisões e resoluções e, por outro lado, o direito à privacidade e à protecção dos dados pessoais (exigindo que a inclusão de dados identificativos (ou a sua anonimização) seja fundamentada no que diz respeito sua finalidade legal e proporcionalidade.) Foram organizadas sessões de formação específicas a este respeito na Academia de Formação Judiciária.

organizadas na Academia de formação judicial (Department for the execution of judgments of the European Court of Human Rights).

O GDPR traz considerações importantes em matéria judiciária. Aborda a Diretiva da União Europeia 2016/680. Fala sobre a necessidade de proteção e livre circulação dos dados pessoais tratados em processos judiciais quando tratem de temas como investigação, execuções penais, segurança pública, a fim de o nível de proteção sem interferir no intercâmbio de dados entre os órgãos e organismos da União. Importante mencionar que o ponto 12 afirma que o regulamento não se aplica à Procuradoria Europeia e nem Europol até que os atos normativos que as criaram estejam adaptados com o regulamento⁹⁸.

A análise sobre a abordagem em matéria judiciária nessa pesquisa é relevante tendo em vista que este trabalho se propõe a discutir a coleta e o tratamento de dados pessoais pelo judiciário durante a realização das audiências remotas. Dessa forma, se justifica trazer a visão do regulamento europeu sobre a regulamentação da atividade judicial em matéria de proteção de dados.

Outra questão de relevância que está também na introdução do Regulamento é o ponto 22. Parte do texto vale ser transcrito para análise:

Para que o tratamento seja lícito, os dados pessoais deverão ser tratados com base na necessidade de desempenho de uma função efetuada no interesse público pelas instituições e pelos órgãos da União, ou no exercício da sua autoridade pública, na necessidade de conformidade com uma obrigação jurídica a que o responsável pelo tratamento dos dados esteja sujeito, ou com outra base legítima, ao abrigo do presente regulamento, incluindo o consentimento do titular dos dados em causa, a necessidade de executar um contrato no qual o titular dos dados seja parte, ou para adotar medidas pré-contratuais a pedido do titular dos dados. O tratamento de dados pessoais para o desempenho de funções de interesse público pelas instituições e pelos órgãos da União inclui o tratamento de dados pessoais necessários à gestão e ao funcionamento dessas instituições e órgãos (...).

O armazenamento das gravações decorrentes das audiências pode ser considerado interesse público, trata-se da atividade do judiciário e os atos são praticados pela autoridade competente durante o exercício da função e em conformidade com a obrigação jurídica. Trata-se de dados necessários à gestão, funcionamento do órgão e exercício jurisdicional. Dessa forma, percebe-se o embasamento fundamentado no Regulamento que esclarece a utilização

⁹⁸ UNIÃO EUROPEIA. Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho relativo a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32018R1725>. Acesso em: 23 mar 2024.

dessas informações em suas atividades (o que se pode aduzir estarem incluídas as gravações das audiências).

Por sua vez, o tópico 21 do Regulamento faz uma observação importante que pode ser referenciada para essa discussão: As operações de tratamento posteriores para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos deverão ser consideradas como operações de tratamento lícito compatível. Aqui a fundamentação também é baseada em interesse público. Observe-se que é falado em arquivo de dados, podendo ser feita analogia ao arquivamento das gravações.

(tópico 33) O tratamento de dados pessoais para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos deverá ficar sujeito a garantias adequadas no que respeita aos direitos e às liberdades do titular dos dados, nos termos do presente regulamento. Essas garantias deverão assegurar a existência de medidas técnicas e organizativas que assegurem, nomeadamente, o princípio da minimização dos dados.

O ponto 35 do GDPR fala assertivamente sobre o princípio da transparência: “Os princípios do tratamento leal e transparente exigem que o titular dos dados seja informado da operação de tratamento de dados e das suas finalidades”. Com esse trecho pode-se compreender que o judiciário, em suas atividades, deve prestar esclarecimentos aos titulares dos dados, quando realiza a coleta das informações pessoais envolvidas nas audiências remotas. Isso inclui também explicar como serão mantidos, o porquê que se faz necessário coletar e a quem o titular deve se dirigir quando precisar alterar essas informações pessoais.

Emanuela Concilio analisa posicionamento jurisdicional sobre privacidade e publicidade. Em caso específico, ela traz em seu texto, explicando a fundamentação judicial, que não é o simples pedido de ocultação de dados que justifica a não identificação. Deve haver ponderação. A publicidade judicial é uma regra. A lei traz as exceções. É necessário um equilíbrio entre os valores opostos a publicidade. Os casos que devem ser considerados são aqueles que visam a protegerem os interesses sensíveis das pessoas⁹⁹.

A abordagem da estudiosa faz refletir sobre a possibilidade de ocultação, todavia ressalta que não é qualquer dado que permite essa atividade. A ponderação dos princípios é um desafio para o operador do direito, pois a publicidade é uma forma de segurança jurídica e a privacidade é um direito fundamental. O equilíbrio dos princípios precisa ser feito de forma amadurecida sem colocar em riscos o titular das informações.

⁹⁹ CONCILIO, Emanuela. Atti Giudiziari e tutela dei dati personali (nota a TAR Lazio, Sez. III, 1º febbraio 2021, n. 579. Disponível em: <https://www.giustiziainsieme.it/it/diritto-e-processo-amministrativo/1641-atti-giudiziari-e-tutela-dei-dati-personali-nota-a-tar-lazio-sez-iii-1-febbraio-2021-n-580>. Acesso em: 30 mar 2024.

Bonfanti comenta que a União Europeia, através da Diretiva 2016/680, Convenção Europeia de Direitos Humanos permitem restrição à privacidade e proteção de dados nos casos de segurança pública. Esse assunto está associado a temática de proteção de dados porque refere-se à restrição ao direito à privacidade que é um direito fundamentalmente protegido.

Entretanto, é importante citar que em matéria de segurança pública o direito à privacidade não é absoluto. Por isso, é importante falar sobre a atividade desenvolvida pela administração pública no que diz respeito ao judiciário que também pode estar relacionada com a segurança pública e, por isso, a privacidade pode sofrer restrição.

La direttiva 2016/680, il GDPR⁴³ e la Convenzione europea dei diritti dell'uomo ("CEDU") legittimano restrizioni del diritto alla privacy e della protezione dei dati personali per esigenze di sicurezza pubblica.⁴⁴ Per quanto concerne la CEDU, il suo art. 8, par. 2, stabilisce l'illegittimità dell'ingerenza delle autorità pubbliche nel diritto alla privacy salvo che essa «sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui»¹⁰⁰¹⁰¹.

Admite-se, portanto, restrição a privacidade e a proteção de dados quando previsto em lei e estiver ligado a segurança nacional, segurança pública, bem-estar econômico do país, à defesa da ordem e à prevenção de delitos, à proteção à saúde ou da moral, ou a proteção dos direitos e liberdade de terceiros. Temas amplos e que exigem análise com interpretação de caso concreto.

Ainda sob a perspectiva da União Europeia sobre o que venha a ser privacidade versus o que pode ser acessível, é importante analisar as decisões da Corte que citam os referidos princípios. Considerando que os julgamentos são prolatados em consonância com o entendimento que veio se consolidando ao longo do desenvolvimento das normativas, estudar as fundamentações das decisões traz uma melhor compreensão da organização Europeia sobre como são interpretados os princípios à luz do ordenamento europeu.

A esse respeito, Bonfanti cita duas decisões importantes, que antecedem o regulamento europeu, mas que mostram a perspectiva sobre privacidade que já era estabelecida a época.

¹⁰⁰ BONFANTI, Angelica. Big Data e polizia predittiva: riflessione in tema di protezione del diritto alla privacy e dei dati personali. Disponível em: <https://hdl.handle.net/2434/605891>. Acesso em: 31 mar 2024.

¹⁰¹ Tradução livre: A Diretiva 2016/680, o RGPD⁴³ e a Convenção Europeia dos Direitos Humanos ("CEDH") legitimam restrições ao direito à privacidade e à proteção de dados pessoais para necessidades de segurança pública.⁴⁴ No que diz respeito à CEDH, o seu art. 8, par. 2º, estabelece a ilegitimidade da interferência das autoridades públicas no direito à privacidade, a menos que "esteja prevista em lei e constitua uma medida que, numa sociedade democrática, seja necessária à segurança nacional, à segurança pública, ao bem-estar econômico do país, a defesa da ordem e a prevenção do crime, a proteção da saúde ou da moral, ou a proteção dos direitos e liberdades de terceiros".

Aborda as sentenças Digital Rights e Tele2 Sverige. Sobre a sentença Digital Rights, a decisão se baseia na Diretiva 2006/24. A diretiva autoriza que provedores de internet armazenem e conservem dados de usuários por um certo tempo, bem como autoriza o acesso por parte de autoridades nacionais.

Entretanto, não apresenta critérios para limitar o acesso. Não há limites sobre o número de pessoas com acesso ou uso dos dados, frente ao objetivo a que se proponha. Isso é inválido, pois permite uma vasta amplitude de acesso a direitos garantidos nos art. 7 e 8 da Carta de Direitos Fundamentais da União Europeia (que abordam a proteção da vida privada e familiar, bem como a proteção de dados). A corte entende pela proporcionalidade e necessidade, observando os direitos individuais¹⁰².

Pertanto occorre che siano previste regole chiare e precise che disciplinino l'applicazione delle misure e impongano garanzie sufficienti contro il rischio di abusi, accessi e usi illeciti ai danni dei titolari dei dati¹⁰³. No Mesmo sentido foi a sentença Tele2 Sverige, que a conservação que ultrapassa os limites do estritamente necessário não se justifica em uma democracia¹⁰⁴.

Sobre esse debate a respeito de privacidade e publicidade, vale mencionar o direito ao esquecimento já julgado pela Corte e já citado ao comentar o GDPR. O direito ao esquecimento pode ser um desdobramento da privacidade. Há embate entre o direito ao acesso à informação processual, envolvendo questões sociais, e o direito do cidadão de recomeçar depois de ter cumprido o determinado em sentença e não querer mais seu nome associado a um determinado fato, por exemplo¹⁰⁵.

Assim, nesse sentido, de acordo com o professor Doneda¹⁰⁶, hoje, surge uma nova conotação sobre privacidade. Dessa forma, ele afirma que se manifesta sobre proteção de dados, mas não apenas sobre esta. Sai do aspecto individualista e passa a reverberar em outros

¹⁰² BONFANTI, Angelica. Big Data e polizia predittiva: riflessione in tema di protezione del diritto alla privacy e dei dati personali. Disponível em: <https://hdl.handle.net/2434/605891>. Acesso em: 31 mar 2024.

¹⁰³ Tradução livre: Portanto, são necessárias regras claras e precisas que regulem a aplicação das medidas e imponham garantias suficientes contra o risco de abuso, acesso e utilização ilícita em detrimento dos titulares dos dados.

¹⁰⁴ BONFANTI, Angelica. Big Data e polizia predittiva: riflessione in tema di protezione del diritto alla privacy e dei dati personali. Disponível em: <https://hdl.handle.net/2434/605891>. Acesso em: 31 mar 2024.

¹⁰⁵ TIGRINO, Andrea. Procedimento Penale e diffusione dei dati personali. Stato dell'arte e quesiti posti dalla riforma Cartabia. Rivista di Diritto dei Media. Disponível em: <https://www.medialaws.eu/rivista/procedimento-penale-e-diffusione-dei-dati-personali-stato-dellarte-e-quesiti-posti-dalla-riforma-cartabia/>. Acesso em 01 mar 2024.

¹⁰⁶ DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. 3ª edição. Revista dos Tribunais, 2021, p.46-47.

interesses ligados a personalidade e liberdades fundamentais, passando a englobar estudos da própria personalidade com o mundo exterior.

No que tange a transparência, trata-se de um dos princípios fundamentais da União Europeia. Está associado a divulgação de informações sobre políticas e despesas, bem como a liberdade da informação. São princípios consagrados no Tratado da União Europeia e no Tratado sobre o funcionamento da União Europeia.

A transparência é um dos princípios fundamentais da UE. Exige que a UE divulgue informações sobre as suas políticas e despesas e que defenda o princípio da liberdade de informação. Estes princípios estão consagrados nos Tratados da UE.

O artigo 10.º do [Tratado da União Europeia](#) estipula que «as decisões são tomadas de forma tão aberta e tão próxima dos cidadãos quanto possível». O artigo 11.º especifica que as instituições devem dar aos cidadãos e às associações representativas a possibilidade de expressarem e partilharem publicamente os seus pontos de vista sobre todos os domínios de ação da União.

O [Tratado sobre o Funcionamento da União Europeia](#) aprofunda estes pontos. Determina que as instituições da UE são obrigadas a agir publicamente e que todos os cidadãos e todas as pessoas singulares ou coletivas que residam ou tenham a sua sede estatutária num Estado-Membro têm direito de acesso aos documentos (artigo 15.º).

Em termos práticos, isto significa que é seu direito a aceder a documentos das instituições, dos organismos e das agências da UE, incluindo textos legislativos, documentos oficiais, atas de reuniões e ordens de trabalhos. Siga as ligações desta página para aceder às bases de dados e registos públicos dos órgãos da UE, onde pode obter documentos diretamente em linha ou mediante pedido¹⁰⁷.

No que diz respeito ao acesso a documentos, são publicados calendários sobre reuniões dos órgãos da União Europeia para que possam ser acompanhados por acesso aos sítios. Além disso, é possível acesso a publicações da UE, incluindo o sítio de Portal de dados abertos.

Sobre acesso do público aos documentos do Provedor de Justiça Europeu:

A transparência e a responsabilização perante o público são prioridades fundamentais que o Provedor de Justiça Europeu procura promover na administração da UE e que orientam igualmente o trabalho do Gabinete do Provedor de Justiça Europeu.

Nos termos do Tratado sobre o Funcionamento da União Europeia (artigo 15.º), os cidadãos e as pessoas coletivas residentes na UE têm o [direito de acesso aos documentos](#) de quase todas as instituições da UE. Trata-se também de um direito fundamental reconhecido na [Carta dos Direitos Fundamentais da UE](#) (artigo 42.º). O direito de acesso aplica-se a documentos escritos (físicos e eletrónicos) e a registos áudio/audiovisuais relacionados com políticas, atividades ou decisões das instituições da UE.

De acordo com as regras da UE em matéria de acesso do público aos documentos ([Regulamento \(CE\) n.º 1049/2001](#)), os cidadãos podem contactar as instituições para solicitar o acesso a documentos específicos (caso tenham conhecimento da sua existência) ou solicitar à instituição que identifique documentos sobre um assunto

¹⁰⁷ UNIÃO EUROPEIA. Acesso à informação. Disponível em: https://european-union.europa.eu/principles-countries-history/principles-and-values/access-information_pt. Acesso em: 08 jul 2024.

específico a que queiram ter acesso. As instituições apenas podem recusar o acesso em circunstâncias excepcionais, caso a divulgação de documentos possa prejudicar os interesses enunciados no Regulamento (CE) n.º 1049/2001¹⁰⁸.

Observa-se que é dada considerável importância ao princípio da transparência no que diz respeito ao acesso à informação na União Europeia. Os sítios eletrônicos trazem desdobramentos com mais detalhes, sinalizam as várias formas de acesso e aos tipos de informações que podem ser feitos. Isso demonstra que, do ponto de vista institucional, a sinalização é de que as informações públicas devem ser disponibilizadas em conformidade com o permitido em lei.

Portanto, debater sobre privacidade, especialmente, é algo complexo e difícil. Além disso, equilibrar esse direito, que hoje está em um outro contexto, com a publicidade, o acesso à informação, torna um grande desafio para o direito. Assim, é necessário buscar desenvolver um trabalho que se enquadre adequadamente atendendo aos preceitos legais sem que haja a violação do direito fundamental. É importante que o tratamento dos dados no ambiente processual esteja adequado à regulamentação pertinente e que os seus titulares estejam informados acerca da destinação de seus dados.

Regulamentações e normativas referentes à privacidade e proteção de dados a partir do GDPR e da LGPD pela Itália e Brasil

Aspectos Gerais

Como observado, a partir do panorama aqui apresentado, observou-se que a influência do texto do Regulamento Europeu ocorre de forma espontânea em outras nações, funcionando como o *modelador de normas*. Isto é, considerando a soberania de cada país, não há dever de obediência de nenhuma nação ao que a União Europeia preceitua. Desse modo, importante afirmar que não há uma obrigatoriedade a ser seguida pelos demais países que não componham a União Europeia. O que ocorre é um espelhamento voluntário utilizado por outros países.

¹⁰⁸ UNIÃO EUROPEIA. European Ombudsman. Acesso Público aos documentos do Provedor de Justiça Europeu. 16/11/2020. Disponível em: <https://www.ombudsman.europa.eu/en/office/publicregister/pt>. Acesso em: 08 jul 2024.

Após a análise sobre o desenvolvimento do Regulamento Europeu, considerando o aspecto histórico da proteção de dados, mas mostrando a construção normativa até chegar à regulamentação que hoje está vigente, dá-se continuidade ao estudo sobre o arcabouço normativo da Itália e do Brasil. Assim, o raciocínio jurídico aqui construído, seguindo a linha designada nesse trabalho, tem como proposta, no presente capítulo, estudar os regulamentos europeu e brasileiro e compreender como cada país vem abordando o tema de proteção de dados e a relação tecnológica em seu território. Fala-se sobre a relação tecnológica porque inevitavelmente há fluxo de dados nessa atividade.

O estudo é direcionado partindo do conteúdo geral para o específico, chegando às leis, regulamentações e regras que regulam o trabalho do judiciário quando da utilização de tecnologia em processo judicial. Assim, busca-se identificar se há normas que normatizem as atividades cotidianas do judiciário, em especial na seara processual e especificamente sobre a realização de audiências remotas. O intuito é identificar se há normas que abordem esse ato judicial.

Isto posto, é examinado e disponibilizado um conteúdo contributivo para compreensão sobre a problemática que envolve toda a sociedade quanto a privacidade e a proteção de dados quando do trabalho do Poder Judiciário em audiências remotas. Dessa forma, estudar os regulamentos e a relação que se desenvolve entre as nações sobre esse tema pode trazer frutos para os próximos estudos e investimentos em relação à privacidade, proporcionando melhor cenário no âmbito internacional.

O presente capítulo pretende analisar as normativas posteriores a regulamentação geral de cada país sobre o tema. Mas antes disso, é importante mencionar a relação sobre proteção de dados da Itália e o contexto Europeu. Isso porque, antes de haver a regulamentação europeia, a Itália já continha um Código de Proteção de Dados, como já referenciado no primeiro capítulo, demonstrando quase um pioneirismo europeu, ao menos italiano.

Assim, delimita-se a pesquisa a estes países por questões metodológicas, mas não há a pretensão de desconsiderar a importância de outras regulamentações em outros países, pois proteção de dados não é apenas uma preocupação local da Itália e do Brasil. Podendo haver uma extensão de estudo para outros países, posteriormente, para tantos quantos forem necessários. É significativo entender como cada país regulamenta o tema e cumpre as exigências legais.

Além disso, a escolha da Itália se dá pelas suas referências normativas e similaridades de sistemas com Brasil. Há de se considerar o legado normativo que a Itália traz para vários países, inclusive o Brasil, ainda que cada nação siga o seu curso normativo independente. Assim, há relevância em estudar o arcabouço normativo italiano que traz um aspecto contributivo a respeito da interpretação dos textos das suas respectivas leis. Analisar onde tudo começou traz propriedade para o desenvolvimento do progresso na adequação legislativa.

Além disso, a criação de entidade regulatória é de origem do direito italiano, como preceituam Lima e Monteiro:

A criação de entidade regulatória autônoma no âmbito da proteção de dados pessoais é natural em legislações alienígenas, tendo por origem o Direito Italiano. A Europa detém entidades nacionais e supranacionais que têm por função primordial a conformidade das leis estatais que introduzem em seus territórios as Diretivas da Comunidade¹⁰⁹.

Dessa forma, compreender acerca da construção de conceitos e normas amplia os horizontes para melhorar o conhecimento da privacidade e dados pessoais, que são propostas no trabalho. É saliente-se que se trata de um tema extraterritorial, e, portanto, envolve todos os países, tornando um tema central global. A proposta é analisar em separado, como cada país está trabalhando com a sua legislação. Aqui analisa-se a Itália, sob a égide do GDPR e o Brasil sob égide da LGPD, sobre como cada um vêm buscando o cumprimento das suas respectivas exigências normativas.

Esse estudo permitirá compreender o que se entende por privacidade e proteção de dados em um cenário extraterritorial, considerando as comunicações que se estabelecem no ciberespaço. Ciberespaço¹¹⁰ é o ambiente virtual e digital e interconectado em todo mundo, onde acontece interação social, conexão de coisas e fluxo de dados e informações.

Considerando que o ciberespaço é o espaço para a realização das audiências remotas, essa análise deve ser avaliada sob a perspectiva das operações feitas ao realizá-las e, consequentemente, ao armazenar as gravações, pois essas mídias encontram-se na internet, no ciberespaço. Tendo em vista que o GDPR estabelece normas vinculativas e de aplicação imediata em todos os países da União, as soluções adotadas pela Itália e em outros países Europeus podem estar no mesmo nível normativo.

¹⁰⁹ LIMA, Caio Cesar Carvalho; MONTEIRO, Renato Leite. Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada. **AtoZ: novas práticas em informação e conhecimento**, v. 2, n. 1, p. 60-76, 2013.

¹¹⁰ LÉVY, Pierre. LÉVY, Pierre. Cíbercultura. Tradução Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

A Itália iniciou a regulamentação sobre o tema com a lei 675/96, a qual aborda o direito sobre os dados pessoais, respeitando a liberdade fundamental, dignidade da pessoa física e refere-se à *riservatezza* e à identidade pessoal. Sobre essa lei, interessante destacar que quando apresenta as definições, ao esclarecer o que é dado pessoal, define como qualquer dado relativo à pessoa física, entretanto, inclui pessoa jurídica e associação¹¹¹.

Já o Código de Proteção de Dados¹¹² italiano vem depois da referida lei e considera suas abordagens e as de diretivas já vigentes, trazendo uma regulamentação e compreensão específica sobre o tema. Trata-se de uma lei que reconhece a importância da privacidade e da segurança da informação em uma sociedade digitalizada e em constante transformação.

O Código, em iniciativa pioneira, compreende o conteúdo da lei anterior sobre a matéria (Lei 675/96), as diversas normas integrativas e modificativas que a sucederam, a Diretiva europeia relativa ao tratamento dos dados pessoais e à tutela da vida privada no setor das comunicações eletrônicas³, bem como a experiência da atividade da Autoridade Garante italiana para a proteção de dados pessoais e de suas decisões em seus 6 anos de existência¹¹³.

Importante afirmar, entretanto, que a Itália não foi a única nação, na Europa, a trazer elaboração legislativa sobre o tema. A Alemanha, em 1970, já elaborava a lei de proteção de dados, assim como outros países também se propuseram¹¹⁴. Portanto, não se trata de pioneirismo italiano, mas, sim, de um bom desenvolvimento sobre o tema¹¹⁵.

A primeira lei no mundo sobre proteção de dados foi editada pela Alemanha em 1970, especificamente pelo estado de Hessen. Posteriormente, o Parlamento aprovou lei federal sobre a matéria. Entretanto, tomou maior proporção a partir da decisão do Tribunal Constitucional Federal acerca do censo demográfico em 1983. Nesse momento ficou estabelecido o direito fundamental à autodeterminação informativa.

¹¹¹ Legge n. 675 del 31 dicembre 1996 – Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. Disponível em: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/28335>. Acesso em 05 abril 2024.

¹¹² DECRETO LEGISLATIVO, 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali. Disponível em: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2003-07-29&atto.codiceRedazionale=003G0218. Acesso em 19 abril 2024.

¹¹³ DONEDA, Danilo. Um código para a proteção de dados pessoais na Itália. **Revista Trimestral de Direito Civil**, p. 117, 2003.

¹¹⁴ UFRN. Evolução Histórica da Proteção de Dados e o Direito à Privacidade. Disponível em: <https://obdi.ccsa.ufrn.br/2020/09/24/evolucao-historica-da-protacao-de-dados-e-o-direito-a-privacidade/>. Acesso em: 05 abril 2024.

¹¹⁵ DONEDA, Danilo. Um Código da Proteção de Dados Pessoais na Itália. Disponível em: <https://egov.ufsc.br/portal/sites/default/files/anexos/29727-29743-1-PB.pdf>. Acesso em 05 abril 2024.

Alemanha pode ser considerada um dos países que apresenta o maior desenvolvimento doutrinário e valorização quanto à proteção de dados, sendo que o tema apresenta tamanha importância que pode até mesmo ser classificado como um instituto autônomo (Datenschutz) no universo jurídico daquele país. A primeira lei no mundo sobre o assunto foi editada em 1970 pelo estado alemão de Hessen. No ano de 1977, o Parlamento alemão aprovou lei federal de proteção de dados (Bundesdatenschutzgesetz). Todavia, o ápice do reconhecimento da proteção de dados ocorreu com a decisão do Tribunal Constitucional Federal sobre a questão do censo demográfico que se realizava na Alemanha no ano de 1983 (Volkszählungsurteil). Esta decisão estabeleceu o direito fundamental à autodeterminação informativa (Grundrecht auf informationelle Selbstbestimmung)¹¹⁶.

Outros países como Espanha e Portugal trazem abordagens regulatórias em seu ordenamento Interno. A Constituição espanhola de 1978 fala sobre problemas informáticos e a Constituição portuguesa de 1976 traz a proteção de dados pessoais. Ainda assim, como afirma o professor Doneda, pode-se considerar a Convenção de Strasbourg como o principal marco de uma abordagem da matéria pela chave dos direitos fundamentais¹¹⁷.

Danilo Doneda¹¹⁸ explica que no Direito Europeu, proteção de dados assumiu um perfil diferente em relação aos Estados Unidos o qual começou a delinear a privacidade sob outra ótica, setorizada. Quando o tema chega à Europa, toma uma perspectiva de proteção humana. Saliente-se que a Convenção 108/1981 já traz a abordagem sobre proteção de dados, entendendo ser direito fundamental.

Nesse sentido, como se afirmou no capítulo anterior, a diretiva Europeia tem o objetivo de estabelecer normas gerais, cabendo a cada país trabalhar seu ordenamento para atender as diretrizes determinadas na diretiva vigente. Dessa forma, quando foi adotada a diretiva 95/46/CE, a Itália recepcionou a Diretiva como lei. Assim, após a lei 675/96 e demais decretos que se sucederam, formou-se o eixo de proteção de dados para a Itália.

A partir do período de adequação, a Itália em processo de atualização, com a diretiva 2002/58/CE, condensou em um texto único tudo que já havia construído sobre o tema, fazendo surgir o Decreto Legislativo 196/2003, o *Codice in materia indi protezione dei dati personali*¹¹⁹.

¹¹⁶ MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. **RJLB, Ano**, v. 5, p. 781-809, 2019.

¹¹⁷ DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico: Journal of Law**, v. 12, n. 2, p. 91-108, 2011.

¹¹⁸ DONEDA, Danilo. Um Código da Proteção de Dados Pessoais na Itália. Disponível em: <https://egov.ufsc.br/portal/sites/default/files/anexos/29727-29743-1-PB.pdf>. Acesso em 05 abril 2024.

¹¹⁹ DECRETO LEGISLATIVO 30 giugno 2003, n. 196. Codice in materia indi protezione dei dati personali. Disponível em: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2003-07-29&atto.codiceRedazionale=003G0218. Acesso em: 05 abril 2024.

O referido Código chega com uma proposta de organizar o tema no país, e atinge o propósito de que os dados devem ser protegidos de forma idêntica, sejam eles tratados por entes públicos ou entes privados. Traz uma visão voltada para direito fundamental como pilar, diferente da legislação alemã que é voltada para o caráter informativo.

É importante destacar como se desenvolveu o entendimento sobre privacidade na Itália, ainda que já houvesse a discussão na Europa sobre o tema. Isso permite demonstrar como se chega ao Código de Privacidade e outras considerações importantes para depois analisar, nos próximos tópicos, como se comportou o país após a vigência do Regulamento.

O mesmo trabalho, aqui desenvolvido, será proposto em relação ao Brasil. É uma análise importante. Imaginar uma convergência sobre entendimento de privacidade poderá ser uma alternativa sobre o desenvolvimento das relações entre as nações garantindo a proteção da dignidade da pessoa humana. Trata-se de um estudo com olhar panorâmico mundial. Isso se justifica pela razão do falado ciberespaço e a conexão, de forma que não há fronteiras físicas como outrora. As comunicações abrangem maior fluxo de dados que circulam por vários sistemas e em vários países, daí a questão sobre como proteger os dados ser um desafio mundial.

Nesse sentido, é importante compreender como o Brasil abordou privacidade antes da lei Geral de Proteção de Dados, pois isso corrobora com a construção de um raciocínio que contribuirá para solidificar o tema no meio acadêmico e social na atualidade. Trata-se de uma análise sobre o momento anterior a lei para, então, analisar o ordenamento pós surgimento da legislação. A análise das normas no espaço de tempo permite avaliar os avanços e as necessidades ainda presentes no sistema jurídico.

Logo, compreender como os países se comprometem com a proteção de dados pode ser uma forma de construção social em matéria de proteção de dados. Daí o recorte metodológico partindo da Itália, mas entendendo-se que a pesquisa precisa ser expandida para tornar o ciberespaço um ambiente seguro.

Desse modo, a Itália, como já dito, formulou a Lei 675/96 em atendimento aos dispositivos exigidos na Diretiva 95/46 CE, que, como diretiva, não tem aplicação imediata entre os Estados membros da União Europeia¹²⁰. Posteriormente, editou o Código de Proteção

¹²⁰ MARTINES, Francesca. Conteúdo abordado em sala de aula em 26 mar 2024. Università di Pisa, Itália.

de Dados que contemplou um conjunto de normas e compreensões sobre o tema para ser norma vigente no Estado italiano.

Entretanto, é importante afirmar que no campo europeu já estava estabelecida a Convenção Europeia dos Direitos Humanos em que há a proteção pela vida privada, familiar, domicílio e correspondência. Além disso, a Constituição Italiana de 1947 reconhece e garante os direitos invioláveis do homem, uma proteção enquanto indivíduo quanto como agente social.

ARTICOLO 8 Diritto al rispetto della vita privata e familiare 1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui¹²¹.

Art. 2. La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale.

¹²²¹²³

Merla traz considerações importantes sobre a regulamentação do uso de drone, antes da entrada em vigor do regulamento europeu. Em seu texto, ela aborda a problemática ocorrida nos Estados Unidos, quando houve o uso de drone por cidadãos comuns e ocorreram dois episódios, um em que um rapaz resolve espionar sua namorada com uso do equipamento e outro em que um homem descobre a traição de sua esposa do mesmo modo.

Nesse sentido, a autora fala sobre a diferença regulatória entre as duas margens do Oceano: Estados Unidos e Europa. Dentre outros questionamentos, ela apresenta as diferenças entre as regulamentações e, no caso da Europa, se estaria sanado o problema a partir da vigência do Regulamento Europeu.

¹²¹ UNIÃO EUROPEIA. Convenzione Europea dei Diritti dell'Uomo. Disponível em: https://presidenza.governo.it/CONTENZIOSO/contenzioso_europeo/documentazione/Convention_ITA.pdf. Acesso em: 25 abril 2024.

¹²² ITÁLIA. La Costituzione della Repubblica Italiana. Disponível em: https://www.cortecostituzionale.it/documenti/download/pdf/Costituzione_della_Repubblica_italiana.pdf. Acesso em 25 abril 2024.

¹²³ Tradução livre: ARTIGO 8.º Direito ao respeito pela vida privada e familiar 1. Toda pessoa tem direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pela sua correspondência. 2. Não pode haver interferência de uma autoridade pública no exercício deste direito, a menos que tal interferência esteja prevista na lei e constitua uma medida que, numa sociedade democrática, seja necessária à segurança nacional, à segurança pública, ao bem-estar económico do país, a defesa da ordem e a prevenção do crime, a proteção da saúde ou da moral, ou a proteção dos direitos e liberdades de terceiros.

Art. 2. A República reconhece e garante os direitos invioláveis do homem, tanto como indivíduo como nas formações sociais onde se desenvolve a sua personalidade, e exige o cumprimento dos deveres obrigatórios de solidariedade política, económica e social.

Occorre spiegare sia i diversi modi in cui il legislatore può astrattamente pensare di regolare l'innovazione tecnologica sia come queste diverse modalità normative abbiano a che fare con un settore, quello della privacy e della protezione dei dati personali, continuamente messo alla prova dall'evolversi ed espandersi della tecnologia qui sotto esame, i "droni"¹²⁴¹²⁵.

Vale uma reflexão, como a autora traz no trecho acima. Ela diz que é importante os diferentes modos de pensar dos legisladores sobre regulamentar as tecnologias e como elas estão relacionadas a um setor: privacidade e proteção de dados pessoais, que são desafiados pela expansão tecnológica. Nesse sentido, ela afirma, que o direito é uma técnica que regula outra técnica, chamando de meta-tecnologia. Como ela bem cita, na União Europeia há uma distinção entre privacidade e proteção de dados. Tema que já foi abordado no primeiro capítulo do trabalho. Ela fala sobre essa diferença para mostrar que a visão sobre a mesma temática é diferente para os Estados Unidos.

Nesse sentido, explica que na União Europeia há uma unificação em um conjunto de direitos, afirmação quando da vigência da Diretiva e que foi seguido pelo Regulamento. Afirma ainda que a preocupação da UE é haver um mercado único digital e que a regulamentação da proteção de dados é um benefício para todos.

Observa-se, a partir dessa compreensão, que em havendo uma similaridade global sobre privacidade e proteção de dados permite que as relações internacionais sigam em um mesmo sentido, pautados em entendimentos semelhantes, oportunizando negociações entre países que convergem para um mesmo sentido. Não se defende a unicidade absoluta sobre o tema, mas que haja semelhanças para que não se torne impasse no cenário internacional.

Ao falar sobre o Brasil em matéria de proteção de dados antes da LGPD, é perceptível o desenvolvimento normativo já fundado na preocupação com a regulamentação sobre esse direito fundamental. Ao analisar a Constituição Federal de 1988 pode-se aduzir interpretação de uma abordagem voltada para proteção da privacidade. Trata-se de um ordenamento que tutela a intimidade do indivíduo. Apresenta a liberdade de expressão, o direito ao acesso à

¹²⁴ MERLA, Lara. Droni, privacy e tutela dei dati personali. **Informatica e diritto**, v. 25, n. 1, p. 29-45, 2016. Disponível em: http://www.ittig.cnr.it/EditoriaServizi/AttivitaEditoriale/InformaticaEDiritto/IeD_2016_01_Merla.pdf. Acesso em 07 abril 2024.

¹²⁵ Tradução livre: É necessário explicar tanto as diferentes formas como o legislador pode pensar abstratamente a regulação da inovação tecnológica, como como esses diferentes métodos regulatórios têm a ver com um setor, o da privacidade e da proteção de dados pessoais, continuamente posto à prova pela evolução e expansão a tecnologia em análise aqui, os "drones"

informação que eventualmente são confrontados com a proteção da personalidade e privacidade. A Constituição Federal¹²⁶ apresenta proteção à vida privada, intimidade e apresenta a modalidade de direito de acesso à modificação de dados por meio do *habeas data*¹²⁷.

Além disso, ainda sobre o aspecto de proteção de dados, o Brasil tem em seu arcabouço normativo o Código de Defesa do Consumidor¹²⁸ que traz previsão que regula cadastro dos dados do consumidor em banco de dados e cadastros. Essa norma é vista pela doutrina como marco normativo dos princípios de proteção de dados pessoais no Direito brasileiro¹²⁹.

A respeito do *habeas corpus*, no Brasil, o professor Doneda explica ser um documento que surgiu com intuito de o interessado solicitar informações em posse do poder Público. O referido instrumento foi regulamentado pela lei nº. 9.507 de 1997 permitindo que o cidadão possa ajuizar uma ação para retificação de dados pessoais junto a entidades governamentais ou caráter público¹³⁰. Quanto a esse instrumento, há críticas porque há alguns requisitos que o tornam ineficaz no que tange a comunicação e tratamento de dados pessoais na atual sociedade da informação. Nesse sentido, a doutrina tece críticas a essa ferramenta¹³¹.

Por conseguinte, no quadro legislativo brasileiro encontra-se o art. 21 do Código Civil Brasileiro¹³², em que traz a previsão da proteção da vida privada da pessoa natural. Nele, o legislador deixa claro essa ser inviolável, permitindo a tutela jurisdicional para fazer cessar ou impedir ato que seja contrário a referida proteção. Protege, portanto, a intimidade e a vida privada, não podendo uma pessoa interferir na vida pessoal de outra, incluindo no ambiente digital.

¹²⁶ BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 abril 2024.

¹²⁷ DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico: Journal of Law**, v. 12, n. 2, p. 91-108, 2011.

¹²⁸ BRASIL. Código de Defesa do Consumidor. Lei nº. 8.078 de 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm#:~:text=LEI%20N%C2%BA%208.078%2C%20DE%2011%20DE%20SETEMBRO%20DE%201990.&text=Disp%C3%B5e%20sobre%20a%20prote%C3%A7%C3%A3o%20do%20consumidor%20e%20d%C3%A1%20outras%20provid%C3%AAs.&text=Art.,da%20Constitui%C3%A7%C3%A3o%20Federal%20e%20art. Acesso em: 20 abril 2024.

¹²⁹ DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico: Journal of Law**, v. 12, n. 2, p. 91-108, 2011.

¹³⁰ DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico: Journal of Law**, v. 12, n. 2, p. 91-108, 2011.

¹³¹ DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico: Journal of Law**, v. 12, n. 2, p. 91-108, 2011.

¹³² BRASIL. Lei 10.406 de 10 de janeiro de 2002. Código Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm. Acesso em 23 abril 2024.

Outra menção legislativa importante a ser feita é sobre a Lei de Acesso à Informação¹³³. Intercala-se o comentário dessa legislação, primeiro porque a data de entrada em vigor antecede as demais legislações pertinentes a dados pessoais, depois porque refere-se à divulgação de dados correlacionado com o princípio da transparência. Promove a transparência, o controle social e a participação cidadã nas decisões governamentais. Se trata de transparência sobre gestão estatal, bem como a disponibilização de dados quando solicitados pelo cidadão. Após o direito de acesso à informação surgem ferramentas que consolidam a Política Nacional de Dados Abertos. Mesmo sendo apresentada essa estrutura, ainda há obstáculos para concretizar o objetivo da lei, quando os dados são disponibilizados inadequadamente, inviabilizando o controle social¹³⁴.

Além da Constituição Federal e do Código de Defesa do Consumidor o ordenamento jurídico brasileiro prevê o Marco Civil da Internet¹³⁵. A elaboração do anteprojeto de lei que se concretizou na lei do Marco Civil foi entendida como uma iniciativa de democracia digital institucional, do Poder Público¹³⁶. Assim, o Marco Civil é resultado de contribuição da sociedade civil e diferentes atores sociais, o que proporcionou um debate participativo através de consultas públicas. Na primeira fase buscou-se analisar princípios e na segunda foi disponibilizado o texto com os artigos para que as pessoas pudessem discuti-los¹³⁷.

A mobilização para a elaboração do projeto de lei que antecedeu o Marco Civil aconteceu de diversas formas proporcionando o acesso das pessoas, seja por meio de site, seja por meio de rede de comunicação como Twitter. Além disso, debates presenciais, audiências públicas de forma que o cidadão pudesse participar e contribuir para o debate¹³⁸.

¹³³ BRASIL. Lei 12.527 de 18 de novembro de 2011. Lei de Acesso à Informação. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm#:~:text=Regula%20o%20acesso%20a%20informa%C3%A7%C3%B5es,de%201991%3B%20e%20d%C3%A1%20outras. Acesso em 21 de abril de 2024.

¹³⁴ DE MIRANDA, Wallace Vieira; ZAGANELLI, Juliana Costa. Marco civil da internet e política pública de transparência: uma análise da e-democracia e do compliance público. **Revista Brasileira de Políticas Públicas**, v. 7, n. 3, p. 633-646, 2017.

¹³⁵ BRASIL. Lei nº. 12.865 de abril de 2014. Marco Civil da Internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 21 abril 2024.

¹³⁶ MAGRANI, Eduardo. *Democracia conecta da: a internet como ferramenta de engajamento político – democrático*. Curitiba: Juruá, 2014. p.165

¹³⁷ MAGRANI, Eduardo. *Democracia conectada: a internet como ferramenta de engajamento político – democrático*. Curitiba: Juruá, 2014.

¹³⁸ MAGRANI, Eduardo. *Democracia conectada: a internet como ferramenta de engajamento político – democrático*. Curitiba: Juruá, 2014.

O professor Magrani¹³⁹ teceu alguns comentários à época dos movimentos para a construção da lei:

(...)não restam dúvidas de que o procedimento de construção e colocação do texto em consulta pública na internet representa por si só um significativo avanço, consideravelmente mais rico democraticamente que as tradicionais consultas públicas presenciais, sediadas em Brasília. A iniciativa de apresentar previamente os princípios à população e abrir seu texto a críticas gerou como produto final um texto tecnicamente melhor e sem dúvida mais legítimo. Com a experiência dos poderes executivo e legislativo com o Marco Civil da internet, o sistema político brasileiro foi capaz de proporcionar uma importante abertura na comporta legislativa do sistema, deixando-se contribuir de forma mais democrática e direta pelos formadores de políticas públicas e pela sociedade civil. No entanto, por ser um procedimento inédito, pode ser aprimorado para melhor atender à condição de validade dependente da contribuição de todos os possíveis atingidos pela norma.

Indubitavelmente, o Marco Civil¹⁴⁰ não só trouxe regras mais detalhadas e específicas para a vida quando no uso da internet no Brasil. Foi resultado de um projeto legislativo participativo, em que a sociedade pôde contemporizar, analisar, discutir o que proporcionou uma construção democrática que buscou atender às demandas sociais brasileiras.

É uma lei que regulamenta o uso da internet no Brasil, estabelecendo princípios, garantias, direitos e deveres para o uso da rede. Além disso, promove a liberdade de expressão e a neutralidade da rede. Este último se traduz em uma garantia de que todos os dados que trafegam na internet sejam igualitários, permitindo que todas as pessoas tenham acesso a todas as coisas com isonomia, sem discriminação.

A lei do MCI é fundamentalmente uma constituição digital. Seus artigos iniciais declaram que os princípios democráticos de liberdade, privacidade e direitos humanos são igualmente aplicáveis no ciberespaço. Em particular, os artigos 2º e 3º expressam esses princípios de direitos civis e estabelecem como fundamentos do uso da internet o “reconhecimento da escala mundial da rede”, bem como o pluralismo, a diversidade, a abertura e a colaboração, e direitos econômicos como livre-iniciativa, livre concorrência e defesa do consumidor.¹⁶ Os direitos civis assumem precedência na linguagem legislativa, mas a livre-iniciativa e novos modelos de negócio também são encorajados “desde que não conflitem com os demais princípios estabelecidos nesta lei”. O direito à privacidade também é garantido pela lei. Dados pessoais são protegidos “na forma da lei”, mas é assegurada a responsabilização de cidadãos e organizações, públicas e privadas, de acordo com suas atividades. No artigo 7º, esse direito à privacidade é definido como a “inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei”¹⁴¹.

¹³⁹ MAGRANI, Eduardo. *Democracia conectada: a internet como ferramenta de engajamento político – democrático*. Curitiba: Juruá, 2014. p. 172.

¹⁴⁰ BRASIL. Lei nº. 12.865 de abril de 2014. Marco Civil da Internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 22 abril 2024.

¹⁴¹ ARNAUDO, Daniel. O Brasil eo Marco Civil da Internet. **Igarapé Institute**, 2017. Disponível em: https://d1wqtxslxzle7.cloudfront.net/53233066/igarape_o-brasil-e-o-marco-civil-da-internet-libre.pdf?1495467259=&response-content-disposition=inline%3B+filename%3DO_Brasil_e_o_Marco_Civil_da_Internet_O_E.pdf&Expires=1729134079&Signature=Wobw5zOqxLqsTn8wXC1oIgOS0EkuRePmFqIJ~7xPleqHIYWnglmeFZCH0y0aj7ikTPHcb0IBA8IU3krZ5IGzYmvER0yHoygbOIVKE0SnkQUI6OtJUIUofOY2jLxomEk1EgyhdJmqIIIDcbD

Regulamentações após vigência do GDPR determinadas pelo Ministero della Giustizia na Itália para o poder judiciário quanto à proteção de dados durante os Procedimentos Judiciais

Considerando o Regulamento de Proteção de Dados Pessoais (General Data Protection Regulation – GDPR), que surgiu na União Europeia como uma normativa sobre proteção de dados e privacidade, tema já debatido em tópicos anteriores, parte-se para uma análise individualizada da Itália.

A proposta do presente subtópico é de analisar como o ordenamento jurídico italiano passou a regular as questões que envolvem proteção de dados pós vigência do GDPR. Em especial, o objetivo do estudo é investigar a existência das normativas que regulamentam os procedimentos processuais judiciais no que tange ao exame sobre a proteção de dados na realização de audiências por videoconferência. O que surge de normativas, resoluções e demais regramentos, após a vigência do GDPR, em matéria processual judicial, deve estar em consonância com o entendimento do referido regulamento europeu. Isso porque, se entende que a norma europeia tem aplicação abrangente também na seara processual.

Vale explicar que a preocupação em abordar o procedimento processual judicial não exclui a preocupação sobre os demais espaços sociais em que ocorre a coleta e tratamento de dados pessoais. O recorte de pesquisa é feito para o processo eletrônico, em específico, para realização de audiências virtuais, como já bastante enfatizado até aqui. Assim, faz-se a análise sobre a incidência do regulamento europeu na Itália, observando a pré-existência de um Código de Privacidade italiano. A partir disso, contextualiza-se o Código e a necessidade de uma interpretação em conformidade com o Regulamento Europeu. Após, segue-se o estudo sobre as normativas específicas processuais sobre o tema.

Nesse sentido, o *Osservatorio Cybersecurity e Data Protection*¹⁴³ que estuda sobre tutela de privacidade e sobre dados pessoais, explica sobre o GDPR e o que acontece depois de sua vigência na União Europeia e, nesse contexto, aborda a Itália. Desse modo, o escopo

¹⁴³ OSSERVATORIO CYBERSECURITY & DATA PROTECTION. **GDPR e Privacy, cos'è e come cambia per il trattamento e la protezione dei dati. La protezione dei dati, prima e dopo l'introduzione del General Data Protection Regulation.** Disponível em: <https://blog.osservatori.net/gdpr-privacy-protezione-dati-personali>. Acesso em: 23 abril 2024.

principal do GDPR foi o de adequar normativamente a partir do desenvolvimento tecnológico de forma que ocorra harmonização a nível europeu quanto a regulamentação da matéria¹⁴⁴.

E ao tratar especificamente sobre a Itália, como dito, é importante analisar o que previamente já existia do ponto de vista normativo: *Il Codice Privacy*. O *Osservatorio* explica que o referido código não está totalmente derogado. Foi necessária uma adequação ao Regulamento Europeu para haver o respeito a normativa da UE¹⁴⁵. Foi necessária adequação para que o código de Privacidade viesse a ser interpretado à luz do regulamento europeu. Para isso, entrou em vigor o decreto legislativo 101/2018¹⁴⁶ que traz justamente a diretriz sobre a interpretação das normas italianas que abordem proteção de dados.

Dunque, è l'intera normativa italiana in materia di tutela dei dati personali che va letta, interpretata e applicata in un quadro estremamente complesso che comprende il GDPR e il Codice oggetto del d.lvo 196 del 2003 come novellato dal d.lvo 101 del 2018¹⁴⁷¹⁴⁸.

O professor Pizzetti afirma que ainda que o texto do Decreto tenha sido claro quanto a compreensão das normas estarem de acordo com o Regulamento europeu, tal entendimento deriva do princípio interpretativo da hierarquia das normas.

Questo non solo perché lo dice con estrema chiarezza l'art. 22, comma 1, ma perché, come correttamente sottolinea la Relazione, la norma non fa altro che esplicitare un canone interpretativo desumibile dalla gerarchia delle fonti del diritto¹⁴⁹.(...)

È evidente, dunque, che la normativa italiana e quella europea sono un ordinamento giuridico integrato e complesso, retto dal principio di supremazia della normativa europea su quella nazionale.

Un principio che ha tre aspetti essenziali.

Le disposizioni italiane sono legittime nel contesto europeo in quanto e nella misura in cui:

¹⁴⁴ OSSERVATORIO CYBERSECURITY & DATA PROTECTION. **GDPR e Privacy, cos'è e come cambia per il trattamento e la protezione dei dati. La protezione dei dati, prima e dopo l'introduzione del General Data Protection Regulation.** Disponível em: <https://blog.osservatori.net/gdpr-privacy-protezione-dati-personali>. Acesso em: 23 abril 2024.

¹⁴⁵ OSSERVATORIO CYBERSECURITY & DATA PROTECTION. **GDPR e Privacy, cos'è e come cambia per il trattamento e la protezione dei dati. La protezione dei dati, prima e dopo l'introduzione del General Data Protection Regulation.** Disponível em: <https://blog.osservatori.net/gdpr-privacy-protezione-dati-personali>. Acesso em: 23 abril 2024.

¹⁴⁶ ITÁLIA. Decreto Legislativo 10 agosto 2018, n. 101. Disponível em: <https://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg>. Acesso em: 25 abril 2024.

¹⁴⁷ PIZZETTI, Franco. Privacy. Codice privacy italiano dopo il Gdpr: come leggerlo e applicarlo ex decreto 101/2018. 14 set 2018. Disponível em: <https://www.agendadigitale.eu/sicurezza/privacy/gdpr-pizzetti-i-consigli-per-leggere-e-applicare-bene-il-decreto-101-2018-dal-19-settembre/>. Acesso em: 25 abril 2024.

¹⁴⁸ Tradução livre: Portanto, é toda a legislação italiana sobre a proteção de dados pessoais que deve ser lida, interpretada e aplicada num quadro extremamente complexo que inclui o RGPD e o Código Objecto do Decreto Legislativo 196 de 2003, alterado pelo Decreto Legislativo 101 de 2018.

¹⁴⁹ PIZZETTI, Franco. Privacy. Codice privacy italiano dopo il Gdpr: come leggerlo e applicarlo ex decreto 101/2018. 14 set 2018. Disponível em: <https://www.agendadigitale.eu/sicurezza/privacy/gdpr-pizzetti-i-consigli-per-leggere-e-applicare-bene-il-decreto-101-2018-dal-19-settembre/>. Acesso em: 25 abril 2024.

- rientrano nelle materie rimesse dal GDPR al legislatore nazionale (competenza per materia);
- il loro contenuto sia conforme alle disposizioni del GDPR;
- esse siano interpretate e applicate nel rispetto del Regolamento¹⁵⁰.

Nesse sentido, ele afirma que as normas italianas são legítimas desde que estejam respeitando as competências estabelecidas no GDPR, que o conteúdo delas estejam em conformidade com o referido regulamento e que a interpretação esteja em conformidade com a norma europeia sobre proteção de dados. O que acontece com o código de proteção de dados italiano que não foi revogado, apenas adaptado.

Desse modo, cite-se a diretiva 2016/680¹⁵¹ que aborda o tema sobre proteção de dados no âmbito criminal. O intuito é sobre o respeito ao direito fundamental de proteção de dados quando da atuação das autoridades nas investigações. A referida diretiva foi publicada através do Decreto Legislativo 51/2018. Trata-se de uma diretiva importante, pois complementa o GDPR no que diz respeito a proteção de dados tratados por autoridade competente quando da prevenção, investigação e repressão de infrações penais ou execução de sanções penais.

Sua importância se deve pelo equilíbrio entre segurança e privacidade, pois necessita proteger a sociedade e garantir o direito fundamental. Traz os princípios a serem cumpridos pelas autoridades competentes quando desse tratamento e, por fim, permite cooperação entre os estados membros da UE na troca de informações.

Para além das normativas elencadas até aqui, há de se mencionar as medidas legislativas tomadas à época da pandemia do Covid-19. Assim, foram publicados Decretos legislativos na

¹⁵⁰ Tradução livre: Isto não ocorre apenas porque a arte diz isso muito claramente. 22, parágrafo 1, mas porque, como bem sublinha o Relatório, o dispositivo nada mais faz do que explicar um cânone interpretativo que pode ser deduzido da hierarquia das fontes do direito.(...)

É evidente, portanto, que a legislação italiana e europeia constituem um sistema jurídico integrado e complexo, regido pelo princípio da supremacia da legislação europeia sobre a legislação nacional.

Um princípio que tem três aspectos essenciais.

As disposições italianas são legítimas no contexto europeu porque e na medida em que:

- enquadram-se nas matérias submetidas pelo RGPD ao legislador nacional (jurisdição da matéria);
- o seu conteúdo está em conformidade com as disposições do RGPD;
- são interpretados e aplicados em conformidade com o Regulamento.

¹⁵¹ ITÁLIA. Decreto Legislativo de 18 maggio 2018, n° 51. Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio. (18G00080) (GU Serie Generale n.119 del 24-05-2018). Disponível em:

<https://www.gazzettaufficiale.it/eli/id/2018/05/24/18G00080/sg>. Acesso em 15 maio 2024.

Itália, bem como orientações e incentivos por parte da União Europeia para o uso de meios telemáticos nesse período de afastamento sanitário.

Na Itália foi publicado o Decreto Legislativo nº. 18 de 2020 (que foi prorrogado pelo Decreto-Lei nº. 23/2020 Come noto, il D.L. 23/2020 ha ulteriormente prorogato fino alla data dell'11 maggio la sospensione dei termini e la soppressione delle udienze, già prevista dal D.L. 18/2020)¹⁵²¹⁵³, conhecido como “Decreto cura Itália” em que há a autorização do uso de meios telemáticos nos processos judiciais. Tal medida permitiu o uso de audiência por videoconferência como forma de manter o distanciamento, bem como dar continuidade a atividade jurisdicional durante a pandemia do Covid-19.

No mesmo sentido de manutenção de medida sanitária no período pandêmico, o Decreto Legge nº. 137 de 2020¹⁵⁴, conhecido como “Decreto Ristori” atribuiu ao Ministério da Justiça da Itália que regulasse o uso de conexões remotas e realização de audiência por videoconferência.

Além das previsões que surgiram no período de afastamento do Covid-19, há se falar sobre o Código de Processo Civil italiano, no que diz respeito ao uso de meios telemáticos. Os artigos 127, 127 bis e 127 ter trazem abordagem sobre realização de atos com o uso da tecnologia. O 127 autoriza a realização de audiência por meio de conexões audiovisuais à distância nos termos do 127 bis e 127 ter. O 127 bis traz a orientação sobre a realização da audiência quando não for necessária a presença de outros sujeitos que não sejam defensores, juiz, partes e Ministério Público e dá outras orientações.

E, finalizando as subdivisões do art. 127, o 127 ter aborda a possibilidade de substituição da realização de audiência por notas escritas. Para isso, se faz necessário que todas as partes

¹⁵² ITÁLIA. Decreto-Legge 17 marzo 2020, nº. 18. Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19. (20G00034). Disponível em: https://www.gazzettaufficiale.it/atto/stampa/serie_generale/originario. Acesso em: 15 maio 2024.

¹⁵³ MARTORANA, Marco. Giustizia digitale e data protection, ecco gli impatti privacy dei processi da remoto. pubblicato il 3 giu 2020. Disponível em: <https://www.agendadigitale.eu/documenti/giustizia-digitale/giustizia-digitale-e-data-protection-ecco-gli-impatti-privacy-dei-processi-da-remoto/>. Acesso em: 17 maio 2024.

¹⁵⁴ ITÁLIA. Decreto Legge 28 ottobre 2020, nº. 137. Ulteriori misure urgenti in materia di tutela della salute, sostegno ai lavoratori e alle imprese, giustizia e sicurezza, connesse all'emergenza epidemiologica da Covid-19. (20G00166) (GU Serie Generale n.269 del 28-10-2020). Disponível em: <https://www.gazzettaufficiale.it/eli/id/2020/10/28/20G00166/sg>. Acesso em: 15 maio 2024.

solicitem que o procedimento siga dessa forma. Importante frisar que os procedimentos judiciais civis foram alterados a partir do Decreto Legislativo nº. 149 de 10 de outubro de 2022. Os artigos acima citados foram analisados com as atualizações do decreto.

De acordo com Mascii¹⁵⁵, o decreto teve o intuito de orientar a interpretação da norma a partir de princípios como cooperação entre partes e juiz, justiça e transparência como elementos chave para o devido processo legal.

Ele ainda menciona aspectos acerca da digitalização:

DIGITIZATION

Electronic filing will be mandatory for all proceedings with no exemptions.^[1]

The judge shall order remote hearings or replace oral discussion with the filing of written notes when only parties, counsel, and public prosecutor^[2] are required to attend. Therefore, this does not apply to witness examination hearings. In any case, parties may always request that a hearing being held in person.

^[1] Electronic filing is already mandatory for most filings, but there are still a few cases in which hard-copy filing can be done, including proceedings before a justice of the peace (where there is currently no electronic filing system).

^[2] In civil proceedings, the public prosecutor is involved in a very limited number of cases¹⁵⁶.

Portanto, as audiências por videoconferência tornaram-se habituais, comuns, a partir do período pandêmico, que assim como vários países, a Itália precisou tomar medidas urgentes

¹⁵⁵ MASCII. Andrea. New Rules on Italian Civil Proceedings: A step forward in improving the italian court system. Disponível em: <https://portolano.it/en/newsletter/litigation-arbitration/new-rules-on-italian-civil-proceedings-a-step-forward-in-improving-the-italian-court-system> Acesso em 16 maio 2024.

¹⁵⁶ Tradução livre: DIGITALIZAÇÃO

O arquivamento eletrônico será obrigatório para todos os processos, sem isenções.^[1]

O juiz ordenará audiências remotas ou substituirá a discussão oral pela apresentação de notas escritas quando apenas as partes, o advogado e o promotor público^[2] forem obrigados a comparecer. Portanto, isso não se aplica às audiências de interrogatório de testemunhas. Em qualquer caso, as partes podem sempre solicitar que a audiência seja realizada presencialmente.

^[1] O arquivamento eletrônico já é obrigatório para a maioria dos arquivamentos, mas ainda existem alguns casos em que o arquivamento em papel pode ser feito, incluindo processos perante um juiz de paz (onde atualmente não há sistema de arquivamento eletrônico).

^[2] Nos processos cíveis, o Ministério Público está envolvido num número muito limitado de casos.

para continuidade do serviço judiciário¹⁵⁷. O Decreto-lei nº. 11 de março de 2020 foi o iniciou a permissão da realização das audiências por videoconferência na Itália¹⁵⁸.

Alguns procedimentos e regramentos foram adotados para outras áreas, como aconteceu com as audiências no Tribunal de Contas, que no período da pandemia também adotou a realização de atos de forma digital. Além de audiência remota, poderiam ser publicadas sentenças e despachos assinados digitalmente pelos juízes. Frise-se que na referida regra técnica elaborada pela *Corte dei Conti*, em seu artigo 3º, nº. 5, traz a possibilidade de gravação das audiências, resguardando o respeito e a confidencialidade dos dados pessoais¹⁵⁹.

Assim, no que tange ao processo judicial, entre o Decreto Lei 28 de 30 de abril de 2020 e o Decreto Lei 28/2020 se estabeleceu, àquela época, que as audiências remotas ficariam, a partir desse último decreto, restritas a hipótese residual ou quando autorizada pelas partes¹⁶⁰. Já referente ao processo civil, houve o Decreto legislativo nº 11 de 8 de março de 2020, que se encontra revogado, previa a realização de audiências por videoconferência. Na sequência, publicou-se o Decreto legislativo de 10 de março de 2020 trazendo as plataformas a serem utilizadas para realização de audiência remota.

¹⁵⁷ BERTI, Ricardo. ZURMELE, Franco. *Giustizia digitale, gli aspetti privacy delle udienze da remoto: ecco le regole*. Le udienze da remoto stanno permettendo alla Giustizia di proseguire la propria attività nonostante l'emergenza coronavirus. Tuttavia, come sottolineato dal Garante della privacy con una lettera al Ministero della Giustizia, non mancano fronti critici sul versante data protection. Pubblicato il 22 mag 2020. Disponível em: <https://www.agendadigitale.eu/documenti/giustizia-digitale/giustizia-digitale-gli-aspetti-privacy-delle-udienze-da-remoto-ecco-le-regole/>. Acesso em 17 maio 2024.

¹⁵⁸ BALDONI, Roberto et al. *Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici*. 2018.

¹⁵⁹ ITÁLIA. Provvedimento. REGOLE TECNICHE ED OPERATIVE IN MATERIA DI SVOLGIMENTO DELLE UDIENZE IN VIDEOCONFERENZA E FIRMA DIGITALE DEI PROVVEDIMENTI DEL GIUDICE NEI GIUDIZI DINANZI ALLA CORTE DEI CONTI. Disponível em: <https://www.corteconti.it/Download?id=ae08f022-9d8d-4782-b521-61fd0f262749>. Acesso em: 17 maio 2024.

¹⁶⁰ BERTI, Ricardo. ZURMELE, Franco. *Giustizia digitale, gli aspetti privacy delle udienze da remoto: ecco le regole*. Le udienze da remoto stanno permettendo alla Giustizia di proseguire la propria attività nonostante l'emergenza coronavirus. Tuttavia, come sottolineato dal Garante della privacy con una lettera al Ministero della Giustizia, non mancano fronti critici sul versante data protection. Pubblicato il 22 mag 2020. Disponível em: <https://www.agendadigitale.eu/documenti/giustizia-digitale/giustizia-digitale-gli-aspetti-privacy-delle-udienze-da-remoto-ecco-le-regole/>. Acesso em 17 maio 2024.

Posteriormente sugiram os Decretos Legislativos nº. 18 de 17 de março de 2020 reafirmando a realização de audiências remotas. Esse Decreto foi dividido em duas fases. A primeira algumas audiências urgentes poderiam ser realizadas de forma remota e no segundo momento as audiências cíveis que não necessitassem da presença de outras pessoas, além dos advogados e partes.

Em 8 de abril de 2020 é publicado o Decreto Legislativo nº. 23 que prorrogou a data para possibilitar a continuidade da realização de audiências por videoconferência. Nesse mesmo período houve a conversão em lei do Decreto Legislativo 18, possibilitando a realização de audiências por videoconferência com a presença de auxiliares do juiz.

O Decreto Lei 28 de 30 de abril de 2020, dentre as determinações, autorizou a audiência remota desde que o juiz estivesse em seu gabinete. A justificativa para isso seria a segurança cibernética. Entretanto, autoriza o juiz optar por outro modo para a realização de audiência. Nesse caso, podendo fazer por escrito, o que evitaria o deslocamento dele para o fórum.

Com todos os esclarecimentos feitos por Berti e Zurmele, incluindo a narrativa das normativas à época pandêmica, vale mencionar que esse entendimento de segurança cibernética e autorização de realização por escrito é alternativa frágil, no pensamento desses estudiosos:

Il D.L. 28 ha inoltre reso decisamente meno appetibili, per i magistrati, le udienze da remoto, disponendo che le stesse vanno celebrate “con la presenza del giudice nell’ufficio giudiziario”, disposizione che rende certo meno “smart” il lavoro del magistrato, costretto a recarsi presso il tribunale per fare quello che nella sostanza avrebbe fatto anche da casa. Sebbene la ragione di questo irrigidimento poggia verosimilmente in comprensibili preoccupazioni in tema di sicurezza informatica, è evidente che questo porterà ad una netta predilezione da parte dei giudici per altre forme di svolgimento dell’udienza che non rendano necessario il suo trasferimento presso l’ufficio (leggasi trattazione scritta), con la conseguenza che, nei fatti, sui PC domestici dei magistrati risiederanno comunque i dati personali delle parti, solo in una forma diversa (e peraltro più durevole) rispetto a quella del flusso video¹⁶¹.

¹⁶¹ Tradução livre: O Decreto Legislativo 28 também tornou as audiências remotas decididamente menos atrativas para os magistrados, prevendo que elas devem ser realizadas “com a presença do juiz no gabinete judicial”, dispositivo que certamente torna o trabalho do magistrado menos “inteligente”, obrigado a recorrer ao tribunal para fazer o que essencialmente ele teria feito em casa. Embora a razão para este endurecimento resida provavelmente em preocupações compreensíveis relativamente à segurança informática, é claro que isto conduzirá a uma clara predileção por parte dos juizes por outras formas de realização da audiência que não exijam a sua transferência para o gabinete (leia escrito discussão), com a consequência de que, de facto, os dados pessoais das partes continuarão a residir nos computadores domésticos dos magistrados, apenas numa forma diferente (e, além disso, mais durável) da do fluxo de vídeo.

Além disso, o garante, aquele responsável pelo cumprimento da proteção de dados, demonstrou a preocupação quanto a possibilidade de acesso aos dados por parte da Microsoft Corporation, os autores comentam:

Esistono poi numerosissime impostazioni interne all'app Teams e accessibili dall'amministratore di sistema che consentono di elevare (o diminuire) il livello di protezione garantito dall'app Teams, impostazioni che però non è dato sapere come siano state implementate nel caso specifico dal Ministero e che soprattutto non consentono di escludere che Microsoft stessa sia in grado di accedere ai dati sui propri server (autonomamente o per ordine del governo USA).

O texto deles explica que tal vulnerabilidade dos dados frente a Microsoft não seria apenas em relação a realização de audiência por videoconferência, mas pela utilização de toda infraestrutura para além do Teams. Em esclarecimentos, o Ministério explica que com uso do Teams Microsoft e Skype for Business, ficam armazenados dados técnicos da sessão, como horário de início e fim da sessão, identificação de usuário etc.

Frise-se que os dados citados que ficam armazenados contemplam dados pessoais. Isso quer dizer que os dados pessoais dos envolvidos nas audiências remotas precisam do tratamento adequado para garantir a maior segurança possível, atendendo a perspectiva da proteção do direito fundamental. Pode-se captar que essa é uma vulnerabilidade cibernética dos dados pessoais em processo judicial, isso porque os sistemas utilizados não apresentam a segurança necessária para garantir camadas de proteção das informações armazenadas.

Sem protocolos rigorosos de segurança, os dados se tornam alvos de fácil acesso para invasores que desejem coletar dados de terceiros sem autorização para tal. E, nesse sentido, não foi identificado na análise do ordenamento, previsão legislativa de condutas pautadas em exigências específicas para garantir a segurança do armazenamento dos dados pessoais nas mídias digitais dos tribunais.

Assim, o art. 127-ter do *Codice di Procedura Civile* foi introduzido pelo Decreto Legislativo nº 149 de 10 de outubro de 2022. O intuito foi de instituir no ordenamento a possibilidade de depósito de notas escritas em substituição à audiência. O que era uma regra estabelecida para o período emergencial, foi incorporado à legislação processual.

A referida regra estabelecida no novo art. 127-ter entrou em vigor em 1 de janeiro de 2023. A intitulada Audiência documental teve início primeiro que as demais alterações trazidas pelo referido decreto. O objetivo disso é não criar lacuna legislativa, já que o Decreto-Lei 228 de 30 de dezembro de 2021 só estaria em vigor até 31 de dezembro de 2022.

L'art. 127-ter c.p.c. , introdotto dal d.lgs. n. 149 del 10 ottobre 2022, inserisce nel codice di rito l'istituto del deposito di note scritte in sostituzione dell'udienza, previsto per la prima volta dalla legislazione emergenziale per fare fronte al diffondersi della pandemia (e prorogato, successivamente, sino al 31 dicembre 2022), anche se con soluzioni tecniche differenti. L'art. 127-ter c.p.c. trova applicazione (anche ai procedimenti pendenti) a partire dal 1° gennaio 2023. La nuova disciplina della c.d. udienza cartolare è già entrata in vigore, trovando applicazione ai giudizi civili pendenti a partire dal 1° gennaio 2023. Diversamente dalla gran parte delle disposizioni della riforma del processo civile introdotta con il d.lgs. n. 149 del 10 ottobre 2022, che saranno applicabili ai procedimenti instaurati dopo il 28 febbraio 2023. Tale soluzione si spiega in quanto la previgente disposizione in materia (l'art. 221 c.4 del D.L. 34 del 2020, convertito con modificazioni dalla legge n. 77 del 2020), a fronte della più recente proroga prevista dal D.L. n. 228 del 30 dicembre 2021, poteva trovare applicazione soltanto sino al 31/12/2022. Conseguentemente, per non dare adito a vuoti normativi, il legislatore ha deciso di annoverare l'art. 127-ter c.p.c. tra le disposizioni con entrata in vigore anticipata rispetto al complesso della riforma del processo civile¹⁶²¹⁶³.

Percebe-se que o código de processo civil italiano determina que o juiz tem discricionariedade para optar entre apresentação de documentos escritos e audiência remota. Entretanto, quando determina prazo para as partes apresentarem os documentos escritos, elas podem solicitar audiência presencial, momento este que o juiz deve dispor em conformidade com o pedido feito.

Il comma 2° della disposizione in commento – diversamente dalla normativa emergenziale che prevedeva dei termini a ritroso da calcolarsi rispetto alla data di udienza originariamente fissata - stabilisce che il Giudice, con il provvedimento con cui sostituisce l'udienza, assegna un termine da calcolarsi in avanti, espressamente definito come perentorio, per il deposito delle note. Ciascuna delle parti può opporsi entro cinque giorni dalla comunicazione ed entro i successivi cinque giorni il Giudice provvede con decreto non impugnabile. Se però la richiesta di svolgimento

¹⁶² PAGLIA, Ricardo. TALENTI, Alfredo. Riforma del processo civile, la nuova disciplina dell'udienza cartolare. 10 febbraio 2023. Disponibile em: <https://ntplusdiritto.ilsole24ore.com/art/riforma-processo-civile-nuova-disciplina-udienza-cartolare-AECCtykC>. Accesso em: 17 maio 2024.

¹⁶³ Tradução livre: A arte. 127-ter c.p.c., instituído pelo decreto legislativo n. O Decreto-Lei n.º 149, de 10 de outubro de 2022, insere no código de procedimento a instituição do depósito de notas escritas no local da audiência, previsto pela primeira vez pela legislação de emergência para fazer face à propagação da pandemia (e posteriormente prorrogado até 31 de dezembro 2022), embora com soluções técnicas distintas. A arte. 127-ter c.p.c. aplica-se (também aos processos pendentes) a partir de 1 de janeiro de 2023. O novo regulamento do chamado a audiência formal já entrou em vigor, aplicando-se aos processos cíveis pendentes a partir de 1 de janeiro de 2023. Ao contrário da maioria das disposições da reforma do processo civil introduzida com o Decreto Legislativo n.º 149, de 10 de outubro de 2022, que será aplicável aos processos iniciados após 28 de fevereiro de 2023. Esta solução explica-se como a disposição anterior sobre a matéria (art. 221 c.4 do Decreto Legislativo 34 de 2020, convertido com alterações pela lei n.º 77 de 2020), em comparação com a mais recente prorrogação prevista no Decreto Legislativo. n. 228, de 30 de dezembro de 2021, só poderia vigorar até 31/12/2022. Consequentemente, para não gerar lacunas regulatórias, o legislador decidiu incluir o art. 127-ter c.p.c. entre as disposições com entrada em vigor anterior à reforma global do processo civil

dell'udienza in presenza è proposta congiuntamente da tutte le parti, non vi è margine discrezionale per il Giudice che deve disporre in conformità¹⁶⁴¹⁶⁵.

Analizando os sítios e portais do governo italiano, o arcabouço normativo italiano posterior, a vigência do GDPR está associado a provimentos e decretos legislativos. O *Portale dei Servizi Telematici del Ministero della Giustizia* traz orientações sobre o uso do processo telemático e tudo que estiver relacionado com o assunto. No referido sítio pode-se encontrar normativas anteriores ao GDPR e até mesmo do período pandêmico. Entretanto, importante mencionar algumas normativas elencadas no portal acima mencionado.

Além disso, há o decreto presidencial italiano¹⁶⁶ regulamenta o uso de instrumentos informáticos e telemáticos no processo civil, no processo administrativo e nas secções jurisdicionais do tribunal de contas.

Está entre os documentos um provimento do Diretor Geral do Sistema de Informação Automatizados do Ministério da Justiça. Esse documento traz as orientações sobre realização de atos processuais e depósito de documentos pelo meio telemático e também os atos dos procedimentos civis de jurisdição voluntária¹⁶⁷¹⁶⁸.

¹⁶⁴ PAGLIA, Ricardo. TALENTI, Alfredo. Riforma del processo civile, la nuova disciplina dell'udienza cartolare. 10 febbraio 2023. Disponível em: <https://ntplusdiritto.ilsole24ore.com/art/riforma-processo-civile-nuova-disciplina-udienza-cartolare-AECCTykC>. Acesso em: 17 maio 2024.

¹⁶⁵ Tradução livre: O § 2º do dispositivo em questão - diferentemente da legislação emergencial que previa que os prazos fossem calculados retroativamente a partir da data da audiência originalmente fixada - estabelece que o Juiz, com o dispositivo pelo qual substitui a audiência, atribua um prazo a ser calculado a termo, expressamente definido como peremptório, para arquivamento de notas. Cada parte poderá contestar no prazo de cinco dias após a comunicação e nos cinco dias seguintes o Juiz emitirá uma sentença incontestável. Contudo, se o pedido de realização da audiência presencial for proposto conjuntamente por todas as partes, não há margem de discricionariedade para o Juiz que deverá dispor em conformidade.

¹⁶⁶ ITÁLIA. DECRETO DEL PRESIDENTE DELLA REPUBBLICA 13 febbraio 2001, n. 123 Regolamento recante disciplina sull'uso di strumenti informatici e telematici nel processo civile, nel processo amministrativo e nel processo dinanzi alle sezioni giurisdizionali della Corte dei Conti. Disponível em: <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:presidente.repubblica:decreto:2001-02-13;123!vig=>. Acesso em: 17 out 2024.

¹⁶⁷ ITÁLIA. Portale dei Servizi Telematici del Ministero della Giustizia. Disponível em: https://pst.giustizia.it/PST/resources/cms/documents/SPECIFICHE_TECNICHE_DM_44_2011REV_04.01.24.pdf. Acesso em: 17 maio 2024.

¹⁶⁸ ITÁLIA. Portale dei Servizi Telematici del Ministero della Giustizia. Disponível em: https://pst.giustizia.it/PST/resources/cms/documents/20231213DGSIATribunaleOnline_SpecificheTecniche_signed.pdf. Acesso em: 17 maio 2024.

Além das orientações acima elencadas, oriundas do Portal de serviço telemático, há o Provvedimento de 7 de dezembro de 2023 que aborda orientações sobre a realização de audiência por videoconferência, garantindo a publicidade, nos termos da lei¹⁶⁹.

A partir da análise sobre o ordenamento jurídico italiano foram identificadas poucas leis voltadas para a realização de audiências por videoconferência. Além disso, não se verifica a declaração expressa na lei sobre procedimentos, treinamentos ou demais atos que estejam atrelados especificamente sobre o assunto. Percebe-se que as leis, códigos, provimentos e demais regulamentações abordam atos no âmbito digital, trazem, inclusive discricionariedade para o juiz quanto a apresentação de memoriais. Entretanto, não é visualizada uma regulamentação dedicada exclusivamente para atos durante a realização de audiência remota.

Não há regras específicas de como devem ocorrer pregões que iniciam as audiências, coleta dos dados das partes e participantes das audiências, bem como, não há referência sobre como deve ser feito o procedimento posterior a finalização do ato. Não há designação legal sobre haver gravação, como se daria o manuseio, uso de práticas de segurança, elucidação das partes sobre o que acontecerá com os dados coletados e, ao final, como serão eliminados. Tampouco explica com detalhes sobre a não necessidade do consentimento da parte para o tratamento dos dados e nem exige que ocorra um esclarecimento para as partes do porquê de não haver obrigatoriedade de consentimento na coleta dos dados pessoais.

Observa-se que os regramentos analisados no presente tópico trazem informações generalistas, não trazendo especificidades quanto aos atos do poder judiciário. Pelas legislações estudadas aqui, percebe-se a regulamentação de forma ampla, sem abordagem sobre os procedimentos processuais judiciais detalhados e voltados para coleta, tratamento e armazenamento de dados pessoais.

Portanto, observa-se que não foram encontradas no ordenamento italiano leis que regulamentem a coleta, tratamento e armazenamento de dados pessoais oriundos das audiências remotas, bem como suas mídias gravadas. Não foi visualizada regra direcionada a procedimento em audiência por videoconferência quanto a explicações para as partes envolvidas no ato quanto ao procedimento de coleta de dados e o papel do judiciário nesse contexto.

¹⁶⁹ ITÁLIA. Portale dei Servizi Telematici del Ministero della Giustizia. Disponível em: https://pst.giustizia.it/PST/resources/cms/documents/m_dg.DOG07.09122023.0007511.ID_Regole_Tecniche_Udienze_da remoto_signed.pdf. Acesso em: 17 maio 2024.

Assim, espera-se que o ordenamento jurídico estabeleça diretrizes específicas para os atos judiciais remotos, como a audiência remota, que vem sendo estudada na presente pesquisa. Dessa forma, o GDPR foi passo regulatório significativo para a compreensão sobre a importância da proteção de dados. O que se faz necessário é que o judiciário alinhe suas atividades ao que está estabelecido no GDPR.

Regulamentações após a vigência da LGPD determinadas pelo Conselho Nacional de Justiça no Brasil para o Poder Judiciário quanto à proteção de dados durante os procedimentos judiciais

A Lei Geral de Proteção de Dados, nº. 13.709 de 2018¹⁷⁰ - LGPD, entrou em vigor no Brasil em setembro de 2020. Tornou-se o referencial normativo no que diz respeito a regulamentação sobre a matéria de proteção de dados no país. Essa lei busca garantir os direitos fundamentais de liberdade, privacidade, honra e imagem dos indivíduos, além de promover a transparência e a segurança no tratamento de dados pessoais

Como já dito nesse trabalho, o Brasil não iniciou suas previsões normativas sobre esse assunto a partir da LGPD, entretanto, foi após a sua vigência que o assunto foi tratado com mais especificidade em todos os setores sociais. Nesse sentido, a LGPD traz, tal como acontece com o GDPR, conceitos, regramentos, aplicações ou não aplicações da norma, os setores e demais instruções para condução sobre o tratamento do direito fundamental que é a proteção dos dados pessoais.

O presente tópico se propõe a abordar os regramentos posteriores a vigência da LGPD para a adequação do Poder Judiciário Brasileiro a proteção de dados. Isso porque a LGPD traz previsões gerais no âmbito judicial e a atividade do Judiciário enseja regras específicas para a sua atuação atendendo os preceitos da lei de proteção de dados.

Na LGPD, no art. 7º¹⁷¹ observam-se as possibilidades que autorizam os tratamentos de dados pessoais de forma ampla. Dentre os vários incisos, além de trazer a previsão de uso dos

¹⁷⁰ BRASIL. Lei nº. 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 29 abril 2024.

¹⁷¹ Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I - mediante o fornecimento de consentimento pelo titular;
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

dados pela administração pública, traz a hipótese de tratamento dos dados para exercício regular de direito em processos judiciais, administrativos e arbitrais.

Pode-se dizer que o artigo citado traz o primeiro direcionamento, no texto da lei, no que se refere a atividade jurisdicional. Entretanto, sabe-se que a abordagem trouxe apenas autorização de atuação, sendo necessário que outras normas específicas regulamentem a ação do poder judiciário em seus vários setores e procedimentos. Importante salientar que o §3º do artigo citado, considera que para o tratamento de dados pessoais seja de acesso público deve-se observar a finalidade, a boa-fé e o interesse público para que se justifique a disponibilização.

Aqui é necessário ressaltar, ao falar sobre processo judicial e o princípio da publicidade, que os dados coletados, tratados e armazenados pelo poder judiciário, como regra, estarão disponíveis ao público. Trata-se de um ponto que merece atenção e reflexão. Assim, é sensível

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

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

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

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

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

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

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

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

§ 1º [\(Revogado\)](#). [\(Redação dada pela Lei nº 13.853, de 2019\)](#)

§ 2º [\(Revogado\)](#). [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

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

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

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

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

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

essa análise porque inicialmente parece um contrassenso disponibilizar dados pessoais para acesso público. Há o princípio da publicidade, da informação, mas há também a privacidade da pessoa detentora dos dados e que disponibilizou para fins processuais, por exemplo. Há a prioridade da publicidade em relação à privacidade dos dados.

Compatibilizar a proteção de dados com a publicidade dos atos processuais demonstra-se uma tarefa excepcionalmente complexa. Isso pois, a priori, os referidos direitos são diametralmente opostos, na medida em que um prevê a proteção e tratamento de dados e o outro sua publicação para o acesso à sociedade¹⁷².

Nesse sentido, os dados coletados em processo judicial, durante uma audiência por videoconferência e que posteriormente são armazenados em repositórios digitais precisam ser pensados sob a ótica da publicidade, entretanto, contemporizando o direito fundamental à proteção de dados. Tal reflexão já foi discutida nessa pesquisa.

O parágrafo 6º do mesmo artigo traz a exigência de que o agente de tratamento de dados mantenha os devidos cuidados quanto aos dados pessoais coletados, ainda que o acesso a eles não tenha sido necessário o consentimento do titular. Nesse caso, o não consentimento para o tratamento de dados não exime a responsabilidade de que se mantenham as obrigações previstas em lei sobre o tratamento como a observância dos princípios gerais e a preservação das garantias do titular dos dados.

Além disso, o artigo 11 traz as hipóteses em que ficam autorizados os tratamentos de dados pessoais sensíveis. Mais uma vez permite o tratamento dos referidos dados, sem consentimento do titular dos dados e nas hipóteses em que forem indispensáveis, citando o processo judicial como uma das situações autorizadas.

Trata-se de ponto ainda mais frágil, pois tornar os dados sensíveis, de qualquer pessoa, disponíveis pode trazer prejuízos irreparáveis, visto que são dados que vulnerabilizam os titulares a estarem suscetíveis a situações constrangedoras. São informações que podem ocasionar discriminações entre outras circunstâncias e condições que ferem a dignidade da pessoa humana.

Outro ponto a se ressaltar, referente aos dados pessoais, é a possibilidade de transferência internacional autorizada no art. 33. Em específico, o inciso III¹⁷³ aborda a

¹⁷² GUIMARÃES, Glayder Daywerth Pereira et al. O princípio da publicidade dos atos processuais civis e o direito fundamental à proteção de dados pessoais: diretrizes para uma balize entre os direitos no Brasil. **Revista de Direito Magis**, v. 1, n. 2, 2022. Disponível em: <https://periodico.agej.com.br/index.php/revistamagis/article/view/17/15>. Acesso em: 17 out 2024.

¹⁷³ Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

possibilidade quando da necessidade de cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução.

A partir desse panorama sobre as previsões na LGPD que regulamentam o tratamento de dados durante a atuação do poder judiciário, parte-se para as normas específicas publicadas posteriormente a lei de proteção de dados, de acordo com as atividades desempenhadas em procedimentos judiciais.

Nesse sentido, entende-se que, no que tange a processo judicial, não há limitação que justifique o desrespeito à proteção dos dados quando coletados, tratados e armazenados pelo Poder Judiciário. Assim, a proteção deve ocorrer durante toda a tramitação processual e em todos os setores do judiciário.

Importante destacar, entretanto, que por questões metodológicas, o recorte de estudo feito na presente pesquisa refere-se à coleta, tratamento e armazenamento de dados pessoais quando da realização de audiências por videoconferência. Ressalte-se que os demais setores e procedimentos judiciais não estão isentos de seguirem as normativas referente à proteção de dados no judiciário.

Nessa seara, é importante considerar o Código de Processo Civil brasileiro de 2015¹⁷⁴, ainda que seja uma norma anterior a LGPD e demais regulamentações pré-existentes. Isso porque ele traz várias hipóteses que autorizam ou regulamentam atuação eletrônica ou uso de plataforma durante os processos judiciais.

Assim, por esse motivo, se faz necessário contextualizar o presente estudo considerando o Código Processual, pois a autorização para realização de atos e atividades processuais que utilizem ferramentas tecnológicas também podem envolver o tratamento de dados pessoais. Busca-se, assim, explicar a previsão normativa e a consonância com o que ocorre na prática cotidiana judiciária e a adequação à LGPD.

Desse modo, inicia-se a análise do CPC a partir da sessão II dessa lei, que é inaugurada com o art. 193. Essa parte do Código traz regras sobre a prática eletrônica de atos processuais. A lei autoriza a produção de atos, comunicados, armazenamento e validação por meios eletrônicos. Vale uma explicação sobre a sessão II, pois propõe regras e autorizações que

III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

¹⁷⁴ BRASIL. Lei 13.105 de março de 2015. Código de Processo Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/113105.htm. Acesso em: 07 maio 2024.

influenciam no modo como são coletados e tratados os dados pessoais dos participantes das audiências. Primeiro, o texto diz que os atos processuais podem ser total ou parcialmente digitais.

Destarte, permite que atos sejam produzidos, comunicados, armazenados e validados por meio eletrônico e na forma da lei. Aqui pode-se aduzir que por se tratar de uma previsão ampla, estejam incluídos, dentre os atos, aqueles realizados em audiência. Dessa forma, conclui-se que os dados pessoais podem ser coletados, tratados e armazenados em meio eletrônico, já que são procedimentos previstos durante a realização de audiência.

Por conseguinte, a referida sessão da lei processual, garante a publicidade dos atos processuais. Afirma que o registro dos atos processuais eletrônicos deverá ser feito em padrão aberto, respeitados os processos em segredos de justiça. Entende-se que padrão aberto está associado a transparência.

A lei que rege o processo civil garante o cumprimento do princípio da publicidade processual, que é um dos pilares do ordenamento jurídico brasileiro. Entretanto, abre-se nesse estudo, mais uma vez, a ressalva sobre inquietude a respeito do equilíbrio entre esse princípio e o direito fundamental de proteção dos dados pessoais processuais coletados durante as audiências por videoconferência.

Há a coexistência no ordenamento jurídico das garantias de proteção aos dados pessoais e a publicidade processual. A prevalência, em absoluto, de um em relação ao outro pode estar violando o direito do próprio cidadão. Desse modo, há de se encontrar alternativas para que ambos estejam protegidos.

A publicidade significa que a informação processual é pública, exceto os segredos de justiça. A proteção dos dados pessoais está relacionada a proteção do direito da personalidade. Nesse sentido, uma hipótese que pode contemporizar a existência de ambos, seria a criptografia ou a anonimização dos dados das pessoas envolvidas no processo, tendo em vista de que essas informações não são o cerne do processo no que diz respeito ao acesso a jurisprudência, por exemplo.

Sobre esse tema, Renan Silva, Lucas da Silva e Karen Silva explicam o impacto da LGPD na Publicidade dos atos processuais:

A LGPD, de fato, representa uma limitação ao princípio da publicidade, uma vez que sua aplicação importa em relativização do acesso amplo à informação, como ocorria antes da edição da Lei Geral de Proteção de Dados. Todavia, a limitação da ampla

publicidade não impõe uma falta de legitimação popular dos atos jurisdicionais, uma vez que se a legitimação do ato judicial não está vinculada à aceitação pública do teor do ato, e sim à sua publicidade. Por decorrência lógica, a legitimação do ato judicial também não está vinculada à exposição dos dados pessoais das partes. A legitimação dos atos judiciais, portanto, está ligada à publicação do teor do referido ato, não sendo necessária a exposição de dados pessoais para atingir sua finalidade. Neste ponto, a LGPD não promoveu ajustes na atividade do poder judiciário no sentido de alterar a lógica da publicidade como regra, sendo cabível, tão somente, a busca por garantir o direito à privacidade, importando numa devida harmonização entre os direitos fundamentais da publicidade, intimidade e da proteção de dados¹⁷⁵.

Nesse caminho, o CPC atribui ao Conselho Nacional de Justiça a responsabilidade de regulamentar a prática e comunicação dos atos processuais por meio eletrônico, autorizando os tribunais a fazerem de forma supletiva. Além disso, o CPC garante a incorporação progressiva dos avanços tecnológicos.

O referido artigo acima discutido está em consonância com o artigo 246 do mesmo diploma legal. Nele há a autorização de realizar citação por meio eletrônico, utilizando aqueles indicados pelo citando no banco de dados do Poder Judiciário. Na sequência da análise normativa processual, o artigo 334, §7º autoriza a realização de audiência por meio eletrônico para conciliações e mediações.

Tanto a conciliação quanto à mediação são tipos de procedimentos que também registram e coletam dados pessoais daqueles indivíduos que participam das sessões. Ainda que seja um processo judicial em sua fase inicial, trata-se de ato praticado pelo Poder Judiciário.

Ainda sobre o texto processual, há se falar sobre o art. 367, §5º que autoriza a gravação da audiência integral de imagem e áudio, em meio digital ou analógico, inclusive o §6º permite que seja feita diretamente por qualquer das partes (independente de autorização judicial). O referido artigo traz duas hipóteses que vulnerabilizam os dados pessoais que venham a ser coletados quando são realizadas gravações. Está autorizado fazer imagens (a imagem é um dado pessoal) da audiência. Quando a gravação é feita pelo judiciário, considera-se responsabilidade do tribunal a proteção do material que será armazenado nos meios digitais respectivos.

Quando, em uma hipótese, a gravação é feita pelas partes, durante a audiência, foge dos limites do tribunal em garantir a segurança do armazenamento de tais dados. Apesar de parecer ser uma forma de proporcionar publicidade, meio de prova, dentre outras questões implícitas,

¹⁷⁵ SILVA, Rennan Gonçalves; DA SILVA, Lucas Gonçalves; DE OLIVEIRA SILVA, Karen Thaiany Puresa. Impacto da LGPD na legitimação dos atos judiciais sob o prisma do princípio da publicidade. **Revista Direito & Paz**, v. 1, n. 46, p. 234-248, 2022. Disponível em: <https://revista.unisal.br/lo/index.php/direitoepaz/article/view/1651/657>. Acesso em: 17 out 2024.

é, em contrapartida, uma fragilidade quanto a segurança dos dados pessoais coletados. Não há proibição legal quanto a possibilidade de haver gravação do ato pelos interessados.

Outro artigo importante é o 385, §3º que autoriza a coleta de depoimento pessoal da parte por videoconferência ou outro recurso tecnológico de transmissão de sons e imagens em tempo real. O artigo ressalta que o ato é realizado durante a audiência de instrução e julgamento e fica permitido fazê-lo quando a parte estiver em comarca diversa daquela em que tramita o processo judicial.

O Código de Processo Penal Brasileiro também traz previsão de uso de meios tecnológicos em processo judicial. Em seu artigo 185, §2º¹⁷⁶ autoriza, como medida excepcional, o interrogatório do réu preso por sistema de videoconferência ou por outro recurso tecnológico de transmissão de sons e imagens em tempo real e diz as situações específicas em que esse modo pode acontecer.

Após a análise da abordagem processual brasileira, é necessário estudar as regulamentações específicas sobre as realizações dos atos processuais em meio digital. Fala-se aqui sobre resoluções, portarias que foram elaboradas para as especificidades de alguns procedimentos processuais.

As resoluções são advindas do Conselho Nacional de Justiça ou do próprio tribunal para a realização dos seus atos. Assim como podem emitir portarias com direcionamentos para a realização dos atos no ambiente digital. Tais normativas tem o intuito de trazer as especificidades que a LGPD não abordou. O tribunal pode emitir regras a serem aplicadas para proporcionar melhor prestação jurisdicional e que estejam adequadas a lei de proteção de dados.

O objetivo de trazer as leis que já abordavam antes do regulamento a temática tecnológica no meio processual é contextualizar o arcabouço normativo pré-existente à LGPD. Desse modo, se permite fazer uma análise sobre como se entrelaçam as referidas normas com as exigências da lei de proteção de dados entrando em vigor. Além disso, busca-se identificar nas referidas regras se há previsão sobre como proceder com a coleta de dados pessoais e demais garantias a serem tomadas para proteger o direito a privacidade e as informações pessoais.

¹⁷⁶ BRASIL. Decreto Lei nº 3.689 de 3 de outubro de 1941. Código de Processo Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 29 abril 2024.

Desse modo, cita-se a Resolução nº. 105 de 06 de abril de 2010 do Conselho Nacional de Justiça - CNJ¹⁷⁷. Tal documento dispõe sobre a documentação dos depoimentos por meio do sistema audiovisual e realização de interrogatório e inquirição de testemunhas por videoconferência. Trata-se de regulamentação sobre o uso de ferramentas tecnológicas para um momento processual específico. Inclusive ao falar sobre depoimento de testemunha que resida em local diverso daquele que tramita o processo, deve ser um procedimento precedido de carta precatória. Isso porque buscou preservar o princípio da identidade física do juiz.

É importante mencionar que a Resolução nº. 105 é anterior ao Código de Processo Civil vigente no Brasil. Essa ressalva se faz necessária porque o documento faz referência a artigo desse código no que se refere a garantia da autenticidade, integridade, temporalidade, não repúdio, conservação e assegura confidencialidade nos casos de segredo de justiça.

Para fins da Resolução acima listada, cite-se a Resolução nº. 222 de 13 de maio de 2016¹⁷⁸ que altera a Resolução nº. 105 em alguns pontos. Nesse sentido, acrescenta que o Conselho Nacional de Justiça - CNJ irá disponibilizar sistemas eletrônicos para gravação dos depoimentos, interrogatórios e inquirição de testemunhas. Além disso, autoriza que os tribunais possam desenvolver repositórios de mídias de armazenamento de documentos de som e imagem, inclusive os decorrentes da instrução do processo.

Importante refletir acerca da existência de sistemas eletrônicos de gravação e de repositórios de armazenamentos de documentos de som e imagem. Como falado mais acima, a permissão da gravação, como autoriza também o CPC, bem como a existência de repositórios são pontos sensíveis.

Ainda que seja necessária a existência do conjunto documental, trata-se, ao mesmo tempo, de algo que necessita de atenção no que tange a manutenção da segurança dos dados contidos nas gravações e nos repositórios. Essa segurança começa a ser essencial desde o momento em que ocorre a coleta dos dados pessoais na realização das audiências por videoconferência.

Continuando sobre os documentos que regulamentam a matéria de uso de tecnologia da informação em processo judicial, é importante falar sobre a Portaria 61 de 31 de março de 2020

¹⁷⁷ BRASIL. Resolução nº. 105 de 06 de abril de 2010 do Conselho Nacional de Justiça. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/166>. Acesso em: 30 abril 2024.

¹⁷⁸ BRASIL. Resolução nº. 222 de maio de 2016 do Conselho Nacional de Justiça. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/atos-normativos?documento=2283>. Acesso em 30 abril 2024.

do CNJ¹⁷⁹. Isso porque essa regulamentação surgiu para legitimar o uso de plataformas emergenciais para audiências por videoconferência durante o período pandêmico do COVID-19. O momento atípico ensejou a necessidade de determinações regulatórias urgentes, pois não havia uma prescrição legal que atendesse às necessidades processuais daquele período.

O Conselho Nacional de Justiça, através da referida portaria, disponibilizou uma plataforma emergencial para a realização de audiências por videoconferência, a Cisco Brasil Ltda¹⁸⁰¹⁸¹. O uso da ferramenta aconteceu sem custos para os tribunais, em todos os graus de jurisdição e incluiu os tribunais superiores. O interesse pelo uso deveria ser manifestado por meio de formulário eletrônico no portal do CNJ. Importante mencionar que a Portaria autoriza a utilização de outras ferramentas computacionais, permitindo a gravação do conteúdo audiovisual e o seu armazenamento.

A gravação que fosse armazenada utilizava o PJe mídias¹⁸² (Processo Judicial Eletrônico Mídias), se assim fosse desejado. Saliente-se que a referida plataforma ficou disponível durante o período pandêmico. Depois disso, cada Tribunal ficou responsável por gerir a sua plataforma. Após a entrada em vigor da Portaria nº 61, o CNJ segue com a publicação da Resolução nº 317 de abril de 2020¹⁸³. Tal resolução também prevê medidas processuais em razão do período de isolamento provocado pela pandemia do Covid-19.

O texto aborda a realização de perícias em meios eletrônicos ou virtuais em ações previdenciárias que discutam benefícios assistenciais previdenciários. Aqui faz-se necessário refletir sobre um ponto importante. Observa-se que a Resolução permite a realização de

¹⁷⁹ BRASIL. Portaria nº. 61 de 31 de março de 2020. Institui a plataforma emergencial de videoconferência para realização de audiências e sessões de julgamento nos órgãos do Poder Judiciário, no período de isolamento social, decorrente da pandemia do Covid-19. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3266>. Acesso em: 29 abril 2024.

¹⁸⁰ BRASIL. Conselho Nacional de Justiça. Plataforma Emergencial de videoconferência para atos processuais. Disponível em: <https://www.cnj.jus.br/plataforma-videoconferencia-nacional/>. Acesso em: 29 abril 2024.

¹⁸¹ BRASIL. Conselho Nacional de Justiça. Disponível em: <https://paineisanalytics.cnj.jus.br/single/?appid=a89ef492-f81e-4679-a58f-f7caa7452d82&sheet=740707b2-b87f-4ac0-a185-b430f855e682&lang=pt-BR&opt=cursel&select=clearall>. Acesso em 08 maio 2024.

Do período de 01/04/2020 a 14/05/2020 foram realizadas 1.255.375 reuniões pela plataforma Cisco Webex, com uma média de 48 minutos de duração e uma média de 6 participantes. Dados do CNJ
¹⁸² Art. 4º A Plataforma permitirá a gravação audiovisual do conteúdo da videoconferência, e seu armazenamento, caso desejado, poderá ocorrer no sistema denominado PJe Mídias.

¹⁸³ BRASIL. Resolução 317 de abril de 2020 do Conselho Nacional de Justiça. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3302#:~:text=Disp%C3%B5e%20sobre%20a%20realiza%C3%A7%C3%A3o%20de,Coronav%C3%ADrus%2C%20e%20d%C3%A1%20outras%20provid%C3%A2ncias.Ac>esso em: 30 abril 2024.

audiências por videoconferência para a análise dos critérios de concessão de benefícios previdenciários.

Os benefícios que podem ser discutidos, de acordo com a Resolução, são aqueles concedidos em razão de incapacidade ou aqueles assistenciais. Para identificar a incapacidade ou a necessidade de benefício assistencial, faz-se necessária a análise de documentos e realização de perícia, considerando o que puder ser feito por videoconferência.

O ponto em questão que deve ser ressaltado é que as informações apresentadas para tais análises são dados pessoais sensíveis. O artigo 1º, §1º, inciso II diz com clareza que podem ser juntados aos autos documentos do periciado que sejam necessários, inclusive médicos.

A Lei Geral de Proteção de Dados, em seu artigo 5º, II¹⁸⁴ esclarece que dentre os dados sensíveis estão os dados referentes à saúde da pessoa. A reflexão segue no sentido de que o armazenamento dos dados nos repositórios não só contém dados pessoais, como também os dados sensíveis.

Cita-se, nesse momento da pesquisa, o texto da LGPD por poder compreender o conceito do que vem a ser dados pessoais sensíveis e o porquê de serem assim chamados. Sabe-se que à época da publicação da Resolução a LGPD ainda não estava em vigor, mas o seu teor já era bastante discutido entre os especialistas na matéria.

Importante ressaltar que os dados sensíveis são aqueles que podem colocar a pessoa em situações constrangedoras, de preconceito, discriminação. A proteção dessa categoria é de relevância ainda maior, é proteção a um direito fundamental intimamente ligado à dignidade da pessoa humana e abrange um lado vulnerável e frágil de qualquer indivíduo.

Em momento posterior a Resolução acima citada, é publicada a Resolução 337 de 29 de setembro de 2020¹⁸⁵. Esta vem com o intuito de abordar o tema de Tecnologia da Informação e Comunicação; Gestão da informação e demandas judiciais.

Esta Resolução traz a diretriz para que cada tribunal adote um sistema de videoconferência para suas audiências e atos oficiais. Isso porque as demandas para realização de audiências, sessões, reuniões continuaram existentes.

¹⁸⁴ BRASIL. Lei nº. 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 30 abril 2024.

¹⁸⁵ BRASIL. Resolução nº. 337 de 29 de setembro de 2020 do Conselho Nacional de Justiça. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3498>. Acesso em: 30 abril 2024.

Um ponto a ser analisado sobre essa Resolução é que ela permite que os tribunais optem livremente sobre qual sistema devem adotar a partir de então. Inclusive autoriza que possam ser soluções tecnológicas disponíveis no mercado de forma onerosa ou gratuita, desde que compatíveis com o sistema processual eletrônico adotado pelo tribunal.

A gratuidade quanto ao uso de ferramentas tecnológicas não necessariamente apresenta o mesmo nível de segurança quanto aquelas que são utilizadas de forma onerosa. Sem dúvidas, o uso de forma gratuita desonera o orçamento do tribunal, entretanto, pode vulnerabilizar ainda mais os dados que são coletados e posteriormente armazenados nos repositórios dos tribunais.

Ainda que em seu artigo 3º traga a informação de que o sistema deve garantir segurança, privacidade e a confidencialidade das informações compartilhadas, a gratuidade de plataformas e ferramentas tecnológicas tem seus prós e contras. E o contra pode ser a fragilidade na segurança.

Na sequência de regulamentações, é publicada em 9 de outubro de 2020 a Resolução nº. 345 de 2020¹⁸⁶. Essa Resolução traz uma inovação, pois autoriza a adoção do “Juízo 100% Digital” no Poder Judiciário. Essa regulamentação traz a oportunidade de realização de todos os atos e procedimentos processuais por meio digital. Desde a realização de audiências por videoconferência até os atendimentos feitos pela secretaria ou pelo juiz.

Trata-se de uma opção a ser manifestada na petição inicial, além de indicar os meios de comunicação, como número de telefone e endereço eletrônico. Refrisa que ficam admitidas citações, intimações e notificações por qualquer meio eletrônico, assim como já prevê o Código de Processo Civil.

A escolha pelo “Juízo 100% Digital” não é obrigatória e dependerá da aceitação da parte contrária para continuidade. Essa terá até a contestação para se opor a utilização desse procedimento. Sobre essa Resolução, dentre tantas regras, está a determinação da realização audiências e sessões por videoconferência de forma exclusiva, quando se opta pelo procedimento de “Juízo 100% Digital”.

Aqui a reflexão é no sentido de que sempre que houver a opção pelo referido procedimento, haverá de ter a audiência por videoconferência. Isso quer dizer que

¹⁸⁶ BRASIL. Resolução nº. 345 de 9 de outubro de 2020 do Conselho Nacional de Justiça. Disponível em: <https://atos.cnj.jus.br/files/original175500202010145f873b7482503.pdf>. Acesso em: 8 maio 2024.

necessariamente haverá utilização de plataformas digitais, bem como a coleta de dados pessoais dos participantes e posterior armazenamento nos repositórios dos tribunais.

Observe-se também que essa Resolução é publicada no mês posterior ao da entrada em vigor da Lei Geral de Proteção de Dados no Brasil. Em 18 de setembro de 2020 passou a vigorar a LGPD. A partir disso, todo o ordenamento jurídico precisa estar em consonância com o previsto na lei de proteção de dados.

A próxima Resolução a ser debatida que regula matéria de tecnologia da informação, gestão da informação e de demandas judiciais, gestão e organização judiciária e transparência é a de nº. 363 de janeiro de 2021. Tal Resolução tem o objetivo de adequação das medidas adotadas pelo judiciário à Lei Geral de Proteção de Dados. As medidas são direcionadas para todos os tribunais do país, exceto o Supremo Tribunal Federal.

Dentre as medidas designadas na Resolução nº. 363, estão: a criação de Comitê Gestor de Proteção de Dados Pessoais, designar encarregado por tratamento de dados pessoais, formar grupos com trabalhos técnicos multidisciplinares que auxiliem o encarregado, criação de sistema de comunicação através de canais próprios e em parceria com as ouvidorias dos tribunais, cria site com informações sobre aplicação da LGPD nos tribunais, bem como disponibilizar informações adequadas sobre o tratamento dos dados pessoais.

Além disso, incluindo os serviços extrajudiciais, a resolução prevê a organização de programa de conscientização sobre a LGPD. Isso é, que todos os serventuários da justiça (magistrados, servidores, terceirizados, estagiários, residentes judiciais, área administrativa e judiciais de 1ª e 2ª instâncias e Côrtes Superiores, exceto o STF) atuem em conformidade com a LGPD.

Aqui é importante tecer alguns comentários. Para alcançar a conscientização de todos aqueles envolvidos em um processo judicial, por exemplo, se faz necessário o conhecimento prévio da legislação. Após o conhecimento, se faz necessário compreender a sua aplicação à realidade de cada atividade. Entende-se que não basta a simples informação de que se faz necessário o respeito e conhecimento da legislação.

Nesse sentido, para que um trabalho conjunto em um processo judicial esteja em conformidade com os preceitos da LGPD é necessário que haja um conhecimento para além da simples leitura. O trabalho daqueles que lidam com dados pessoais precisa ser no mesmo sentido de compreensão sobre a matéria.

Aqueles que lidam com a coleta, tratamento e armazenamento de dados pessoais durante a realização de uma audiência por videoconferência precisam ter a ciência da seriedade com o que estão trabalhando. É necessário o conhecimento dos possíveis riscos e desafios que se encontram nas atividades cotidianas dos atos judiciais. Isso se traduz em responsabilidade, porque aquele que trata ou que opera efetivamente com o dado, se torna responsável por ele. Sobre agente e operador, Maria Eugênia e Claudio explicam a responsabilidade dos agentes e operadores:

Eles são responsáveis também por assegurar a segurança das informações que realizam tratamentos, devendo se precaver para que pessoas não autorizadas tenham acesso a elas. Em caso de infrações à Lei, os agentes de tratamento poderão responder por sanções administrativas, que podem variar de advertências a multas¹⁸⁷.

Para isso, a propagação da informação, do conhecimento sobre tudo que circunda o conteúdo de proteção de dados em âmbito judicial pode minimizar os riscos de vazamentos e usos indevidos dos dados coletados durante um processo judicial. Ainda que a resolução traga todas as diretrizes sobre o que precisa ser feito por cada tribunal no país, é necessário que os tribunais promovam internamente as políticas que propiciem a correta adequação à legislação.

Aqui vale citar o artigo 47 da LGPD que atribui a responsabilidade de garantir a segurança da informação ao agente ou qualquer outra pessoa que intervenha em uma das fases do tratamento dos dados pessoais. Ainda no art. 49 estabelece que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma que atendam os requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na lei e demais normas regulamentares.

A resolução 363 de 2021 instrui no sentido de adequação à LGPD e traz as recomendações de forma esmiuçada, de modo que consiga atingir às diversas situações em que o processo judicial e as atividades administrativas estejam envolvidas. Nesse sentido, o CNJ publicou a resolução nº. 372 de 12 de fevereiro de 2021¹⁸⁸ com o intuito de abordar o tema de gestão da informação e de demandas judiciais e a gestão e organização judiciária, tratando do “Balcão Virtual”.

¹⁸⁷ FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. Privacidade e lei geral de proteção de dados pessoais. **Revista de Direito Brasileira**, v. 23, n. 9, p. 284-301, 2019. Disponível em: <https://indexlaw.org/index.php/rdb/article/view/5343/4545>. Acesso em: 17 out 2024.

¹⁸⁸ BRASIL. Conselho Nacional de Justiça. Resolução nº. 372 de 12 fevereiro de 2021. Dispõe sobre Gestão da Informação e de Demandas Judiciais; Gestão e Organização Judiciária. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3742>. Acesso em 16 maio 2024.

Trata-se da disponibilização da ferramenta de videoconferência, nos sítios eletrônicos de todos os tribunais, excetuando o STF, para que advogados (as) e partes possam ter atendimento tal como acontece de forma física em balcões das secretarias de varas.

A Resolução intitula a plataforma de videoconferência de “Balcão Virtual” e dá as outras providências para as situações em que não sejam possíveis uso da tecnologia por deficiência de infraestrutura. Nesses casos, determina que seja utilizada outra forma de comunicação assíncrona e que as respostas dos solicitantes sejam dadas em tempo razoável.

Assim, inegável a facilidade que o uso de “Balcão Virtual” permite aos usuários. O atendimento pode ser realizado de qualquer lugar, evitando a necessidade de deslocamento da pessoa ao fórum. Entretanto, ocorre a preocupação sobre a coleta de dados que acontece durante o atendimento pela plataforma. Há coleta de dados nesse procedimento, e entende-se que seja necessária para que as partes possam direcionar as dúvidas identificando o processo objeto de atendimento.

Todavia, a coleta de dados nesse caso também requer cuidados que garantam a segurança das informações apresentadas. A partir da análise das legislações que antecederam a Lei Geral de Proteção de Dados que contextualiza a sequência de estudo sobre as regulamentações que surgiram após a publicação e vigência da LGPD, pôde-se compreender o engajamento para a adequação do judiciário à referida lei.

Esse estudo panorâmico normativo proporciona o conhecimento sobre a base necessária para a segurança sobre o tema de proteção de dados no Brasil. Entende-se que não é matéria exaustiva no que diz respeito a regulamentação. Indubitavelmente, as atualizações deverão ser uma constante. Desenvolvimento tecnológico e demais iniciativas digitais serão cada vez mais utilizadas no direito e, por conseguinte, no judiciário.

As atividades do judiciário e os operadores do direito acompanharão os avanços tecnológicos, de acordo com as necessidades e utilidades. Por isso, torna-se necessário o constante debate sobre as problemáticas oriundas das novas formas de trabalho no direito.

Desse modo, compreende-se que a direção normativa nacional, dada até o presente momento, como apresentado nesse tópico, oportuniza um ideal de uso consciente das ferramentas tecnológicas imaginando estar adequado às exigências legais e às necessidades processuais, judiciais e da sociedade. Assim, a partir das normativas e regulamentações nacionais, cabe ao Poder judiciário de cada estado compreender as dificuldades, os desafios e

as necessidades da sua região de modo que possa colocar em uso o que ficou determinado pelo legislador e regulador.

No Decreto Ministerial nº 44 de 21 de fevereiro de 2011¹⁸⁹ ficaram estabelecidas regras técnicas para o processo civil e penal no que diz respeito à tecnologia da informação e comunicação. Dentre as prescrições técnicas estão requisitos sobre segurança no tratamento dos dados visando protegê-los de acessos por pessoas não autorizadas, perdas, divulgações não permitidas. Além disso, preceitua que sejam utilizados métodos de autenticação forte, criptografia e assinaturas eletrônicas.

Importante mencionar que há a abordagem sobre a estrutura de gestão informática no que diz respeito a base de dados e devem ser uniformes e seguras a nível nacional. O que se pode compreender no ordenamento jurídico brasileiro é que há muitas iniciativas normativas para regular diversas atividades remotas, incluindo a realização de audiências por videoconferência. Entretanto, esbarra na mesma dificuldade visualizada no ordenamento italiano. Não há regramento detalhado voltado para os procedimentos de coleta de dados durante essas audiências.

Percebe-se que as normativas ainda estão sendo desenvolvidas e apresentam-se distantes no que diz respeito a preverem protocolos de segurança para a coleta, tratamento e armazenamento de dados. Dessa forma, tanto a Itália, quanto o Brasil, possuem regramentos insuficientes, dentro do que foi encontrado, para cobertura do cotidiano judiciário das realizações de audiências por videoconferência. Isso porque, não se identificou regras específicas para a realização do ato de coleta de dados pessoais dos envolvidos em audiência remota, bem como, nenhuma exigência sobre esclarecimentos específicos para os titulares dos dados sobre o uso de seus dados pessoais.

Portanto, o regramento encontrado na pesquisa é insuficiente quanto a prever o passo a passo das condutas a serem realizadas nas audiências remotas. Apenas tem-se os regulamentos

¹⁸⁹ ITÁLIA. Decreto 21 febbraio 2011, nº. 44. Regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale, delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2, del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010 n. 24. (11G0087) (GU Serie Generale n.89 del 18-04-2011). Disponível em: <https://www.gazzettaufficiale.it/eli/id/2011/04/18/011G0087/sg>. Acesso em: 28 maio 2024.

que trazem as regras amplas no que diz respeito ao exercício da prestação jurisdicional, mas as regras específicas que devem vir subsequentemente, ainda se encontram de forma primária, sejam as resoluções, sejam outras espécies de regulações. Se faz necessário não apenas que sejam criadas regras e protocolos específicos para a coleta de dados pessoais durante as audiências por videoconferência, mas que aborde com mais detalhes a operação de realização de audiências remotas.

Importância do acompanhamento da adequação do judiciário às leis de proteção de dados e a vulnerabilidade desse direito

Aspectos Gerais

Analisando a importância da proteção dos dados pessoais no atual contexto atual do desenvolvimento humano e tecnológico, como está sendo proposto no presente trabalho de pesquisa, é necessário compreender como os setores sociais estão se adequando às normativas regulatórias sobre esse direito fundamental.

Nos primeiros capítulos foram apresentadas as legislações relacionadas a temática, bem como, o desenvolvimento normativo posterior às referidas leis. Foi feita a reflexão sobre o posicionamento internacional, as iniciativas regulatórias e visões sobre o que vem a ser proteção de dados no contexto social, considerando o ciberespaço.

Dessa forma, compreende-se que estabelecer um controle acerca do cumprimento legal sobre proteção de dados pessoais é essencial para preservação dos direitos dos cidadãos. Isso porque deve existir uma busca em minimizar os riscos de violação da privacidade dos titulares desses dados nas circunstâncias em que estiverem sendo tratados.

Essa preocupação decorre do fato de que se não houver segurança na coleta, tratamento e armazenamento dos dados pessoais, pode torná-los vulneráveis cibernéticos. Atentando-se ao fato de que os dados estão na rede mundial de computadores, dessa forma, estão passíveis de serem violados a partir de alguma invasão.

Uma vez que a segurança não venha a ser implementada ou seja implementada de forma que não atenda o mínimo de proteção, caso ocorra alguma apropriação do sistema por hackers, os dados pessoais estão passíveis de sofrerem ataques cibernéticos.

A título de exemplo, o Tribunal Superior Eleitoral¹⁹⁰ sofreu um ataque de hacker no primeiro semestre de 2024. Nesse caso, foi desviado R\$1,2 milhão a uma empresa terceirizada de tecnologia da informação. Há suspeita de que informações pessoais e empresariais foram utilizadas.

Ainda em 2020, o Superior Tribunal de Justiça¹⁹¹ sofreu ataque de hackers o que fez suspender os prazos processuais. Tal problema ocasionou inclusive suspensão da realização de audiências por videoconferência.

Nesse sentido, o Poder Judiciário, como serventário social e porta de acesso à justiça, também está compreendido dentre os que devem cumprir as normativas relativas à proteção de dados. Para isso, não basta apenas haver a previsão legal genérica sobre o assunto. É necessário acompanhamento das atividades e fiscalização sobre a adequação à legislação de proteção de dados.

Na sequência do estudo, observou-se os legisladores, das normas analisadas no presente trabalho, que regularam a proteção de dados pelo judiciário em capítulo separado, entretanto, a matéria é apresentada de forma ampla em tais normativas. Isso significa que há necessidade de regras específicas para o exercício das atividades judiciais.

O art. 23 do GDPR, por exemplo, permite flexibilidade para que os Estados-membros possam fazer ajustes em suas legislações para atender as necessidades de cada sistema judicial, bem como, garanta a segurança pública.

Dessa forma, a regulação direcionada proporciona que o trabalho do judiciário fique mais próximo do ideal quanto a proteção de dados, atendendo o objetivo do legislador nacional, no caso do Brasil a LGPD, e europeu, no caso do GDPR sobre proteção do direito fundamental aqui discutido.

¹⁹⁰ CISO Adviso. Ataque ao TSE desviou R\$ 1,2 mi a uma empresa terceirizada de TI. 29/04/2024. Disponível em: <https://www.cisoadvisor.com.br/ataque-ao-tse-desviou-r-12-mi-uma-empresa-terceirizada-de-ti/>. Acesso em: 18 jul 2024.

¹⁹¹ TECNOBLOG. STJ sofre ataque hacker e suspende atividades por uma semana. Disponível em: <https://tecnoblog.net/noticias/stj-sofre-ataque-hacker-e-suspende-atividades-por-uma-semana/>. Acesso em: 18 jul 2024.

Para a referida adequação judicial, é necessário um instrumento efetivo de controle. Se faz necessário um agente, órgão ou instituição que possam realizar o trabalho de regulação específica das atividades judiciais, bem como o controle do respectivo cumprimento da legislação pertinente.

No Brasil, o trabalho é realizado pela instituição Pública chamada Conselho Nacional de Justiça – CNJ¹⁹² que tem o papel de aperfeiçoamento do trabalho do sistema judiciário brasileiro, principalmente sobre controle e transparência administrativa e processual. O CNJ desenvolve e coordena vários programas de âmbito nacional que priorizam áreas como Gestão Institucional, Meio Ambiente, Direitos Humanos e Tecnologia.

Já na Itália, o trabalho semelhante é desenvolvido pelo *Ministro della Giustizia*¹⁹³ que exerce um papel importante. O Ministro está voltado para elaboração e implementação das regulamentações no âmbito judicial.

Além do Ministro, há ainda a atividade do *Consiglio Superiore della Magistratura*¹⁹⁴ que possui poderes relevantes sobre organização da informática judiciária, respeitando as competências do *Ministro della Giustizia*. O *Consiglio* Estabelece regras gerais, objetivas e predefinidas para atribuições dos juízes e dos processos e tem o poder de adotar atos normativos de caráter geral sobre regulamento interno e regulamento de administração, por exemplo, dentre outros. É voltado para a administração e disciplina dos juízes.

La Costituzione prevede dunque le **due funzioni fondamentali** del Ministro: **l'organizzazione dei servizi** e la **titolarità dell'azione disciplinare** nei confronti dei magistrati. Le altre funzioni sono definite con legge ordinaria¹⁹⁵¹⁹⁶.

Dessa forma, fica demonstrado que é necessária a constante análise do funcionamento dos trabalhos do poder judiciário para que estejam em conformidade com a previsão legal. Ao

¹⁹² BRASIL. Conselho Nacional de Justiça. Disponível em: <https://www.cnj.jus.br/sobre-o-cnj-3/>. Acesso em: 27 maio 2024.

¹⁹³ ITÁLIA. Ministero della Giustizia. Circolare 31 maggio 2019 - Regolamento generale sulla protezione dei dati (regolamento ue 2016/679) - valutazione d'impatto sulla protezione dei dati (cd. dpia) - istruzioni operative e modulistica. Disponível em: https://www.giustizia.it/giustizia/it/mg_1_8_1.page?contentid=sdcl94013&previouspage=mg_1_8. Acesso em: 28 maio 2024.

¹⁹⁴ ITÁLIA. Consiglio Superiore della Magistratura. Disponível em: <https://www.csm.it/web/csm-internet/csm/attribuzioni-e-funzionamento>. Acesso em: 28 maio 2024.

¹⁹⁵ ITÁLIA. Consiglio Superiore della Magistratura. Disponível em: <https://www.csm.it/web/csm-internet/csm/attribuzioni-e-funzionamento>. Acesso em: 28 maio 2024.

¹⁹⁶ Tradução livre: A Constituição prevê assim as duas funções fundamentais do Ministro: a organização dos serviços e a titularidade da ação disciplinar contra os magistrados. As demais funções são definidas pela lei ordinária.

mesmo tempo, o acompanhamento do trabalho judiciário serve também para que outras regulações sejam elaboradas frente aos novos desafios na sociedade hiperconectada.

É importante abordar o cenário da hiperconectividade, o que quer dizer comunicação intensa utilizando tecnologia e internet e acontece de forma constante. Trata-se de um fenômeno característico da era digital e abrange várias relações, desde as pessoas até a relação com as coisas, diga-se internet das coisas.

Chega-se, portanto, ao que se convencionou denominar hiperconectividade, na vida pública e na vida privada, via Internet, Intranet, Deep Web ou Dark Web, partindo-se da concepção de que, cada vez mais se impõe às pessoas se conectarem a alguma rede, especialmente a Internet, para interagir com o Estado, com as empresas e com as demais pessoas, de forma geral¹⁹⁷.

O estudioso Magrani traça algumas palavras sobre o assunto, dizendo que o termo hiperconectividade foi cunhado, inicialmente, para descrever o estado de disponibilidade dos indivíduos para se comunicar a qualquer momento:

Este termo possui alguns desdobramentos importantes. Podemos citar alguns deles: o conceito de always-on, estado em que as pessoas estão conectadas a todo o momento; a possibilidade de estar prontamente acessível (readily accessible); a riqueza de informações; a interatividade; e o armazenamento ininterrupto de dados (always recording). O termo hiperconectividade encontra-se hoje atrelado às comunicações entre indivíduos (person-to-person, P2P), indivíduos e máquina (human-to-machine, H2M) e entre máquinas (machine-to-machine, M2M) valendo-se, para tanto, de diferentes meios de comunicação. Há, neste contexto, um fluxo contínuo de informações e massiva produção de dados¹⁹⁸.

Nesse diapasão, um dos desafios desse formato de relação de comunicação e atividade social é a segurança. Tratando de dados pessoais, estes fazem parte desse cenário da conectividade. É um dos objetos que está entre o tráfego de informações.

Isso quer dizer que um trabalho efetivo e minucioso de controle em matéria de proteção de dados no judiciário permite identificar falhas de sistemas, bem como de rotinas que venham a vulnerabilizar os dados coletados pelo judiciário. Nesse sentido, o controle jurisdicional permite o constante aperfeiçoamento, tanto regulatório, quanto de capacitação dos serventuários da justiça.

¹⁹⁷ DE TARSO BRANDÃO, Paulo; BOUMANN, Gabrielle Amado. A INSERÇÃO DIGITAL DE QUALIDADE COMO DIREITO FUNDAMENTAL NA ERA DE HIPERCONECTIVIDADE: O DIREITO A ACESSAR DIREITOS. **Revista de Direito, Governança e Novas Tecnologias**, v. 7, n. 2, p. 91-112, 2021.

¹⁹⁸ MAGRANI, Eduardo. Ética e privacidade na era da hiperconectividade. Rio de Janeiro: Konrad Adenauer Stiftung, 2018. P. 15-16. Apud DE TARSO BRANDÃO, Paulo; BOUMANN, Gabrielle Amado. A INSERÇÃO DIGITAL DE QUALIDADE COMO DIREITO FUNDAMENTAL NA ERA DE HIPERCONECTIVIDADE: O DIREITO A ACESSAR DIREITOS. **Revista de Direito, Governança e Novas Tecnologias**, v. 7, n. 2, p. 91-112, 2021.

Sobre segurança da informação, Carlos Alberto da Silva explica:

A segurança da informação é algo que atualmente tem levantado inúmeros debates sobre o tema, que possuem como intuito encontrar novas maneiras de proteção a todo o momento. A proteção a dados passa por diversas áreas e a manipulação de informações de maneira adequada não visa apenas assegurar que dados estão protegidos. A segurança da informação possui como objetivo também evitar crimes. Entende-se que a segurança da informação não é apenas uma área de TI, mesmo que esta apresenta inúmeras ferramentas de proteção a dados. Quando se trata de proteção a dados em ambientes organizacionais, esta proteção deve envolver todos os departamentos e deve ter total comprometimento do grupo diretivo. Contudo, compreende-se de forma geral que a segurança da informação passa por três áreas principais. A tecnologia, o direito e a psicologia¹⁹⁹.

O autor explica que a tecnologia traz os recursos que quando bem aplicados trazem alto nível de segurança. O direito aplica sanções quando ocorre o uso indevido das informações e a psicologia enxerga que o maior desafio sobre proteção de dados está nas pessoas. Ele entende que a orientação de como mitigar os riscos que surgem do comportamento humano e compreender como as características humanas podem ajudar sobre como as pessoas lidam os riscos de informações secretas em risco.

Diante disso, se faz necessário analisar os regramentos gerais e os emitidos pelo *Ministero della Giustizia*, assim como aqueles remetidos ao Conselho Nacional de Justiça, como já feito nos capítulos anteriores, sobre proteção de dados e orientações de procedimentos de segurança. A partir disso, estabelecer um confronto com o cotidiano do judiciário a respeito da fiscalização quanto adequação à regulação de proteção de dados.

Essa análise realizada no presente trabalho instrui para posterior interpretação dos relatórios produzidos pelo judiciário como resultado para acompanhamento e identificação de possíveis riscos de segurança dos dados nas atividades judiciais. São informações que permitem identificar possíveis falhas no tratamento dos dados pelo judiciário.

Conforme a *Circolare 31 maggio 2019* emitida pelo *Ministero della Giustizia*, a Avaliação de Impacto na Proteção de Dados deve conter documentos detalhados e indicar os responsáveis pelo tratamento dos dados. Tais documentos devem descrever os riscos, as medidas adotadas e a fundamentação das medidas tomadas para minimizar os riscos sobre a segurança dos dados.

Sendo assim, o presente capítulo tem o intuito de analisar os relatórios emitidos pelas instituições acerca do tratamento de dados pelo Poder judiciário no processo judicial eletrônico,

¹⁹⁹ SILVA, Carlos Alberto. O elo mais fraco da segurança da informação. Pessoas representam o maior desafio. Oliveira MG, 2015. Livro digital. P. 92-93.

em especial nas audiências por videoconferência. Trata-se de um ponto da atividade jurisdicional, o que não exclui a necessidade de dar efetividade à regulação nas demais funções jurisdicionais.

Além disso, para complementar o estudo feito sobre os relatórios esse trabalho de pesquisa se propôs a desenvolver um questionário designado a um tribunal brasileiro e a um tribunal italiano. O objetivo é exemplificativo, o que não impede um posterior aprofundamento em outras pesquisas sobre outros tribunais brasileiros e italianos para fins obtenção de mais dados para análise sobre adequação às regulações de proteção de dados.

Entretanto, acredita-se que a coleta realizada nesse trabalho traga contribuições significativas para necessárias discussões sobre proteção de dados no judiciário. Proporcionam um debate construtivo e reflexão sobre deficiências das práticas identificadas nas coletas de dados pessoais nas realizações de audiências por videoconferência.

As perguntas formuladas foram direcionadas às duas instituições para fins de compreensão de como funcionam os sistemas judiciais no cotidiano de suas atividades quando da realização de audiências por videoconferência. Os questionamentos foram elaborados com base nas normas existentes e nos conceitos estudados nesse trabalho.

Os referidos questionários não foram realizados, portanto, com o intuito de generalizar o cotidiano judiciário, mas, sim, de trazer exemplos, semelhantes ou distintos, de como efetivamente os tribunais escolhidos de cada país estão se adequando às legislações de proteção de dados.

Os tribunais escolhidos foram o Tribunal de Justiça de Pernambuco e *Tribunale di Pisa*. Como a pesquisa não traz o objetivo de apresentar um padrão nacional de cada país, os tribunais acima indicados foram objeto do trabalho pela razão de serem tribunais de justiça comum onde ocorrem corriqueiras demandas da sociedade.

Assim, considerando as exigências legais sobre a matéria, o capítulo analisa tanto os relatórios disponíveis para acesso público, acessíveis em sítios eletrônicos oficiais, como as respostas dos questionários. Essa análise proporciona identificar se os dados tratados estão protegidos, conforme a legislação preceitua.

Após as análises documentais, o último subtópico do presente capítulo tem o intuito de trazer reflexões sobre as problemáticas oriundas das atividades desenvolvidas no espaço digital. O estudo observa as operações adequadas e as deficiências para que sejam feitas ponderações

e sugestões no que tange à adequação legislativa e o que se entende por ciberespaço na atualidade.

Por conseguinte, baseando-se nas doutrinas especializadas em proteção de dados, direito digital, ciberespaço e afins, serão tecidas considerações acerca do que está em conformidade com a previsão legislativa de cada país, considerando uma perspectiva global.

O trabalho traz o viés do tratamento de dados pelo judiciário. Entretanto, a problemática sobre proteção de dados tem vários braços e, em todos eles, se faz necessário o cuidado sobre como realizar as operações de modo protetivo.

Assim sendo, o último ponto busca analisar o contexto extraterritorial, as vulnerabilidades cibernéticas, bem como trazer contribuição para minimizar os possíveis danos quanto a atual forma de tratamento de dados. Dessa forma, permitirá a possibilidade de aperfeiçoamento da segurança buscando garantir o respeito ao direito à proteção de dados durante as atividades jurisdicionais.

Existência de acompanhamento no Brasil e Itália sobre o Poder Judiciário e a adequação às regulamentações sobre proteção de dados pessoais (relatório e ofício ao tribunal)

Considerando que não bastam prescrições normativas generalista ou específica que visem a proteger algum direito, se faz necessário o acompanhamento sobre o seu cumprimento em todos os campos sociais na busca da efetividade normativa. Dessa forma, a análise desse tópico será feita sobre documentos oficiais dos respectivos órgãos responsáveis por fiscalizar e regulamentar o judiciário de cada país disponíveis para acesso público nos sítios eletrônicos.

Além dos relatórios, é de grande valia o estudo sobre as respostas aos questionários que foram enviados ao Tribunal de Justiça do Estado de Pernambuco e ao *Tribunale di Pisa*. As perguntas enviadas para cada um dos tribunais foram iguais (questionário em anexo), guardadas as devidas traduções para o idioma italiano para que o Tribunal pudesse compreender o documento e poder prosseguir com as respostas.

Deve-se considerar ainda que o questionário foi elaborado com base nas exigências regulatórias, circulares, resoluções e demais normas pertinentes ao tema e aqui estudadas, relativos aos dois países. São perguntas voltadas para os momentos iniciais da coleta, bem como

para o tratamento dos referidos dados durante as audiências remotas e posterior armazenamento.

A pesquisa tem como objetivo compreender como se dão os procedimentos nas audiências. Identificar a existência de esclarecimentos para as pessoas envolvidas na audiência sobre a coleta de seus dados pessoais. Se há informação do porquê são coletados, como são tratados e armazenados e se há algum procedimento que o cidadão tenha direito de reivindicar junto ao poder judiciário.

Sendo assim, busca-se, portanto, compreender como ocorrem o controle e acompanhamento das atividades judiciais no que diz respeito ao tratamento de dados pessoais quando da realização de audiências remotas. A partir disso, como se dão o tratamento e armazenamento dos dados, além de identificar como são conduzidas as realizações das audiências remotas.

Sobre esse assunto, há a previsão legal da existência de relatórios periódicos sobre as atividades que abrangem tratamento de dados pessoais. São os chamados Relatórios de impacto à Proteção de dados. Esse documento informa quais medidas são tomadas a respeito dos dados coletados, bem como atenuar os riscos que estes possam estar sujeitos.

Os tribunais brasileiros devem produzir seus próprios relatórios, pois a legislação não exige o Poder Público da elaboração desses documentos. Outros documentos com teor de relatório também fazem parte do estudo e que foram identificados nas buscas dos sítios eletrônicos dos tribunais e dos órgãos de fiscalização.

Importante informar que aqui serão analisados os registros que estão disponíveis para acesso público, documentos que transmitam informações as mais próximas possíveis do que se espera acerca de resultados das atividades dos tribunais. Estes documentos que explicam a atividade desempenhada pelo órgão jurisdicional e o seu desempenho contêm informações de toda ordem, inclusive acerca do uso de tecnologia da informação, comunicação, segurança, entre outros temas.

Seguindo essa esteira, inicia-se o exame sobre a compreensão acerca da publicidade que está expressa em um trabalho disponibilizado pelo CNJ, quando aborda os desafios e as perspectivas quando do tratamento dos dados pessoais na consulta de jurisprudência:

Os serviços de divulgação de jurisprudência devem estar permanentemente atentos à necessidade de equilíbrio entre publicidade processual e privacidade dos cidadãos e,

diante dos novos elementos normativos introduzidos pela LGPD, não podem se furtar ao esforço de reavaliar o tratamento que conferem aos dados das pessoas naturais²⁰⁰.

O referido trabalho traz um conjunto de ações realizadas em 2021 pelo Comitê de Apoio para elaboração de estudos e pareceres técnicos sobre a sistematização do serviço de jurisprudência no Poder Judiciário do CNJ – Conselho Nacional de Justiça, desde pesquisas sobre jurisprudência até estudos de doutrinas e reuniões.

Abre-se aqui a oportunidade para falar sobre os referidos princípios e a correlação com pesquisas de jurisprudências. Isso porque tais pesquisas são possíveis após a existência de um processo e que incluem os resultados das audiências. Daí a importância da análise desse documento, pois demonstra a visão do CNJ a respeito do equilíbrio entre publicidade e privacidade.

Dessa forma, a consulta de processos faz parte da publicidade processual. Tem a ver com transparência. Convém falar sobre esse princípio, tendo em vista que haverá de ter um balanceamento entre ele e a privacidade. Isso porque, todos os processos disponibilizados possuem dados pessoais dos envolvidos, inclusive das audiências remotas.

Em um trecho o CNJ fala sobre a publicidade processual atualmente, sobre não poder ser irrestritamente utilizado tal princípio em razão dos avanços tecnológicos e diz as vulnerabilidades:

Ocorre, todavia, que, no atual estágio de desenvolvimento tecnológico, já não é mais possível afirmar candidamente a irrestrita publicidade de informações judiciais sem levar em consideração os riscos concretos que ela pode oferecer à privacidade dos cidadãos. Os processos judiciais são uma fonte inesgotável de dados pessoais (inclusive sensíveis) titularizados pelos mais variados atores processuais (partes, testemunhas, vítimas, magistrados(as), advogados(as), auxiliares da justiça etc.) e por terceiros²⁰¹.

O texto do referido artigo traz reflexões sobre a publicidade e a pseudonimização quanto aos dados pessoais, como nome, identificação, e-mail, entre outros. A publicização de tais informações das partes em nada alteram pesquisas jurisprudenciais quando o interesse é no

²⁰⁰ BRASIL. Conselho Nacional de Justiça. Tratamento de dados pessoais na consulta de jurisprudência: desafios e perspectivas. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2022/02/tratamento-dados-pessoais-consulta-jurisprudencia30-11-21.pdf>. Acesso em: 29 maio 2024.

²⁰¹ BRASIL. Conselho Nacional de Justiça. Tratamento de dados pessoais na consulta de jurisprudência: desafios e perspectivas. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2022/02/tratamento-dados-pessoais-consulta-jurisprudencia30-11-21.pdf>. Acesso em: 29 maio 2024.

conteúdo jurídico das decisões e a divulgação dos dados pessoais coloca a privacidade dos envolvidos no processo em situação de vulnerabilidade.

Considerando o acesso à informação no Brasil, governança e gestão dos órgãos judiciários, há um controle sobre essa temática realizado pelo CNJ feito anualmente chamado Índice de Governança, Gestão e Infraestrutura de TIC (Tecnologia da informação e comunicação) do Poder Judiciário (iGovTIC-JUD).

São analisados 93 órgãos que são classificados a partir das notas obtidas sobre o nível de maturidade. Os níveis podem ser “baixo”, “satisfatório”, “aprimorado” e “excelência”. Para essa análise são realizados questionários elaborados pelo órgão e posteriormente são disponibilizadas informações em relatórios ano a ano.

O relatório do ano de 2023²⁰² apresenta gráficos com média por tema. De 2021 a 2023, a evolução por temas ocorreu, em sua maioria, com o nível “aprimoramento”. Dentre os temas estão: Estruturas Organizacionais e Macroprocessos; Infraestrutura Tecnológica e Serviços de Nuvem; Riscos, Segurança da Informação e Proteção de Dados; Sistema da Informação; Transformação Digital.

Analisando especificamente o tema sobre Riscos, Segurança da Informação e Proteção de Dados, em 2021 o nível foi “satisfatório” com nota 62,33. Em 2022 nível foi “aprimorado” com nota 71,61. Já em 2023 o nível voltou a ser “satisfatório”, entretanto, com nota 67,63.

Essa análise inicial traz informações relevantes. Isso porque demonstram que o desenvolvimento em vários setores precisa ser aprimorado. O tema de Riscos, Segurança da Informação e Proteção de Dados está relacionado com as preocupações trazidas aqui sobre como vem ocorrendo o trabalho no cotidiano dos tribunais. Informações mais detalhadas não estão disponíveis nos referidos relatórios.

Nos outros temas também houve variação de nível e de notas, mas em nenhum ano, dentro do período estimado, e em nenhuma categoria houve nível “baixo”. Desse modo, o relatório traz evidências de que o trabalho dos tribunais na busca da excelência vem sendo desenvolvido de forma construtiva, entretanto sinaliza alguns déficits ensejando a necessidade de aprimoramento para garantir maior segurança de dados.

²⁰² BRASIL. Conselho Nacional de Justiça. Levantamento de Governança, Gestão e Infraestrutura de TIC do Poder Judiciário. iGovTIC-JUD 2023. Resultado Geral. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2023/10/relatorio-geral-do-igovtic-jud-2023-2023-09-27-v2.pdf>. Acesso em 29 maio 2024.

O Tribunal de Justiça de Pernambuco apresenta classificação 66 dentre os tribunais avaliados. O nível de maturidade é “aprimorado” e, de acordo com o formulário utilizado pelo iGovTIC-JUD 2023, o TJPE obteve o resultado 83,47, tudo isso em uma classificação geral.

As perguntas realizadas pelo CNJ nos órgãos do judiciário são elaboradas em consonância com as diretrizes da TIC, que são estabelecidas na Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD). Portanto, o relatório é elaborado a partir de dados oficiais de cada tribunal, em cada área considerando os eixos previamente estabelecidos.

O documento informa que estão entre os questionamentos: sobre quem realiza as funções gerenciais de TIC, sobre processo de planejamento e sobre o processo de gerenciamento de TIC (se é institucional), se elaborou, entregou, executou planos previstos na ENTIC-JUD, se possui Comitê de Governança de TIC e se é atuante, dentre outras.

A partir dessas perguntas que geraram os relatórios²⁰³²⁰⁴, pode-se afirmar que atendem em parte a LGPD. Quando se questiona sobre planos, gerenciamento, atuação do Comitê de Governança, se há convergência com as exigências de resolução do CNJ, atribui-se uma responsabilidade direcionada a cada tribunal.

Os requisitos do questionário estão previstos na Resolução nº 370/2021 do CNJ²⁰⁵. Nesse documento estão diversas orientações sobre Tecnologia da Informação e Comunicação; Gestão da informação e de Demandas Judiciais; Gestão e Organização Judiciária.

No art. 1º, parágrafo único da Resolução determina que o objetivo da Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário é:

Parágrafo único. O objetivo da Estratégia nacional de Tecnologia da Informação e Comunicação do Poder Judiciário é constituir o principal instrumento de promoção da governança ágil e da transformação digital do Poder Judiciário por meio de serviços e soluções digitais inovadoras que impulsionem a evolução tecnológica do Poder Judiciário.

²⁰³ BRASIL. Conselho Nacional de Justiça. iGovTIC-JUD – Resultado Geral. Disponível em: https://paineisanalytics.cnj.jus.br/single/?appid=36047c1e-acf8-4030-8474-78a20bae7c96&sheet=fb1b4d86-5d2f-4ac5-a4fd-345065ec8bd4&lang=pt-BR&theme=cnj_theme&opt=ctxmenu. Acesso em: 29 maio 2024.

²⁰⁴ BRASIL. Conselho Nacional de Justiça. Resultado do Questionário de TIC. Disponível em: <https://www.cnj.jus.br/tecnologia-da-informacao-e-comunicacao/comite-nacional-de-gestao-de-tecnologia-da-informacao-e-comunicacao-do-poder-judiciario/resultado-do-questionario-de-tic/>. Acesso em: 29 maio 2024.

²⁰⁵ BRASIL. Resolução nº. 370 de 28/01/2021. Tecnologia da Informação E Comunicação; Gestão da Informação e de Demandas Judiciais; Gestão e Organização Judiciária. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3706>. Acesso em: 29 maio 2024.

Determina também que todos os Órgãos do Poder Judiciário deverão constituir ou manter um Comitê de Governança de Tecnologia da Informação e Comunicação multidisciplinar. Tal Comitê tem diversas atribuições, dentre elas propor modelos e padrões referentes à Governança de Tecnologia da Informação e Comunicação por meio de campanha institucionais, dentre outras demandas.

Assim, a partir de tais relatórios, compreende-se que ocorre um acompanhamento do sistema judicial de forma nacionalizada, por meio do CNJ, analisando determinados tópicos. Dessa maneira, atribui a execução dos planos aos respectivos tribunais em suas demandas cotidianas, bem como a gestão das atividades e seu respectivo rastreio para que estejam em conformidade com a LGPD.

Entretanto, não foi encontrado um relatório específico, detalhado sobre a realização de audiências por videoconferência e o tratamento dos dados realizados nesse ato. Tampouco orientações acerca de como proceder sobre coleta, tratamento e armazenamento de dados. Entende-se que ainda que sejam relatórios com temas amplos, as audiências são atos que devem estar abrangidos pelas previsões normativas acerca de procedimentos sobre a referida coleta.

Ressalte-se aqui a importância de um acompanhamento mais próximo e detalhado das atividades cotidianas nos tribunais, relatando o modo de realização dos procedimentos para poder identificar se a prática está efetivamente em consonância com a previsão normativa. Ou seja, adequadas à Lei de Proteção de dados. Isso pode ser feito por meio de pesquisas e questionários, aplicados diretamente nas varas e gabinetes feitos pelo próprio tribunal, tal como se propôs aqui nesse trabalho ao dirigir o questionário à instituição judiciária.

Vale mencionar, que há uma Recomendação de nº. 73²⁰⁶ de 20 de agosto de 2020 em que o CNJ orientou o Poder Judiciário sobre as primeiras medidas adotadas para adequação a LGPD. Dentre as medidas está a elaboração de plano de ação com alguns tópicos que precisam necessariamente ser abordados, como comunicação, direito do titular, gestão de consentimento, retenção de dados e mais outros pontos.

A recomendação traz orientações pertinentes para garantir a proteção de dados quando são tratados pelo judiciário. Remete a criação de grupo de trabalho, política de segurança da informação.

²⁰⁶ BRASIL. Conselho Nacional de Justiça. Recomendação nº. 73 de 20 de agosto de 2020. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3432>. Acesso em: 07 jun 2024.

Os planos de ação deverão contemplar questões como organização e comunicação, direitos do titular, gestão de consentimento, retenção de dados e cópia de segurança, contratos e plano de respostas a incidentes de segurança com dados pessoais. Os usuários também deverão ser orientados sobre a nova lei, sobre requisitos para o tratamento de dados, as obrigações dos controladores e também sobre os direitos dos dados. Os registros relativos ao tratamento de dados pessoais dos usuários também devem ser públicos e informar sobre a finalidade do tratamento, base legal, descrição dos titulares, categorias de dados e de destinatários, transferência internacional, prazo de conservação, medidas de segurança adotadas e apolítica de segurança da informação²⁰⁷.

No que tange aos questionários elaborados pelo órgão para produção do relatório, as respostas precisam estar em consonância com o que está na recomendação. Trata-se de responsabilidade do Poder Judiciário frente ao trabalho desenvolvido e as coletas de dados pessoais em todos os âmbitos de sua atuação.

Observe-se que a preocupação com a utilização dos meios tecnológicos também é pensada no âmbito europeu. No caso da justiça eletrônica que se traduz em *e-justice* ou *Cyberjustice*, aplicado na União Europeia, segue uma orientação elaborada pela *Commissione europea per l'efficienza della giustizia del Consiglio d'Europa*.

Dentre as preocupações que consistem na referida orientação estão o acesso à justiça e a administração judicial. Pode-se aduzir que a respeito de administração judicial está compreendida a gestão dos atos e procedimentos, ação dos serventuários, bem como gestão de documentos e informações.

Nesse sentido, Professo Mensi faz as seguintes considerações:

La risoluzione n. 2054 (2015) dell'Assemblea parlamentare del Consiglio d'Europa, Commissione per l'uguaglianza e la non discriminazione, "Uguaglianza e non discriminazione nell'accesso alla giustizia", indica che il concetto ampio di accesso alla giustizia riguarda elementi quali informazioni su diritti e procedure, assistenza legale, rappresentanza legale, posizione giuridica o accesso generale ai tribunali. E' l'accesso alla giustizia alla base dell'uso di strumenti digitali volti ad aumentare la quantità di informazioni o la qualità dei servizi disponibili per gli utenti dei tribunali o ridurre le barriere (i costi) per l'accesso ai servizi. In tal senso, nel consentire vieppiù comunicazioni da remoto la tecnologia dell'informazione agevola l'accesso alla giustizia, naturalmente a condizione che i cittadini stessi siano connessi a internet²⁰⁸²⁰⁹.

²⁰⁷ BRASIL. Conselho Nacional de justiça. Recomendação orienta tribunais sobre proteção de dados. 27/08/2020. Agência de Notícias. Disponível em: <https://www.cnj.jus.br/recomendacao-orienta-tribunais-sobre-protecao-de-dados/>. Acesso em 07 jun 2024.

²⁰⁸ MENSI, Maurizio. Caratteristiche e criticità della comunicazione da remoto in tema di giustizia. 23 de setembro de 2020. Disponível em: <https://www.amministrazioneincammino.luiss.it/wp-content/uploads/2020/09/MENSI.pdf>. Acesso em: 09 jun 2024.

²⁰⁹ Tradução livre: Resolução nº. 2054 (2015) da Assembleia Parlamentar do Conselho da Europa, Comissão para a Igualdade e Não Discriminação, "Igualdade e não discriminação no acesso à justiça", indica que o conceito amplo de acesso à justiça abrange elementos como informação sobre direitos e procedimentos, apoio judiciário, representação legal, situação jurídica ou acesso geral aos tribunais. O acesso à justiça é a base da utilização de ferramentas digitais que visam aumentar a quantidade de

Dessa forma, compreende-se que o conceito de acesso à justiça é amplo. Nesse sentido, é esse o fundamento para o uso de ferramentas digitais e, como ele afirma, aumenta o acesso a informações e elimina barreiras para o acesso a serviço.

Entretanto, deve haver investimento em ferramentas, organização para oferecer melhor prestação à sociedade. Ou seja, garantir o direito de acesso à justiça de forma eficiente que não viole outros direitos. Dentre esses direitos está o da proteção de dados. O professor Mensi cita o parecer *su Giustizia e tecnologie dell'informazione*:

Nel suo parere n. (2011) 14 su “Giustizia e tecnologie dell'informazione” (IT) il Consiglio consultivo dei giudici europei (CCJE) sottolinea che l'introduzione dell'IT nei tribunali in Europa non dovrebbe tuttavia compromettere i volti umani e simbolici della giustizia. Se la giustizia viene percepita dagli utenti come puramente tecnica, senza la sua funzione reale e fondamentale, rischia di essere disumanizzata. La giustizia è e dovrebbe rimanere umana in quanto tratta principalmente delle persone e delle loro controversie²¹⁰²¹¹.

Esse parecer traz ponto relevante. Isto é, a justiça não deve deixar de ser humanizada. Isso significa dizer que não pode ser apenas técnica, deve permanecer humana, pois trata de pessoas e suas controvérsias. Nesse sentido, entende-se que a informação explicada de maneira acessível a população permite a compreensão sobre o sentido do que está sendo realizado. Trata-se de uma facilitação que orienta o público leigo em matéria jurídica. Essa pode ser uma etapa que faça parte de um roteiro de condutas para a realização das audiências remotas.

A Comissão Europeia elabora *Quadro de valutazione UE della Giustizia* que traz um panorama sobre a eficiência, qualidade e independência do sistema judiciário dos Estados Membros²¹². A comissão apoia reformas estrutural e projetos relacionado com a eficácia da justiça, como a digitalização.

informação ou a qualidade dos serviços disponíveis aos utilizadores dos tribunais ou reduzir as barreiras (custos) de acesso aos serviços. Neste sentido, ao permitir cada vez mais comunicações remotas, as tecnologias de informação facilitam o acesso à justiça, naturalmente desde que os próprios cidadãos estejam ligados à internet

²¹⁰ MENSÌ, Maurizio. Caratteristiche e criticità della comunicazione da remoto in tema di giustizia. 23 de setembro de 2020. Disponível em: <https://www.amministrazioneincammino.luiss.it/wp-content/uploads/2020/09/MENSI.pdf>. Acesso em: 09 jun 2024.

²¹¹ Tradução livre: Na opinião dele não. (2011) 14 sobre “Justiça e tecnologias de informação” (TI), o Conselho Consultivo dos Juizes Europeus (CCJE) sublinha que a introdução das TI nos tribunais da Europa não deve, no entanto, comprometer as faces humanas e simbólicas da justiça. Se a justiça for percebida pelos utilizadores como puramente técnica, sem a sua função real e fundamental, corre o risco de ser desumanizada. A justiça é e deve continuar a ser humana, uma vez que trata principalmente das pessoas e dos seus litígios.

²¹² Importante ressaltar que há convenção do Conselho Europeu sobre acesso a documentos oficiais. UNIÃO EUROPEIA. Convenzione del Consiglio d'Europa sulla Accesso ai documenti ufficiali

No referido documento, informa que a Comissão monitora a digitalização dos sistemas judiciais nacionais porque é uma forma de aumentar a eficiência e facilitar o acesso à justiça. Todavia, esse não é o único indicador de avaliação da justiça, outros como acessibilidade da justiça para cidadãos e para empresas, recursos financeiros e humanos adequados, implementação de ferramentas de avaliação e digitalização.

O documento aborda a análise sobre o uso de soluções digitais para casos são chamados de civis/comerciais, administrativos e criminais. Afirma que se faz necessário regulamentação frequente e o gráfico 41²¹³ informa as possibilidades estabelecidas em lei para a utilização da tecnologia digital nos tribunais, como o uso de videoconferência. O uso está relacionado com as atividades dos tribunais e procedimentos judiciais.

Sobre a possibilidade, na Itália, de as partes serem ouvidas à distância, utilizando meios tecnológicos, o gráfico pontua de 0 a 2, em um máximo de 12. Sobre ouvir testemunhas, no âmbito civil não houve sinalização de ocorrência, já no âmbito administrativo e criminal, atribuiu-se de 3 a 4 e de 4 a 5, respectivamente. Todos avaliados nos parâmetros de 0 a 12.

No mesmo gráfico, no quesito de procedimento poder ser feito inteiramente de forma oral, com uso das tecnologias, as médias estão atribuídas ao administrativo e criminal, com pontuações de 2 a 3 e de 3 a 4 respectivamente.

Em relação a Itália, o gráfico demonstra que sobre a interpretação da linguagem durante o uso da tecnologia, acerca dos processos civis e comerciais, a avaliação está entre 8 e 10, ainda há dados sobre casos administrativos ou criminais. Sobre especialistas que podem ser ouvidor à distância, varia entre 6 e 8.

Sobre poder conduzir parte oral à distância, varia entre 4 e 6. Evidências em formato digital, o gráfico apresenta o nível de 2 a 4. Sobre a possibilidade de as partes serem ouvidas

(STCE no. 205). Trata-se de instrumento jurídico internacional vinculante que reconhece o direito geral de acesso a documentos públicos. Disponível em: <https://www.coe.int/it/web/conventions/full-list?module=treaty-detail&treatynum=205>. Bem como, o Regulamento do Parlamento Europeu e do Conselho nº 1049/2001 relativo ao acesso a documentos públicos do Parlamento Europeu, do Conselho e da Comissão. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32001R1049>. Acesso em: 11 jun 2024.

²¹³ UNIÃO EUROPEIA. European Commission. The 2023 EU Justice Scoreboard. Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions COM(2023) 309. Disponível em: https://commission.europa.eu/document/download/db44e228-db4e-43f5-99ce-17ca3f2f2933_en?filename=Justice%20Scoreboard%202023_0.pdf&prefLang=it. Acesso em 10 jun 2024. p. 41.

ou vítimas serem ouvidas à distância, por meio da tecnologia de comunicação à distância, a pontuação foi de 0 a 2. Além disso, o documento informa:

Use of digital tools – Beyond digital-ready procedural rules, courts and prosecution services need to have appropriate tools and infrastructure in place for distance communication and secure remote access to the workplace (Figure 42). Adequate infrastructure and equipment is also needed for secure electronic communication between courts/prosecution services and legal professionals and institutions (Figures 43 and 44). ICT, including innovative technology, plays an important role in supporting the work of judicial authorities. It therefore contributes significantly to the quality of justice systems. The availability of various digital tools at the disposal of judges, prosecutors and judicial staff can streamline work processes, ensure fair workload allocation and lead to a significant time reduction²¹⁴²¹⁵.

Em outras palavras, o trecho acima explica que os tribunais e serviços, além de precisarem de regras processuais para o digital, também necessitam de ferramentas e uma infraestrutura para comunicação à distância. Tudo isso precisa ocorrer de forma segura. Deixa claro que tecnologias inovadoras contribui para a qualidade do sistema de justiça (tradução livre).

Sobre a publicidade, mais um trecho do documento relata a importância da publicação das decisões, princípio da publicidade, entretanto, ressalta a necessidade do equilíbrio em relação ao GDPR. Há uma predominância do interesse público em divulgar as informações, mas há países que exigem a pseudoanonimização dos dados:

The online publication of court decisions requires balancing a variety of interests, within the boundaries set by legal and policy frameworks. The General Data Protection Regulation (86) fully applies to the processing of personal data by courts. When assessing what data to make public, a fair balance has to be struck between the right to data protection and the obligation to publicise court decisions to ensure the transparency of the justice system. This is particularly true when there is a prevailing public interest that justifies the disclosure of those data. In many countries, the law or practice requires the anonymisation or pseudonymisation (87) of judicial decisions

²¹⁴ UNIÃO EUROPEIA. European Commission. The 2023 EU Justice Scoreboard. Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions COM(2023) 309. Disponível em: https://commission.europa.eu/document/download/db44e228-db4e-43f5-99ce-17ca3f2f2933_en?filename=Justice%20Scoreboard%202023_0.pdf&prefLang=it. Acesso em 10 jun 2024. p. 42.

²¹⁵ Tradução livre: Utilização de ferramentas digitais – Para além das regras processuais preparadas para o digital, os tribunais e os serviços do Ministério Público precisam de ter ferramentas e infraestruturas adequadas para comunicação à distância e acesso remoto seguro ao local de trabalho (Figura 42). São também necessárias infraestruturas e equipamentos adequados para a comunicação eletrônica segura entre os tribunais/serviços do Ministério Público e os profissionais e instituições jurídicas (Figuras 43 e 44). As TIC, incluindo as tecnologias inovadoras, desempenham um papel importante no apoio ao trabalho das autoridades judiciais. Contribui, portanto, significativamente para a qualidade dos sistemas judiciais. A disponibilização de diversas ferramentas digitais à disposição dos juizes, procuradores e funcionários judiciais pode agilizar os processos de trabalho, garantir uma repartição justa da carga de trabalho e conduzir a uma redução significativa do tempo.

before publication, either systematically or upon request. Data produced by the judiciary are also governed by EU legislation on open data and the reuse of public sector information (88). The availability of judicial decisions in a machine-readable format (89), as displayed in Figure 49, facilitates an algorithm-friendly justice system (90)²¹⁶²¹⁷.

De acordo com o referido documento, em uma valoração de 0 a 7²¹⁸²¹⁹, no ano de 2022, o uso de tecnologia de comunicação à distância, especialmente por videoconferência, em relação a Itália, o gráfico variou entre 3 e 4. A informação tanto está relacionada às atividades das cortes, quanto aos serviços intitulados de acusação (courts; prosecution service, fig. 42).

A partir das informações gráficas acima sinalizadas, o relatório dispõe de algumas análises:

Figure 42 reveals the use of digital technology by courts and prosecution services. It shows that, with two exceptions, Member States do not fully use the potential allowed by their procedural rules (cf. Figure 41). Member States' courts, prosecutors and court staff already have various digital tools at their disposal, such as case-management systems, videoconferencing systems and teleworking arrangements. However, further

²¹⁶ UNIÃO EUROPEIA. European Commission. The 2023 EU Justice Scoreboard. Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions COM(2023) 309. Disponível em: https://commission.europa.eu/document/download/db44e228-db4e-43f5-99ce-17ca3f2f2933_en?filename=Justice%20Scoreboard%202023_0.pdf&prefLang=it. Acesso em 11 jun 2024. p. 43

²¹⁷ Tradução livre: A publicação online de decisões judiciais exige o equilíbrio de uma variedade de interesses, dentro dos limites estabelecidos pelos quadros jurídicos e políticos. O Regulamento Geral sobre a Proteção de Dados (86) aplica-se integralmente ao tratamento de dados pessoais pelos tribunais. Ao avaliar quais os dados a tornar públicos, deve ser alcançado um equilíbrio justo entre o direito à proteção de dados e a obrigação de divulgar as decisões judiciais para garantir a transparência do sistema judicial. Isto é particularmente verdade quando existe um interesse público preponderante que justifica a divulgação desses dados. Em muitos países, a lei ou a prática exige a anonimização ou a pseudonimização (87) das decisões judiciais antes da publicação, de forma sistemática ou mediante pedido. Os dados produzidos pelo poder judicial também são regidos pela legislação da UE relativa aos dados abertos e à reutilização de informações do setor público (88). A disponibilidade de decisões judiciais num formato legível por máquina (89), conforme apresentado na Figura 49, facilita um sistema de justiça amigável aos algoritmos (90)

²¹⁸ UNIÃO EUROPEIA. European Commission. The 2023 EU Justice Scoreboard. Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions COM(2023) 309. Disponível em: https://commission.europa.eu/document/download/db44e228-db4e-43f5-99ce-17ca3f2f2933_en?filename=Justice%20Scoreboard%202023_0.pdf&prefLang=it. Acesso em 11 jun 2024. p. 42.

²¹⁹ Tradução livre da autora: Pontuação máxima possível: 7 pontos. Para cada critério, um ponto foi dado se os tribunais e os serviços de acusação, respectivamente, utilizam uma determinada tecnologia e 0,5 ponto foi concedido quando a tecnologia não é sempre utilizada por eles.

progress could still be achieved in electronic case allocation systems, with automatic distribution based on objective criteria²²⁰²²¹.

Na figura 42 está relacionado o uso da tecnologia nos procedimentos de acusação e a conclusão do relatório é de que os Estados membros não utilizam completamente o potencial permitido pelas regras processuais. Além disso, traz as seguintes considerações:

Courts in all Member States have some secure electronic tools for communication at their disposal. These tools are available for communication among courts and between courts and lawyers. However, 10 Member States still lack tools for digital communication with notaries, detention facilities or bailiffs/judicial officers (Figure 43). All Member States now provide for secure electronic communication within the prosecution services, as well as between prosecution services and courts, which represents an improvement compared to 2021 (Figure 44). Nevertheless, a third of Member States still lack tools for electronic communication between the prosecution services and defence lawyers²²².

O trecho informa que todos os tribunais têm ferramentas seguras à disposição para comunicação entre tribunais e entre tribunais e advogados, mas alguns Estados membros ainda carecem dessa comunicação para outros serviços, como oficial de justiça, etc. Apresentou melhoria em relação a 2021 no que diz respeito da comunicação eletrônica nas acusações e os tribunais, ficando com déficit em relação a comunicação entre os serviços de acusação e advogados de defesa.

In general, there is a tendency to introduce more arrangements, particularly for downloading the judgments free of charge (databases and other automated solutions),

²²⁰UNIÃO EUROPEIA. European Commission. The 2023 EU Justice Scoreboard. Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions COM(2023) 309. Disponível em: https://commission.europa.eu/document/download/db44e228-db4e-43f5-99ce-17ca3f2f2933_en?filename=Justice%20Scoreboard%202023_0.pdf&prefLang=it. Acesso em 11 jun 2024. p. 48.

²²¹ Tradução livre: A Figura 42 revela a utilização da tecnologia digital pelos tribunais e pelos serviços do Ministério Público. Mostra que, com duas exceções, os Estados-Membros não utilizam plenamente o potencial permitido pelas suas regras processuais (cf. figura 41). Os tribunais, os procuradores e os funcionários judiciais dos Estados-Membros já dispõem de diversas ferramentas digitais, tais como sistemas de gestão de processos, sistemas de videoconferência e modalidades de teletrabalho. No entanto, ainda poderão ser alcançados mais progressos nos sistemas eletrônicos de atribuição de processos, com distribuição automática baseada em critérios objetivos

²²² Tradução livre: Os tribunais de todos os Estados-Membros dispõem de algumas ferramentas eletrônicas seguras de comunicação. Estas ferramentas estão disponíveis para comunicação entre tribunais e entre tribunais e advogados. No entanto, 10 Estados-Membros ainda não dispõem de ferramentas para a comunicação digital com notários, centros de detenção ou oficiais de justiça/funcionários judiciais (figura 43). Todos os Estados-Membros proporcionam agora comunicações eletrônicas seguras dentro dos serviços do Ministério Público, bem como entre os serviços do Ministério Público e os tribunais, o que representa uma melhoria em comparação com 2021 (figura 44). No entanto, um terço dos Estados-Membros ainda não dispõe de ferramentas para a comunicação eletrônica entre os serviços do Ministério Público e os advogados de defesa

for modelling judgments to make them machine-readable, or for anonymising/pseudonymising judgments using algorithms²²³²²⁴²²⁵.

As informações relatadas sobre a Itália, trazem dados para aprimoramento das atividades prestadas pelo judiciário. Os gráficos demonstram pontuações de outros países, o que faz observar as diferenças de resultados em uma visão macro. De toda forma, o relatório informa que a partir dos resultados há uma tendência de organização para proporcionar acesso às sentenças, bem como automatizar ou anonimizar os dados.

Por fim, o relatório conclui que:

The 2023 EU Justice Scoreboard presents a diverse picture of the effectiveness of justice systems in the Member States. It shows that efforts to improve the efficiency, quality and independence of the justice systems are underway in many jurisdictions. However, challenges remain to ensure full trust of citizens in the legal systems of all Member States. The information in the EU Justice Scoreboard contributes to the monitoring carried out in the framework of the European Rule of Law Mechanism and feeds into the Commission's annual Rule of Law report²²⁶²²⁷.

Considerando que as referidas conclusões dizem respeito aos vários pontos abordados no relatório e, não somente sobre uso de tecnologia, o documento mostra uma diversificada variação do judiciário nos Estados membros. Demonstra que muitos estão em andamento para

²²³ Em geral, há uma tendência de introduzir mais arranjos, especialmente para baixar as sentenças gratuitamente (bancos de dados e outras soluções automatizadas), para modelar as sentenças para torná-las legíveis por máquina, ou para anonimizar/pseudonimizar as sentenças usando algoritmos. (tradução livre da autora).

²²⁴ Tradução livre: Em geral, há uma tendência para introduzir mais disposições, nomeadamente para descarregar os acórdãos gratuitamente (bases de dados e outras soluções automatizadas), para modelar os acórdãos para os tornar legíveis por máquinas, ou para anonimizar/pseudonimizar os acórdãos utilizando algoritmos

²²⁵ UNIÃO EUROPEIA. European Commission. The 2023 EU Justice Scoreboard. Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions COM(2023) 309. Disponível em: https://commission.europa.eu/document/download/db44e228-db4e-43f5-99ce-17ca3f2f2933_en?filename=Justice%20Scoreboard%202023_0.pdf&prefLang=it. Acesso em 11 jun 2024. p. 48.

²²⁶ UNIÃO EUROPEIA. European Commission. The 2023 EU Justice Scoreboard. Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions COM(2023) 309. Disponível em: https://commission.europa.eu/document/download/db44e228-db4e-43f5-99ce-17ca3f2f2933_en?filename=Justice%20Scoreboard%202023_0.pdf&prefLang=it. Acesso em 11 jun 2024. p. 63.

²²⁷ Tradução livre: O Painel de Avaliação da Justiça na UE de 2023 apresenta uma imagem diversificada da eficácia dos sistemas judiciais nos Estados-Membros. Mostra que estão em curso esforços para melhorar a eficiência, a qualidade e a independência dos sistemas judiciais em muitas jurisdições. No entanto, subsistem desafios para garantir a plena confiança dos cidadãos nos sistemas jurídicos de todos os Estados-Membros. As informações constantes do Painel de Avaliação da Justiça na UE contribuem para o acompanhamento realizado no âmbito do Mecanismo Europeu para o Estado de Direito e contribuem para o relatório anual da Comissão sobre o Estado de Direito

melhoria da prestação jurisdicional, e, portanto, as informações contribuem para o monitoramento no âmbito europeu fazendo parte dos relatórios da comissão.

Quanto aos sítios de internet dos tribunais, algumas considerações podem ser feitas. O objetivo da pesquisa é analisar as disposições voltadas para a proteção de dados em cada um dos tribunais selecionados para essa pesquisa.

Nesse sentido, o Tribunal de Justiça de Pernambuco dispõe, em seu portal da transparência²²⁸, um espaço que aborda a LGPD. O propósito disso é informar como o tribunal vem se adequando às exigências legais no que tange a proteção de dados. É composto de apresentação, requisitos, encarregado, formulário, política de privacidade e política de proteção de dados. Todos os tópicos visam elucidar o assunto e informar a sociedade sobre como funciona o tratamento de dados pessoais no tribunal.

Nesse diapasão, orienta como os titulares dos dados podem proceder a respeito de correções, informações e eliminações dos dados. Há um link de formulário para que o interessado possa se dirigir à ouvidoria de forma eletrônica para que possa exercer os seus direitos quanto aos dados.

O portal apresentou uma formatação, no dia em que foi feita a consulta ao sítio eletrônico, com parte da margem esquerda ocultada pela aba de possibilidade de acessos ao portal. Além disso, o link de formulário, ao clicar no momento da pesquisa, não se encontrava disponível.

Sobre essa disponibilidade de informações sobre a Lei Geral de Proteção de Dados no portal do tribunal, não se pode dizer que é acessível a todos. Isso porque, parte da população não tem conhecimento sobre o manuseio do site ou compreendem as informações que constam ali. Além disso, acredita-se que não seja hábito da população consultar o sítio eletrônico do tribunal para obter informações dessa seara. Dessa forma, a busca por tais informações no sítio do tribunal tende a ser feita por poucos usuários.

Acredita-se que a informação deve estar disposta de forma clara. O titular dos dados precisar saber onde encontrar as informações e compreender o que está disposto pelo responsável por tratar os dados. O que se almeja é que as informações sobre a coleta, tratamento e armazenamento de dados pessoais durante a realização das audiências remotas sejam

²²⁸ BRASIL. Tribunal de Justiça do Estado de Pernambuco. Portal da Transparência. Disponível em: <https://portal.tjpe.jus.br/web/transparencia/gestao/lei-geral-de-protecao-de-dados-lgpd/formulario>. Acesso em: 11 jun 2024.

dispostas de forma que o interessado compreenda o que lê. Nesse sentido, é importante que se inclua uma rotina dos serventuários para esclarecimentos sobre o assunto para o público em geral.

Observa-se, no portal, que há um plano de capacitação dos serventuários²²⁹ previsto para o ano de 2024. Foi elaborada uma lista de cursos a serem realizados para nivelamento das habilidades e conhecimentos frente a implantação de novas tecnologias. Dentre eles, está um curso sobre Gestão da Segurança da Informação.

Além disso, há um Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC²³⁰. Nesse documento há projetos e ações, dentre eles, compra de equipamentos para gravação de audiência. Há também o objetivo de desenvolvimento para atingir o nível de excelência no que diz respeito a fortalecer a estratégia nacional de TIC e a proteção de dados. Esse objetivo está pautado no indicador do nível de maturidade informado pelo IGovTIC.

Não fica demonstrado, a partir dos documentos até aqui analisados, como efetivamente devem ocorrer os procedimentos quando da realização de audiência por videoconferência. De acordo com os relatórios, os serventuários são capacitados para estarem habilitados acerca de várias temáticas, dentre elas a de proteção de dados, mas não há informação, até a presente data, de concretização de alguma etapa do planejamento previsto nos documentos e como tenha ocorrido.

Não foram encontrados documentos que comprovem a realização de atividades anteriores ao planejamento de 2024. Documentos que relatem resultados alcançados e os propósitos de cada um deles. Nada que esclareça sobre rotina do judiciário acerca de proteção de dados pessoais.

Dessa forma, idealizou-se, para maior precisão sobre as informações cotidianas do judiciário, a elaboração do formulário pela autora da pesquisa com o questionário e enviado para cada tribunal.

²²⁹ BRASIL. Tribunal de Justiça do Estado de Pernambuco. Plano de capacitação de TIC. Secretaria de tecnologia da informação e comunicação – SETIC. Disponível em: <https://portal.tje.jus.br/documents/d/transparencia/05-plano-de-capitacao-2024-setic-pdf-1->. Acesso em 11 jun 2024

²³⁰ BRASIL. Tribunal de Justiça do Estado de Pernambuco. Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC. Disponível em: <https://portal.tje.jus.br/documents/d/transparencia/02-pdtic-2024-2026-1->. Acesso em: 11 jun 2024.

Assim, observa-se uma estrutura do judiciário de Pernambuco com planejamentos e estratégias estabelecidos para a melhoria da prestação jurisdicional, sem aprofundamento sobre como se darão as abordagens nas audiências remotas em matéria de proteção de dados. Entretanto, pode-se aduzir que demonstra preocupação com a segurança da informação, qualificação do quadro funcional e transparência quanto ao que vem realizando.

No que diz respeito ao judiciário italiano, o portal do *Ministero della Giustizia*²³¹ apresenta explicações sobre o tratamento dos dados pessoais que consultam o sítio. Tem a sinalização da realização de um *Seminario su Data Protection e Civil Enforcement*, direcionado a *ufficiali giudiziari e funzionare UNEP*.

A partir do artigo de Filomena Storelli²³², quando aborda a realização de audiências por videoconferência durante o período pandêmico do COVID-19, ela relata como se procedia para que esse ato processual acontecesse. Relatou que havia o uso de plataforma como Skype for business e Teams. Informa também que na sala virtual eram realizados vários atos como intervenções verbais, registros em ata, anexação de documento, entretanto, não era permitida a gravação da audiência. Ao final da audiência, a ata era lida em voz alta ou por compartilhamento de tela.

O texto traz algumas considerações sobre áreas do direito e a utilização, previsão de audiência remota. Sobre o juiz de paz, não há previsão. Entretanto, na pandemia do COVID-19 houve o uso da forma telemática de forma emergencial. Na seara trabalhista, que tem natureza processual de urgência, além de outras características que poderiam ser afetadas pelo uso do processo telemático.

Tanto ao juiz de paz quanto ao processo trabalhista, tiveram uso de audiências remotas de forma emergencial, todavia, não houve uniformidade em toda a Itália sobre os procedimentos. E, na *Corte di Casazione*, que é a última instância, houve a possibilidade de processo telemático, mas o pedido quanto a utilização desse modo tem um prazo²³³.

²³¹ ITÁLIA. Ministero della Giustizia. Protezione dei dati personali. Disponível em: <https://www.giustizia.it/giustizia/page/it/privacy>. Acesso em: 14 jun 2024.

²³² STORELLI, Filomena Marianna. Processo Telematico e da Remoto: l'udienza è smart. 04/05/2020. In IusItinere Revista Giuridica. Disponível em: <https://www.iusinitinere.it/processo-telematico-e-da-remoto-ludienza-e-smart-27530>. Acesso em: 15 jun 2024.

²³³ STORELLI, Filomena Marianna. Processo Telematico e da Remoto: l'udienza è smart. 04/05/2020. In IusItinere Revista Giuridica. Disponível em: <https://www.iusinitinere.it/processo-telematico-e-da-remoto-ludienza-e-smart-27530>. Acesso em: 15 jun 2024.

Foi identificada uma proposta de protocolo²³⁴ para adaptar o sistema judicial às exigências de medidas de emergência durante o período pandêmico. Dentre os pontos tratados no documento, estão as críticas e desafios tanto quanto a uniformidade dos procedimentos, quanto a segurança e privacidade. Saliente-se que essa proposta foi elaborada no período emergencial pandêmico.

Nesse diapasão, durante a pesquisa que se buscou aprofundar foi constatada uma ferramenta elaborada pela Comissão Europeia para Eficiência da Justiça com orientações para a mudança para ciberjustiça²³⁵. Importante ressaltar que o documento é datado de 2019, período anterior à pandemia do coronavírus. Esse documento traz projetos para o judiciário, estratégias de TI para o judiciário e, com isso, trazer uma melhor forma de transformação digital.

Acrescente-se aqui a opinião de Mensi a respeito da necessidade de que os sistemas de softwares, utilizados para audiência, sejam utilizados por pessoas preparadas e que seja garantido o maior nível de segurança: *Importante altresì che il sistema sia gestito da personale specificamente preparato e che siano previsti i più elevati standard di sicurezza a protezione di reti, sistemi e dati*²³⁶²³⁷. Dessa forma, importante salientar que não foi encontrado no portal do *Tribunale di Pisa* orientações sobre o tratamento de dados pessoais pelo poder judiciário, bem como a quem o titular dos dados deve se dirigir em caso de qualquer dúvida ou necessidade de orientação.

Portanto, sobre o material que foi possível ser analisado não contém informações suficientes que façam concluir que os tribunais estão adequados às suas respectivas regulamentações sobre proteção de dados. Essas observações são referentes aos tribunais aqui selecionados para estudo.

²³⁴ ITÁLIA. Consiglio Nazionale Forense. Presso il Ministero della Giustizia. Proposta di Protocollo per udienze civili tramite collegamento da remoto – art. 83 lett. f, D.L. 18/2020. Disponível em: <https://www.consiglionazionaleforense.it/documents/20182/677549/Protocollo+per+udienze+civili.pdf/56847321-9706-4347-a14b-2c9bcee3a089>. Acesso em: 15 jun 2024.

²³⁵ UNIÃO EUROPEIA. EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE (CEPEJ). Toolkit for supporting the implementation of the Guidelines on how to drive change towards Cyberjustice.

²³⁶ MENSI, Maurizio. Caratteristiche e criticità della comunicazione da remoto in tema di giustizia. 23 de setembro de 2020. Disponível em: <https://www.amministrazioneincammino.luiss.it/wp-content/uploads/2020/09/MENSI.pdf>. Acesso em: 15 jun 2024

²³⁷ Tradução livre: É também importante que o sistema seja gerido por pessoal especificamente treinado e que sejam previstos os mais elevados padrões de segurança para proteger redes, sistemas e dados.

Dessa forma, que se pode concluir é que de acordo com os planejamentos, leva a crer estarem se encaminhando para uma adequação. Ainda nesse sentido, apresentam dados genéricos sobre produtividades e resultados de atividade jurisdicional em relatórios disponibilizados para consultas públicas.

Acerca dos questionários disponibilizados para o *Tribunale di Pisa* e Tribunal de Justiça de Pernambuco, a análise é feita a partir de perguntas iguais, de modo a compreender como cada instituição vem dando sequência às atividades.

Sobre o *Tribunale di Pisa*, as respostas foram encaminhadas pelo setor responsável, através de *funzionario Ufficio per il Processo*. As respostas foram as seguintes:

SEZIONE CIVILE

- 1. I dipendenti (responsabili, incaricati e addetti al trattamento dei dati personali) del Tribunale di Pisa ricevono formazione sul Regolamento Europeo sulla protezione dei dati e su altre normative e risoluzioni pertinenti al tema?***

No.

Tradução:

- 1. Os funcionários (diretores, responsáveis e responsáveis pelo tratamento de dados pessoais) do Tribunal de Pisa recebem formação sobre o Regulamento Europeu de Proteção de Dados e sobre outros regulamentos e resoluções relevantes para o tema?**

Resposta:

Não.

Comentario:

Observa-se que o Tribunal de Pisa nao promoveu formação acerca das regulamentações e normativas sobre proteção de dados. Desse modo, não se tem uma uniformidade sobre o conhecimento da legislação entre os servidores do tribunal, o que se compreende a partir da resposta acima. Dessa forma, torna-se desafio a efetiva proteção de dados em âmbito do tribunal.

Tal resposta demonstra não só na realização de audiências por videoconferência, mas em todas as atividades desempenhadas pelo tribunal, que são realizadas por servidores que não

receberam treinamento sobre como proceder para coletar, tratar e armazenar dados pessoais das partes e usuários em processo.

O fato de não haver treinamento dificulta a abordagem dos servidores com os titulares dos dados do processo e as demais pessoas que venham a participar de qualquer audiência por videoconferência. Isso quer dizer que o desconhecimento sobre a lei pode afetar a forma de prestação de atendimento durante a realização do ato.

Via de regra, não se há como saber quais servidores detém o conhecimento sobre a matéria e, portanto, não é possível deduzir que o tribunal tem a prestação jurisdicional pautada na legislação de proteção de dados e demais normas correlatas.

2. Esiste una politica di protezione dei dati stabilita nell'ambito del Tribunale di Pisa?

La politica di protezione dei dati per il Tribunale di Pisa si allinea a quella indicata dalla normativa europea (regolamento 679/2016 e direttiva 680/2016) così come recepita a livello nazionale nel d.lgs 18 maggio 2018, n.51 (recante disposizioni di attuazione della direttiva UE 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016) e nel d.lgs 10 agosto 2018, n. 101 (recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento UE 679/2016 del Parlamento Europeo e del Consiglio del 27 aprile 2016). I decreti legislativi menzionati sono andati ad integrare ed aggiornare il cd. "Codice della Privacy", d.lgs 30 giugno 2003 n.196.

Tradução:

2. Existe uma política de proteção de dados estabelecida no Tribunal de Pisa?

Resposta:

A política de proteção de dados do Tribunal de Pisa está alinhada com a indicada pela legislação europeia (regulamento 679/2016 e diretiva 680/2016), conforme implementada a nível nacional no Decreto Legislativo de 18 de maio de 2018, n.51 (contendo disposições que implementam a Diretiva da UE 2016 /680 do Parlamento Europeu e do Conselho de 27 de abril de 2016) e no Decreto Legislativo de 10 de agosto de 2018, n. 101 (contendo disposições para a adaptação da legislação nacional às disposições do regulamento UE 679/2016 do Parlamento Europeu e do Conselho de 27 de abril de 2016). Os decretos legislativos mencionados integraram e atualizaram os chamados. "Código de Privacidade", Decreto Legislativo de 30 de junho de 2003 n.196.

Comentário:

A pergunta acerca da existência de política de privacidade busca averiguar se a instituição buscou adequar-se a legislação. Isto é, em havendo política de privacidade, significa que o tribunal deve estar respeitando as diretrizes legais.

Entretanto, para que haja o efetivo cumprimento normativo, se faz necessária a aplicação em todos os âmbitos. A publicidade da política é um requisito essencial para que seja efetiva na instituição. Todavia, torna-se um desafio compatibilizar o cumprimento da legislação de proteção de dados sem que os servidores tenham algum treinamento voltado para mínimo de conhecimento do teor da lei.

- 3. Durante lo svolgimento delle udienze tramite videoconferenza nel Tribunale di Pisa, avviene la raccolta di dati personali dei partecipanti, siano essi parti, dipendenti, giudici, membri del Ministero Pubblico, testimoni o qualsiasi altra persona partecipante?**

Sì, al momento dell'inizio dell'udienza, il giudice dà lettura dell'intestazione del verbale che contiene i nomi delle parti, oltre che dei difensori ed eventuali intervenuti o ausiliari del magistrato collegati. All'atto della fissazione dell'udienza da remoto, vengono altresì richiesti i contatti telefonici e di posta elettronica delle parti chiamate a partecipare all'udienza e/o dei propri procuratori costituiti.

Inoltre, secondo il provvedimento del 7 dicembre 2023 – “Individuazione dei collegamenti audiovisivi a distanza per lo svolgimento dell'udienza e delle modalità attraverso le quali è garantita la pubblicità dell'udienza in cui si discute la causa, ai sensi dell'articolo 127-bis del codice di procedura civile e dell'articolo 196-duodecies, quinto comma, delle disposizioni di attuazione del codice di procedura civile” emanato dal Ministero della Giustizia, i sistemi di Microsoft Teams provvedono a conservare dati quali orario di inizio e fine sessione, identificativo utente, durata, sistema operativo del dispositivo utilizzato, indirizzo IP, nome dispositivo e CPU.

Tradução:

- 3. Durante as audiências via videoconferência no Tribunal de Pisa, ocorre a coleta de dados pessoais dos participantes, sejam eles partes, funcionários, juízes, membros do Ministério Público, testemunhas ou qualquer outra pessoa participante?**

Resposta:

Sim, no início da audiência o juiz lê o cabeçalho do relatório que contém os nomes das partes, bem como dos defensores e eventuais participantes ou auxiliares do magistrado vinculados. No agendamento da audiência remota, também são solicitados os contatos telefônicos e de e-mail das partes convocadas para participar da audiência e/ou dos seus procuradores designados.

Além disso, de acordo com a disposição de 7 de dezembro de 2023 - "Identificação das ligações audiovisuais remotas para a realização da audiência e dos métodos através dos quais é garantida a publicidade da audiência em que o caso é discutido, nos termos do artigo 127-bis do código de processo civil e artigo 196.º-duodécimos, quinto parágrafo, das disposições de execução do código de processo civil" emanadas do Ministério da Justiça, os sistemas Microsoft Teams encarregam-se de armazenar dados como horários de início e fim da sessão, usuário identificador, duração, sistema operacional do dispositivo utilizado, endereço IP, nome do dispositivo e CPU.

Comentário:

Pelo fundamento da pergunta 3, o *Tribunale di Pisa* coleta dados pessoais dos envolvidos em audiência por videoconferência. Além disso, mantém armazenadas as mídias no Microsoft Teams.

Conforme a resposta ao questionário, pode-se aduzir que além da coleta de dados, há o tratamento e armazenamento. Todavia, considerando a resposta 1 do questionário, a qual informa que não há treinamento, apesar de a resposta 2 trazer a afirmação de que há política de proteção de dados, o sistema judiciário necessita proporcionar um preparo aos servidores para que a coleta, tratamento e armazenamento dos dados estejam devidamente protegidos e de acordo com o Regulamento Europeu.

4. **Nel caso di suddetta raccolta di dati, come viene effettuata? Verbalmente, tramite immagini di documenti, scritti in chat o altri mezzi? Le persone sono informate dello scopo della raccolta, della sicurezza e di altre istruzioni pertinenti all'atto compiuto?**

La raccolta avviene mediante comunicazione orale delle parti presenti alla videoconferenza e le informazioni vengono annotate sul verbale redatto dal funzionario o Cancelliere, che viene poi trasmesso ai difensori, agli eventuali intervenuti e agli ausiliari.

Tradução:

4. No caso da referida coleta de dados, como é realizada? Verbalmente, através de imagens de documentos, escritos em chat ou outros meios? As pessoas são informadas sobre a finalidade da coleta, segurança e demais instruções pertinentes ao ato praticado?

Resposta:

A coleta ocorre por meio de comunicação oral das partes presentes na videoconferência e as informações são anotadas no relatório elaborado pelo dirigente ou Chanceler, que é então transmitido aos defensores, eventuais participantes e auxiliares.

Comentário:

A pergunta nº. 4 do formulário visa a saber como se dá a comunicação entre os serventuários da justiça e o jurisdicionado acerca da coleta, tratamento e armazenamento de dados durante a realização da audiência por videoconferência.

A partir da resposta dada pelo *Tribunale di Pisa*, observa-se que os titulares dos dados pessoais coletados não são informados sobre como será o procedimento acerca do tratamento e armazenamento dessas informações pessoais. Dessa forma, não se identifica que haja o atendimento aos preceitos do art. 39 do GDPR²³⁸, o qual preza pelo tratamento de dados pessoais transparente, inclusive determinando que a finalidade específica deverá ser explícita e legítima.

As informações coletadas são registradas em relatório e comunicadas aos defensores, entretanto, não se pode aduzir que o teor da informação contenha o esclarecimento sobre a finalidade da coleta, bem como serão utilizados os dados e armazenados.

Vale salientar também, que o artigo 58 do GDPR exige que qualquer informação destinada ao público ou titular dos dados seja concisa, de fácil acesso e compreensão. Além disso, precisa ter uma linguagem clara e simples. Desse modo, pode se aduzir que o *tribunale di Pisa* não atende ao preceito do regulamento europeu, pois falta clareza ao informar aos titulares de dados sobre o procedimento adotado pelo órgão quando da coleta dos dados pessoais do jurisdicionado.

²³⁸ REGULAMENTO EUROPEU (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679> Acesso em 3 nov 2024.

- 5. Come avviene l'archiviazione delle registrazioni delle udienze tramite videoconferenza nell'ambito del Tribunale di Pisa? Il/la responsabile segue qualche criterio specifico?**

Le udienze da remoto svolte mediante piattaforma Teams non vengono registrate, mentre le audizioni dei minori che si svolgono tramite un sistema di videofonoregistrazione, vengono conservate sulla memoria esterna del sistema stesso (consistente in una scheda SD e un disco rigido). La stessa viene periodicamente svuotata e il suo contenuto copiato su un altro hard disk conservato presso la Segreteria del Tribunale. L'archiviazione avviene per data di udienza e viene svolta dal tecnico informatico e dall'Ufficio Digitalizzazione.

Tradução:

- 5. Como são realizadas as gravações das audiências por videoconferência no Tribunal de Pisa? O gestor segue algum critério específico?**

Resposta:

As audiências remotas realizadas através da plataforma Teams não são gravadas, enquanto as audiências de menores que ocorrem através de um sistema de videogravação são armazenadas na memória externa do próprio sistema (composta por um cartão SD e um disco rígido). O mesmo é periodicamente esvaziado e seu conteúdo copiado para outro disco rígido mantido na Secretaria do Tribunal. O arquivamento ocorre por data da audiência e é realizado pelo técnico de informática e pelo Gabinete de Digitalização.

Comentário:

Sobre o armazenamento dos atos de audiência por videoconferência, importante tecer alguns comentários sobre o procedimento realizado pelo *Tribunale di Pisa*. Informa que apenas são arquivados os processos que envolverem menores de idade, mantendo as mídias em memória externa.

Nesse sentido, o conteúdo a respeito de menores de idade é sensível, pois versa sobre pessoas que não têm o discernimento necessário para analisar os riscos da vulnerabilidade dos dados. De acordo com o art. 38 do GDPR, os dados de crianças merecem proteção especial por estas estarem menos cientes dos riscos, consequências e garantias, além dos direitos relacionados ao tratamento dos dados pessoais.

- 6. Per quanto tempo le registrazioni rimangono archiviate nei file del Tribunale?**

Attualmente, in assenza di una normativa specifica in merito, le registrazioni vengono conservate permanentemente negli hard disk del Tribunale.

Tradução:

6. Por quanto tempo as gravações permanecem armazenadas nos arquivos do Tribunal?

Resposta:

Atualmente, na ausência de legislação específica sobre o assunto, as gravações ficam armazenadas permanentemente nos discos rígidos do Tribunal.

Comentário:

A respeito do tratamento e armazenamento dos dados no ambiente judicial, importante citar o art. 20 do GDPR, o qual informa que o referido regulamento é aplicado nas atividades dos tribunais, devendo ser assegurado o seu cumprimento.

Entretanto, o fato de não haver uma regulamentação específica sobre como e onde armazenar os dados, permite a designação livre para tal o que torna a prática frágil do ponto de vista da segurança dos dados. É importante que se tenha um local específico para o armazenamento dos dados, além de um procedimento padrão para a realização do depósito dos dados coletados.

O local deve ser seguro, e somente pessoas autorizadas tenham acesso. Importante que seja protegido com senha e camadas de segurança para minimize os riscos de vazamento, acessos não autorizados ou perdas dos dados que possam ocasionar danos aos seus titulares.

7. Quali sono i criteri di sicurezza e protezione delle registrazioni? È richiesta l'adozione di protocolli specifici, come l'uso di password, formazione specifica?

Le registrazioni sono accessibili soltanto agli addetti ai lavori, ovvero funzionari, giudici e cancellieri, i quali hanno ricevuto una formazione di base per l'utilizzo delle apparecchiature. Periodicamente le stesse vengono rimosse dal supporto di archiviazione informatica locale, per essere conservate sull'hard disk della Segreteria, da questo momento in poi sono accessibili soltanto su richiesta. Il materiale non è protetto da password. Attualmente, il sistema SICID non consente il caricamento dei file delle registrazioni,

tuttavia i difensori e le parti che ne fanno richiesta possono prendere visione dei video delle udienze su appuntamento.

Tradução:

7. Quais são os critérios de segurança e proteção das gravações? É necessária a adoção de protocolos específicos, como uso de senhas, treinamentos específicos?

Resposta:

As gravações são acessíveis apenas a profissionais, ou seja, funcionários, juízes e escrivães, que tenham recebido formação básica na utilização do equipamento. São periodicamente retirados do meio de armazenamento informático local para serem armazenados no disco rígido da Secretaria, a partir deste momento só podem ser acessados mediante solicitação; O material não é protegido por senha. Atualmente, o sistema SICID não permite o upload de arquivos de gravação, porém os defensores e partes que solicitarem podem visualizar os vídeos das audiências mediante agendamento.

Comentário:

A partir da resposta do item 7, não se pode compreender como se dá efetivamente o acesso aos dados pessoais coletados. Isso porque a resposta informa que apenas funcionários, juízes ou escrivães que receberam formação básica poderão acessar os dados. Não se sabe qual formação se refere, tendo em vista que a pergunta 1 que abordou sobre a formação dos servidores sobre a matéria de proteção de dados, e esta foi respondida como não tendo sido feita.

Outro ponto a ser debatido é a ausência de senha. Não é possível deduzir que a segurança dos dados está mantida. O fato de estarem armazenados em disco rígido da secretaria e não haver senhas para acesso, pode ser uma vulnerabilidade para acesso indevido a eles. É necessário que se tenha medidas que fortaleçam a segurança do local em que estão armazenados os dados.

8. La realizzazione delle udienze è effettuata da qualsiasi dipendente del settore/sezione?

Partecipano all'udienza per la verbalizzazione funzionari e tirocinanti, i quali si occupano di effettuare tutti gli adempimenti necessari all'avvio e all'archiviazione della registrazione.

Tradução:

8. A realização de audiências é realizada por algum funcionário do setor/seção?**Resposta:**

Participam na audiência de lavratura da ata os funcionários e estagiários, cabendo-lhes cumprir todas as formalidades necessárias ao início e arquivo da lavratura.

Comentário:

A resposta não informa se há uma pessoa específica ou se qualquer servidor pode conduzir o ato da audiência por videoconferência. Considerando que não há um servidor específico para conduzir a audiência, o controle de acesso não é restrito. Nesse sentido, os dados apresentam-se menos protegidos, ante a inexistência de tantos fatores considerados fases de segurança para o armazenamento dos dados pessoais.

9. Qualsiasi dipendente del settore/sezione ha accesso all'archiviazione delle registrazioni?

Hanno accesso alle registrazioni soltanto i funzionari dei giudici e i magistrati stessi, oltre che il personale della Segreteria.

Tradução:**9. Algum funcionário do setor/seção tem acesso ao armazenamento de registros?****Resposta:**

Apenas os funcionários dos juízes e os próprios magistrados, bem como os funcionários da Secretaria, têm acesso às gravações.

Comentário:

O acesso a todos os serventuários torna vulnerável o armazenamento dos dados pessoais dos participantes das audiências por videoconferência. Não houve um treinamento específico sobre o regulamento de proteção de dados, não há armazenamento específico, ou seja, local criado para armazenar os dados das audiências, tampouco há senha de segurança que possa tornar difícil o acesso às informações.

Ao se tratar de proteção de dados, se faz necessário que a segurança ocorra tanto no ambiente físico, quanto no ambiente digital. Apenas os servidores que lidam com esses dados em razão das suas atribuições, que deverão ter acesso a eles. Os demais não necessitam ter

contato com as informações e caso haja algum propósito para esse acesso, deveriam procurar o setor responsável por tutelar os dados.

SEZIONE PENALE

- 1. I dipendenti (responsabili, incaricati e addetti al trattamento dei dati personali) del Tribunale di Pisa ricevono formazione sul Regolamento Europeo sulla protezione dei dati e su altre normative e risoluzioni pertinenti al tema?**

NO

Tradução:

1.Os funcionários (diretores, responsáveis e responsáveis pelo tratamento de dados pessoais) do Tribunal de Pisa recebem formação sobre o Regulamento Europeu de Proteção de Dados e sobre outros regulamentos e resoluções relevantes para o tema?

NÃO.

- 2. Esiste una politica di protezione dei dati stabilita nell'ambito del Tribunale di Pisa?**

Vedi risposta per sezione civile.

2.Existe uma política de proteção de dados estabelecida no Tribunal de Pisa?

Resposta:

Vea a resposta para a seção civil

Considerando que essas duas primeiras perguntas da *Sezione Penale* apresentaram as mesmas respostas da *Sezione Civile*, os comentários a serem tecidos são os mesmos já realizados acima.

- 3. Durante lo svolgimento delle udienze tramite videoconferenza nel Tribunale di Pisa, avviene la raccolta di dati personali dei partecipanti, siano essi parti, dipendenti, giudici, membri del Ministero Pubblico, testimoni o qualsiasi altra persona partecipante?**

Nel processo penale la totalità delle udienze si svolge nell'Aula del Tribunale alla presenza delle parti. Può essere disposta la videoconferenza qualora l'imputato, ristretto in un istituto penitenziario, faccia richiesta di partecipare all'udienza da remoto. Lo stesso, qualora un

testimone chieda di essere escusso a distanza. In ogni caso, all'inizio di ogni udienza – sia in videoconferenza che non – il Giudice verifica la regolare costituzione delle parti dando atto delle generalità di ciascuna di esse.

Tradução:

3. Durante as audiências via videoconferência no Tribunal de Pisa, ocorre a coleta de dados pessoais dos participantes, sejam eles partes, funcionários, juízes, membros do Ministério Público, testemunhas ou qualquer outra pessoa participante?

Resposta:

Nos julgamentos criminais, todas as audiências decorrem na Sala do Tribunal, na presença das partes. Poderá ser providenciada videoconferência caso o acusado, confinado em instituição penitenciária, solicite participação remota na audiência. O mesmo se aplica se uma testemunha solicitar ser interrogada remotamente. Em qualquer caso, no início de cada audiência – seja por videoconferência ou não – o Juiz verifica a regular constituição das partes anotando os dados pessoais de cada uma delas.

Comentário:

Conforme mencionado, o juiz colhe os dados pessoais das partes. Quando realizada a videoconferência, o ato também é praticado. Portanto, as audiências remotas são realizadas com a coleta dos dados pessoais das partes envolvidas.

Permanece a preocupação acerca da coleta, tratamento e armazenamento. O modo da operação é similar ao da *Sezione Civile*. Dessa forma, mantém-se o raciocínio de que as medidas de segurança devem ser mais robustas para que os dados estejam protegidos minimizando os riscos de perda e violação.

4. Nel caso di suddetta raccolta di dati, come viene effettuata? Verbalmente, tramite immagini di documenti, scritti in chat o altri mezzi? Le persone sono informate dello scopo della raccolta, della sicurezza e di altre istruzioni pertinenti all'atto compiuto?

Nel verbale di udienza vengono riportate le generalità dell'imputato, della parte offesa, dei testimoni e dei consulenti, mentre per i giudici e i difensori viene rilevato esclusivamente il nome e il cognome. La riforma Cartabia ha, inoltre, introdotto la riproduzione audiovisiva dell'esame dei testimoni, dei periti, dei consulenti tecnici e delle parti private nonché degli atti di ricognizione e confronto.

Per dare attuazione a quanto previsto dall'art. 510 co. 2 bis c.p.p., le videoregistrazioni vengono effettuate sulla piattaforma Teams all'interno del dedicato canale distrettuale "FIRENZE_VDR", ove ciascun'udienza è identificata con il c.d. "codice identificativo videoconferenza" che viene generato dall'applicativo in uso alla sezione penale (S.I.C.P.).

Nel verbale di udienza viene dato atto che si procede alla videoregistrazione dell'assunzione dei mezzi di prova.

Tradução:

4. No caso da referida coleta de dados, como é realizada? Verbalmente, através de imagens de documentos, escritos em chat ou outros meios? As pessoas são informadas sobre a finalidade da coleta, segurança e demais instruções pertinentes ao ato praticado?

Resposta:

A ata da audiência contém os dados pessoais do arguido, do ofendido, das testemunhas e dos consultores, enquanto para os juízes e defensores apenas são registrados o nome e apelido. A reforma de Cartabia também introduziu a reprodução audiovisual do interrogatório de testemunhas, peritos, consultores técnicos e particulares, bem como dos documentos de reconhecimento e comparação.

Para implementar o disposto no art. 510 co. 2 bis c.p.p., as gravações de vídeo são feitas na plataforma Teams dentro do canal distrital dedicado "FIRENZE_VDR", onde cada audiência é identificada com o chamado "código de identificação de videoconferência" que é gerado pela aplicação utilizada pela secção criminal (S.I.C.P.).

A ata da audiência reconhece que a coleta de provas será gravada em vídeo.

Comentário:

O método de realização do ato se assemelha ao da *Sezione Civile*. Entretanto, na *Sezione Penale* há o código de identificação. Acredita-se que se trate de organização documental. Importante frisar que a informação de gravação de vídeo é relatada na ata de audiência, o que subentende que os titulares sejam informados no ato.

Todavia, não informa medidas de segurança a respeito do procedimento de armazenamento. Portanto, pode-se supor que apenas a criação do código de identificação é que é gerado, não havendo mais medidas aplicadas.

- 5. Come avviene l'archiviazione delle registrazioni delle udienze tramite videoconferenza nell'ambito del Tribunale di Pisa? Il/la responsabile segue qualche criterio specifico?**

Terminata l'assunzione della prova testimoniale, la registrazione viene interrotta e la stessa viene automaticamente archiviata sui sistemi in cloud e successivamente resa disponibile, su un'apposita piattaforma, al personale del Ministero della Giustizia (magistrati e cancellieri/funzionari), tramite accesso con la rete giustizia, per la successiva fruizione.

Tradução:

- 5. Como são realizadas as gravações das audiências por videoconferência no Tribunal de Pisa? O gestor segue algum critério específico?**

Resposta:

Concluída a obtenção da prova testemunhal, a gravação é interrompida e a mesma é automaticamente arquivada nos sistemas cloud e posteriormente disponibilizada, em plataforma específica, aos funcionários do Ministério da Justiça (magistrados e escrivães/funcionários), via acesso à rede de justiça, para posterior utilização.

O armazenamento feito em nuvem, sem nenhum critério específico para garantir a segurança, vulnerabiliza os dados pessoais. Mais uma vez indentifica-se que os procedimentos adotados pelo tribunal não precedem de medidas específicas para proteção de dados pessoais.

O servidor procede com a coleta do depoimento, efetua a gravação e armazenamento em nuvem, entretanto, nada mais foi demonstrado que pudesse levar a crer que haja medidas seguras para os dados pessoais coletados nas audiências remotas.

- 6. Per quanto tempo le registrazioni rimangono archiviate nei file del Tribunale?**

Non è stato specificato dal Ministero della Giustizia, ma è presumibile che le stesse siano conservate quanto meno fino all'irrevocabilità della sentenza.

Tradução:

- 6. Por quanto tempo as gravações permanecem armazenadas nos arquivos do Tribunal?**

Resposta:

Não foi especificado pelo Ministério da Justiça, mas é presumível que o mesmo seja mantido pelo menos até que a sentença seja irrevogável.

A estimativa afirmada na resposta sobre o tempo de armazenamento da gravação nos arquivos do tribunal, permite supor que a vulnerabilidade acontece durante o tempo em que o tribunal estiver responsável pela tutela das informações. Ao tempo em que forem eliminados os dados, as chances de os dados estarem vulneráveis é mínima.

Todavia, dentre as medidas necessárias, é importante estabelecer um padrão sobre como se dará o descarte dos dados pessoais que forem coletados nas audiências remotas.

7. Quali sono i criteri di sicurezza e protezione delle registrazioni? È richiesta l'adozione di protocolli specifici, come l'uso di password, formazione specifica?

Tutte le registrazioni possono essere attivate e riprodotte previa autenticazione del personale (magistrati e cancellieri/funzionari). Inoltre, le stesse sono fruibili solo con collegamento alla rete giustizia, salvo richiesta copia digitale da parte delle parti processuali.

Tradução:

7. Quais são os critérios de segurança e proteção das gravações? É necessária a adoção de protocolos específicos, como uso de senhas, treinamentos específicos?

Resposta:

Todas as gravações podem ser ativadas e reproduzidas após autenticação por funcionários (magistrados e escrivães/funcionários). Além disso, só podem ser utilizados com ligação à rede de justiça, salvo se for solicitada cópia digital pelas partes no processo.

Comentário:

Mais uma vez observa-se que mais de um servidor pode ter acesso às informações armazenadas sobre dados pessoais. Não houve a especificação sobre uso de protocolos, treinamentos. Há autenticação feita pelos funcionários, que acredita-se ser uma medida de segurança genérica, adotada para todas as atividades jurisdicionais.

Dessa forma, o tribunal parece estar desprovido de medidas especiais para a abordagem a respeito da coleta, tratamento e armazenamento dos dados pessoais dos envolvidos nas audiências remotas.

8. La realizzazione delle udienze è effettuata da qualsiasi dipendente del settore/sezione?

Le videoregistrazioni vengono effettuate dal personale dipendente assegnato alla sezione GIP/GUP o Dibattimento che assiste il giudice in udienza.

Tradução:

8. A realização de audiências é realizada por algum funcionário do setor/seção?

Resposta:

As gravações de vídeo são feitas por funcionários lotados no GIP/GUP ou Seção de Audiência que auxiliam o juiz na audiência.

Comentário:

As gravações serem realizadas por funcionários de um setor específico pode ser analisado de forma positiva. Isso porque, imagina-se que sejam pessoas designadas apenas para essa atividade.

Entretanto, a problemática da falta de senha para acesso aos dados ainda é um desafio, pois em se tratando de meios virtuais, o acesso realizados por invasores mais facilitado. As medidas de segurança precisam ser pautadas na construção de etapas e camadas que tornem dificultoso o acesso às informações dessa natureza.

9. Qualsiasi dipendente del settore/sezione ha accesso all'archiviazione delle registrazioni?

Può accedere al sistema di archiviazione delle registrazioni solo il personale dipendente abilitato (magistrati, cancellieri, funzionari della sezione penale).

Tradução:

9. Algum funcionário do setor/seção tem acesso ao armazenamento de registros?

Resposta:

Apenas funcionários autorizados (magistrados, escrivães, funcionários da secção criminal) podem aceder ao sistema de arquivo de registros.

Comentário:

O acesso aos dados apenas para funcionários, magistrados e escrivães é uma das formas que podem ser adotadas para proteger os dados pessoais. Porém, não se trata da única forma

para garantir segurança. É necessário que outras medidas sejam proporcionadas e seguidas por todos que estejam na atividade jurisdicional.

TRIBUNAL DE JUSTIÇA DE PERNAMBUCO – BRASIL

- 1. Os servidores (controladores, operadores e encarregados pelo tratamento dos dados pessoais) do Tribunal de Justiça de Pernambuco recebem treinamento sobre a Lei Geral de Proteção de Dados e demais regulamentos e resoluções pertinentes ao tema?**

Sim. Periodicamente a ESMape oferece cursos sobre proteção de dados, LGPD e segurança da informação.

Comentário:

Observa-se, a partir da resposta a esse questionamento, que o Tribunal de Justiça do Estado de Pernambuco oportuniza treinamento aos servidores para que tenham conhecimento sobre as normativas em matéria de proteção de dados. Nesse sentido, o pessoal tende a estar habilitado a seguir as diretrizes legais e garantir a segurança para a proteção dos dados pessoais coletados nas audiências remotas.

Assim, conhecendo os preceitos legais e as responsabilidades que as legislações impõem, os serventuários devem praticar os atos judiciais em conformidade com as exigências normativas. Isso porque, a partir dos treinamentos, ficam aptos a agirem nos liames legais.

- 2. Há política de proteção de dados estabelecida no âmbito do Tribunal de Justiça do Estado de Pernambuco?**

Sim. É a RESOLUÇÃO Nº 454, DE 08 DE JUNHO DE 2021, disponível no nosso portal

(<https://portal.tjpe.jus.br/documents/72267/2721558/Resolucao+454+de+2021.pdf/ec068e7f-7e3c-cfee-b211-348e1921eb14>)

Comentário:

A partir da referida resolução, pode-se inferir que o Tribunal prevê o cumprimento dos preceitos estabelecidos na Lei Geral de Proteção de dados. A resolução prevê que o tribunal é controlador ou co-controlador de dados, conforme art. 23, quando no exercício de suas atribuições jurisdicionais. Além disso, prevê outras normativas.

O art. 44 dispõe sobre a previsão de medidas técnicas e administrativas de segurança para a proteção dos dados pessoais contra acessos não autorizados, bem como para situações acidentais ou incidentes culposos ou dolosos de destruição, perdas e etc. Assim, no art. 45 está previsto que o judiciário adote boas práticas e governança para comportamentos adequados que mitiguem riscos que comprometam os dados. Trata-se da disseminação de cultura protetiva no ambiente do tribunal.

Além disso, prevê que o Tribunal deverá, dentre suas atribuições, elaborar o Relatório de Impacto de Proteção de Dados pessoais, com apoio do Comitê Gestor de Proteção de Dados Pessoais. Isso significa dizer que é possível ter diagnósticos a respeito de como ocorrem as atividades no que tange a coleta, tratamento e armazenamento de dados das audiências remotas.

O relatório de impacto proporciona análise sobre os riscos que os dados podem estar sujeitos. Serve para criar planos para adequação à legislação de proteção de dados, pois permite compreender os processos e procedimentos e a vulnerabilidade para minimizar ou evitar dano a eles.

3. Durante a realização das audiências por videoconferência, no Tribunal de Justiça de Pernambuco, ocorre a coleta de dados pessoais dos participantes, sejam partes, servidores, juízes, membros do Ministério Público, testemunhas ou qualquer outra pessoa participante?

Sim. Normalmente, são coletados dados de identificação e solicitado documento pessoal com foto das partes, advogados e intervenientes.

Comentário:

A resposta a essa pergunta permite compreender quais informações são efetivamente coletadas durante a realização do ato de audiência remota. Nesse sentido, identifica-se a evidência da ingerência da legislação de proteção de dados.

Uma vez que ocorre a coleta, tratamento e armazenamento dos dados pessoais oriundos da audiência, compreende-se que o teor da LGPD tem aplicação no âmbito da realização das audiências remotas.

Dessa forma, se faz necessário haver preparação dos servidores, juízes, precauções para evitar riscos de dano sobre os dados coletados. Para isso, treinamento, medidas de segurança e ferramentas adequadas são necessários para atingir o objetivo legal de proteção de dados.

- 4. Em havendo a referida coleta de dados, como esta é realizada? De forma oral, imagens de documentos, escritas em chat ou outro meio? As pessoas são cientificadas do propósito da coleta, segurança e demais orientações pertinentes ao ato praticado?**

Não há procedimento pré-estabelecido, pelo que pode variar de uma unidade judiciária para outra. Porém, frequentemente é solicitado o envio da imagem dos documentos.

Comentário:

A partir da coleta de nome, identidade, imagens e demais informações pessoais, é possível identificar os titulares dos dados. Uma vez coletados e armazenados, exige-se a segurança, sob risco de roubos e outros prejuízos para os titulares.

Dessa forma, como afirma a legislação, apenas devem ser coletados os dados essenciais para a realização dos atos processuais. Todavia, o fato de não haver um procedimento mínimo a ser utilizado, pode tornar a prática inadequada por ausência do cumprimento normativo.

Isso porque não foi identificada, por exemplo, a informação sobre a justificativa da coleta de dados, bem como, como estes serão tratados e armazenados nos arquivos do tribunal. A explicação precisa ocorrer durante a realização da coleta para que o titular fique ciente sobre o motivo de fornecer suas informações pessoais e a conformidade com a legislação de proteção de dados. Deve informar também quais meios que o titular deve procurar, caso necessite alterar seus dados ou precise suprir dúvidas sobre os arquivos deles.

- 5. Como se dá o armazenamento das gravações de audiência por videoconferência no âmbito do Tribunal de Justiça de Pernambuco? O servidor(a) responsável segue algum critério específico?**

Conforme orientação da setic, as gravações são armazenadas na rede do Tribunal, na nuvem (Microsoft - Onedrive).

Comentário:

O armazenamento realizado em rede, nuvem, necessita de meios de segurança eficientes para proteger a identidade dos titulares. Não foi informado se há algum critério específico para a realização desse ato. Desse modo, o fato de estar em um espaço virtual, o material coletado pode estar vulnerável.

Não há como afirmar se a forma de armazenamento atende os critérios de segurança. Considerando que há política de proteção de dados pessoais e que o tribunal realiza treinamento sobre a matéria, pode-se supor que medidas sejam adotadas para minimizar ou impedir riscos de segurança. Todavia, é importante para a segurança que sejam estabelecidas rotinas, como por exemplo, uso de senhas de segurança para fortalecer o sistema.

6. Por quanto tempo as gravações ficam armazenadas nos arquivos do Tribunal?

Não há nenhum ato estabelecendo um limite temporal, de modo que fica a critério da unidade.

Comentário:

Importante mencionar que o tempo de armazenamento dos dados é o tempo que eles precisam estar tutelados pelo tribunal. Isso porque, é responsabilidade do órgão o cuidado com as informações que forem coletadas durante o exercício de sua função jurisdicional.

Entretanto, é importante compreender o motivo que fundamenta a manutenção das gravações nos arquivos digitais do tribunal. A justificativa do motivo de armazenamento servirá para analisar as necessidades de medidas preventivas para evitar danos aos dados.

Em não havendo tempo para a manutenção dos arquivos, pode-se presumir que a obrigação com a tutela das informações é permanente. Isso quer dizer que é crescente o número de dados alojados nas nuvens, o que por sua vez enseja um trabalho constante do tribunal para preservação deles.

7. Quais critérios de segurança e proteção das gravações? Há exigência de protocolos específicos, como uso de senhas, treinamento específico? Os critérios de segurança são os mesmos aplicados a qualquer ato/documento processual.

Não há protocolo ou treinamento específico para videoconferências.

Comentário:

Os riscos podem ser minimizados em razão do trabalho específico para a atividade desenvolvida. Isto é, adotando-se medidas ou protocolos específicos para cada atividade, a tendência de a medida de proteção ser específica e adequada para cada ato é maior.

Nesse sentido, a análise minuciosa das atividades permite elaboração de um procedimento padrão e adequado às operações realizadas. Ao padronizar as práticas, permite-

se melhor organização, identificação e minimização de erros que venham a causar prejuízo aos dados.

O art. 9º da resolução menciona que os dados tratados serão mapeados e inventariados. Serão protegidos por procedimentos internos, sendo mantidos os registros de tratamento, incluindo finalidade, base legal utilizada, avaliação de riscos aos titulares, com trilhas de auditoria para registrar autorizações, utilização, impactos e violações.

Além disso, o inciso V do mesmo artigo, prevê revisão em periodicidade, sinalizando que serão eliminados os dados depois de cumpridos as suas finalidades ou por ter encerrado o seu prazo de retenção. Como respondido no questionário, não previsão de tempo para o armazenamento. Tampouco, há informação de quais critérios devem ser utilizados para que se dê por encerrado o tempo de manutenção dos dados em arquivos.

8. A realização das audiências é feita por qualquer servidor do setor/vara?

Não. a designação de qual/quais servidores responsáveis é realizada pela própria unidade.

Comentário:

A realização da audiência por qualquer servidor, considerando que não há um treinamento específico e protocolo específico, pode-se aduzir que há inadequação a lei geral de proteção de dados e a resolução do procedimento de coleta, tratamento e armazenamento dos dados pessoais durante a realização das audiências remotas.

Isso porque, não há um padrão previamente definido e o acesso às informações é dado a qualquer servidor o que pressupõe uma vulnerabilidade, tendo em vista que não há um protocolo específico, tampouco o uso de senhas e demais cautelas pertinentes para garantir a segurança da informação.

9. Qualquer servidor do setor/vara tem acesso ao armazenamento das gravações?

Não. Assim como os demais atos/documentos processuais são armazenados no perfil específico da unidade (Vara, gabinete), cujo acesso é restrito a servidores com determinados perfil ou pontualmente autorizados.

Comentário:

A resposta a esse questionamento auxilia em uma melhor compreensão da rotina da vara quando da realização da audiência remota. Em questionamentos anteriores, foi informado sobre não haver protocolo específico para a realização de audiências por videoconferência. O recomendado é que seja traçado um procedimento voltado para a atividade específica para que se possa minimizar os riscos que forem inerentes a essa atividade.

Todavia, reconhece-se que tornar restrito o acesso às gravações, ainda que na própria vara, é medida segura para minimizar a vulnerabilidade dos dados. Essa medida visa a dar acesso apenas às pessoas que necessitem dos dados para a realização da atividade. As informações pessoais dos envolvidos nos processos devem ser consultadas apenas quando necessário e por motivo justificado, qual seja, para prosseguimento processual.

Considerando que as audiências são registradas em ata processual e anexadas aos autos, as mídias de gravações são mantidas por medida de garantia documental do processo, não há previsão de delas durante os atos processuais. Ou seja, a lei não exige algum ato a ser realizado que necessite de acesso às gravações.

Considera-se, dessa forma, que, a partir dos questionários disponibilizados para os tribunais italiano e brasileiro, pode-se concluir que o *Tribunale di Pisa* não atende o regulamento europeu, tendo em vista que apresenta atividade não específica, sem maiores cautelas por se tratar de proteção de dados pessoais. O trabalho realizado pelo judiciário não é diferente em relação as demais funções e atividades.

Em razão de existir uma regulamentação específica que tem objetivo de proteger os dados pessoais dos envolvidos, não se observou protocolo voltado para a segurança dessas informações. Nesse diapasão, inclui-se na análise que não há como concluir que os servidores tenham conhecimento total sobre a legislação vigente sobre a matéria, o que inclui o regulamento e demais resoluções e código.

Considera-se, dessa forma, que por não haver informações suficientes, não se pode afirmar estarem adequados às legislações de proteção de dados. Apenas algumas resoluções e regramentos não são suficientes para tirar a conclusão sobre a adequação à normativa, inclusive sobre as operações sobre os dados pessoais coletados em audiências por videoconferência. Logo, ainda que existam tais documentos e informações, não se encontram de fácil acesso, permitindo concluir que ainda não estão em nível de adequação às normas protetivas dos dados pessoais nas audiências remotas.

Prospectivas sobre a vulnerabilidade de dados pessoais na sociedade da informação

O presente tópico tem o propósito de analisar a pesquisa desenvolvida sobre proteção de dados pessoais nesse trabalho à luz da pós-modernidade. Nesse exame, além de discutir as vulnerabilidades das pessoas que disponibilizam os dados pessoais para o judiciário, se propõe também a trazer reflexões, sugestões, mantendo o espaço aberto para outros debates futuros.

Aqui se analisa a conjuntura do ciberespaço, a sociedade da informação e a fragilidade que ainda se perpetua no que diz respeito aos dados pessoais, especialmente no cenário do judiciário. Isso porque, ainda que haja legislação, fiscalização por parte dos órgãos responsáveis, é necessário pensar além para trazer soluções acerca dos desafios encontrados. O buscar mais está atrelado ao desenvolvimento social natural que é constante e por isso se faz necessário um acompanhamento no mesmo ritmo.

Falar sobre essa sociedade da informação é pensar na imersão de uma infinidade de dados em um ambiente virtual, a internet, formando o banco de dados. Dentre as várias nuances que envolvem esse tema, ao falar sobre a vulnerabilidade dos dados pessoais, é necessário pensar sobre a visão trazida por Han²³⁹. Isso porque, em suas obras, ele reflete sobre os problemas da sociedade atual sob perspectivas realistas.

Han elabora o seu entendimento sobre o controle social que pode ser feito a partir dos dados. Em *Sociedade da Transparência*, ele traz a expressão sociedade do controle demonstrando o funcionamento atual das tecnologias e a alimentação do ciberespaço.

Além disso, importante comentar sobre o livre convencimento do titular dos dados. A legislação permite situações em que se exime o controlador dos dados de ter o consentimento para a coleta dos dados pessoais. Nesse sentido, isso vale tanto para pessoas jurídicas de direito público como as de direito privado, quando a lei exige que seja feita a coleta, tratamento e armazenamento das informações.

No que tange ao consentimento, outro ponto importante a ser explicado é o legítimo interesse. Sem uma definição específica elaborada pela lei, diz respeito a uma justificativa de acordo com a atividade desempenhada pelo controlador para que seja realizada com mais

²³⁹ HAN, Byung-Chul. *Sociedade da transparência*. Trad. Lucas Machado. Petrópolis, RJ: Vozes, 2017.

segurança. Além disso, deve estar em compatibilidade com o ordenamento jurídico. O guia de legítimo interesse explica que:

A segunda providência a ser adotada pelo controlador diz respeito à identificação do interesse que justifica o tratamento e à avaliação de sua legitimidade. 16 guia anpd · Hipóteses legais de tratamento de dados pessoais | Legítimo Interesse O interesse é um conceito amplo que abrange qualquer benefício ou proveito que resulta do tratamento de dados pessoais. Garantir maior segurança e promover serviços do controlador são exemplos de interesses que podem ser atendidos com o tratamento de dados pessoais. Por sua vez, o interesse será considerado legítimo quando atender a três condições: (i) compatibilidade com o ordenamento jurídico; (ii) lastro em situações concretas; e (iii) vinculação a finalidades legítimas, específicas e explícitas²⁴⁰.

Sobre o legítimo interesse e o poder público, de acordo com o guia, de maneira geral, a base legal do legítimo interesse deve ser evitada de forma compulsória. E quando o poder público se utilizar do instituto, deverá fazer de forma transparente, respeitando os direitos fundamentais, informando o titular e garantindo a proteção:

Em síntese, no caso do Poder Público, a adoção da base legal do legítimo interesse deve ser evitada quando o tratamento de dados pessoais for realizado de forma compulsória, ou no cumprimento de obrigações, atribuições legais ou regulatórias, sendo admitida, eventualmente, em casos específicos, dependendo do caso concreto. Do mesmo modo, tal qual os demais controladores, o Poder Público, ao realizar o tratamento de dados pessoais com base no legítimo interesse, deve realizá-lo de forma transparente e com a observância dos direitos fundamentais dos titulares, informando-os claramente sobre a finalidade do tratamento, garantindo o acesso a esses dados e adotando medidas de segurança adequadas para garantir a sua proteção²⁴¹.

Nesse sentido, cabe ao controlador e ao operador seguirem o cumprimento do regulamento de proteção de dados, bem como as outras legislações vigentes quanto a responsabilidade sobre os dados pessoais que está sob sua custódia o dever de se adequar à lei.

Além disso, se faz necessário compreender outros pontos acerca dos dados e informações na atual conjuntura. Os autores Menezes Neto, Bolzan e Victoria Fausto trazem algumas considerações sobre a mudança na forma de comunicação, tempo, espaço e previsibilidade quando discutem proteção de dados:

Com isso, noções de espaço, tempo, comunicação, previsibilidade e permanência são forçadas a uma nova composição para ajustar-se às demandas dos fluxos de dados alheios a elementos tão intrínsecos ao regime convencional, como a territorialidade. Nessa perspectiva, conceitos como surveillance e metadados são indispensáveis para a presente análise, uma vez que o primeiro termo se refere à caracterização abrangente

²⁴⁰ BRASIL. ANPD. Guia orientativo. Hipóteses legais de tratamento de dados pessoais. Legítimo interesse. Fev/2024. p. 15. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf. Acesso em 23 jul 2024.

²⁴¹ BRASIL. ANPD. Guia orientativo. Hipóteses legais de tratamento de dados pessoais. Legítimo interesse. Fev/2024. p.27. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf. Acesso em: 23 jul 2024.

do momento atual das relações; ao passo que o outro diz respeito a uma definição indispensável ao estudo que envolve fluxos de dados²⁴².

Eles citam como elementos importantes para esse contexto o *surveillance* e metadados. O *surveillance* não pode ser entendido de forma restrita, pois se caracteriza pelo controle de maior extensão e em todas as camadas da sociedade com uso das tecnologias da informação. Ainda nesse entendimento, eles explicam o conceito de metadados, definindo-os como um conjunto organizado de informações para identificar outras informações ou dados.

A distância entre essa última e aquela está na extensão e envolvimento de todas as camadas da sociedade com as tecnologias da informação, característica da *surveillance*; diferentemente quando da concentração daqueles instrumentos para controle centralizado de informações e influência sobre a maioria, em que ocorre a vigilância, mas não mais condizente ao estado atual de fluidez das relações.

Além disso, convém citar o conceito de metadados como sendo o conjunto organizado de informações que permite localizar, identificar ou definir outro conjunto de dados ou informações. É comum referir-se ao metadado, portanto, como a informação sobre a informação²⁴³.

Na sequência do artigo, os autores refletem sobre as produções normativas são essenciais para proteger direitos humanos, entretanto, ele tem o entendimento que se a abordagem for sem compreender o *surveillance* de nada adiantará.

Os metadados, portanto, são dados dos dados e o *surveillance* é a vigilância sobre esses dados. Trata-se de monitoramento sobre as informações coletadas. Dessa forma, entende-se que a proteção que está em pauta abrange também os metadados.

A pesquisa desse trabalho de tese considera um ponto significativo no contexto mundial. Isso foi tratado no primeiro capítulo quando se abordou a União Europeia como *Modelador de Normas* em matéria de proteção de dados.

Assim, o ponto de vista da União Europeia sobre a matéria tem se replicado em outros países no que diz respeito ao direito fundamental de proteger os dados pessoais dos cidadãos europeus. Nesse sentido, o Brasil seguiu o entendimento europeu como espelho para elaborar a sua regulamentação.

²⁴² DE MORAIS, Jose Luis Bolzan et al. DEMOCRACIA, FLUXO DE DADOS E SOCIEDADE EM REDE: LIMITES DE PROTEÇÃO E CONTROLE ESTATAL A PARTIR DA LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA. *Revista Juridica*, v. 3, n. 70, p. 770-791, 2022. Disponível em: <https://revista.unicuritiba.edu.br/index.php/RevJur/article/view/2913/pdf>.

²⁴³ DE MORAIS, Jose Luis Bolzan et al. DEMOCRACIA, FLUXO DE DADOS E SOCIEDADE EM REDE: LIMITES DE PROTEÇÃO E CONTROLE ESTATAL A PARTIR DA LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA. *Revista Juridica*, v. 3, n. 70, p. 770-791, 2022. Disponível em: <https://revista.unicuritiba.edu.br/index.php/RevJur/article/view/2913/pdf>.

Entretanto, apesar de ter se discutido aqui conceitos, debates sobre publicidade e privacidade, leis e orientações posteriores às regulamentações no Brasil e Itália, como realizado no presente trabalho, identifica-se que o Tribunal de Justiça de Pernambuco encontra-se parcialmente adequado, enquanto o *Tribunale di Pisa* está em processo de adequação. Todavia, há a necessidade de aprimoramento em ambos sobre a condução do tratamento de dados pessoais. Essa medida inclui, dentre as várias condutas, o acompanhamento das atividades desenvolvidas com relação a proteção de dados pessoais.

Destacando o ponto estudado nesse trabalho, qual seja, tratamento de dados pessoais nas audiências por videoconferência, há de se afirmar que o judiciário é Poder Público. Nesse sentido, é um órgão que está em uma exposição, pois sua atividade o coloca em maior evidência, tem função de prestação jurisdicional para a sociedade.

Assim, fala-se sobre a visibilidade do judiciário quanto ao seu banco de dados. Dessa forma, pode-se aduzir que o poder judiciário também apresenta um arquivo virtual atacável quanto à possibilidade de vazamento das informações coletadas em processos judiciais²⁴⁴.

Os autores Bolzan de Moraes, Menezes Neto e Vitoria Fausto debatem sobre regulamentação da internet, comunicação e fluxo de dados, argumentam a forma reducionista que vem sendo tratado o tema privacidade. Além disso, alertam que os problemas da “modernidade líquida” não podem ser resolvidos compreendendo limites territoriais.

Isso não significa dizer que a proteção da privacidade não seja importante. Entretanto, a partir dos estudos analisados nesta obra, objetiva-se deixar claro, fundamentalmente, dois aspectos: primeiro, que é insuficiente a forma reducionista como vem sendo tratada a questão da privacidade, apenas como sinônimo de vida particular, ou seja, de intromissão nas comunicações privadas armazenadas (vide inciso III); segundo, que os problemas oriundos da “modernidade líquida” não podem ser resolvidos a partir de soluções dependentes da territorialidade, como é o caso do marco civil²⁴⁵.

Assim, quando essa pesquisa se propôs examinar os sistemas judiciais, tanto brasileiro, quanto italiano, pôde identificar a necessidade de uma visão sob uma perspectiva mais ampla

²⁴⁴ SECURITY REPORT. Tribunal de Justiça do Pará sofre ataque cibernético. Disponível em: <https://securityleaders.com.br/tribunal-de-justica-do-para-sofre-ataque-cibernetico/>. Acesso em 14 jun 2024.

Ressalte-se que não perda de dados nesse caso. Entretanto, esse episódio demonstra a vulnerabilidade a que o sistema pode estar suscetível.

²⁴⁵ DE MORAIS, Jose Luis Bolzan et al. DEMOCRACIA, FLUXO DE DADOS E SOCIEDADE EM REDE: LIMITES DE PROTEÇÃO E CONTROLE ESTATAL A PARTIR DA LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA. *Revista Juridica*, v. 3, n. 70, p. 770-791, 2022. Disponível em: <https://revista.unicuritiba.edu.br/index.php/RevJur/article/view/2913/pdf>.

no que tange a fluxo de dados. Essa compreensão se consolida a partir da citação acima, que esclarece que o funcionamento da atualidade tem direcionamento diferente de outrora.

Interessante falar sobre a modernidade líquida, expressão de Bauman²⁴⁶. Isso porque corresponde a mudanças constantes em sociedade. Não há estaticidade. O modelo de sociedade hoje é aquele que está em constante movimento. A expressão sobre a liquidez, dentre tantos vieses, está associada de que em um instante as coisas podem não estar mais do mesmo modo. A liquidez tem outras vertentes, como a questão da superficialidade das relações e outras questões que englobam o atual funcionamento social.

No dizer do filósofo: Ser moderno passou a significar, como significa hoje em dia, ser incapaz de parar e ainda menos capaz de ficar parado. Essa expressão traduz o movimento atual da sociedade, constantemente em mudança.

Mas, aqui, falar sobre a liquidez é compreender que as preocupações e estruturas sociais devem caminhar juntas às transformações, as mudanças sociais. A evolução tecnológica é um exemplo do que constantemente evolui. Associado a isso, falar em dados pessoais e a proteção deles, é compreender que se faz necessário um acompanhamento e aprimoramento do sistema em sincronia com os avanços que se apresentam.

Seguindo esse raciocínio, ao pesquisar sobre o sistema judicial italiano, pôde-se encontrar a adoção da mesma medida feita no Brasil, no que diz respeito às audiências. Isso é, sobre o uso de audiências remotas pelo judiciário italiano, instituído durante o período de emergência sanitária do COVID-19, foi estabelecido pelo Decreto-lei nº 11 de 8 de março de 2020 para dar continuidade à prestação jurisdicional e garantir o acesso à justiça.

Ao comentar sobre o assunto e as regras processuais, o professor Mensi²⁴⁷ explica uma temática importante tanto para questões processuais, quanto ao princípio da publicidade e a proteção de dados. Ele informa que não há expressamente uma determinação de restrição de publicidade quanto à matéria de saúde pública. Trata-se de um exemplo importante para as análises aqui feitas.

Isso explica que não haveria de ter impedimento para a realização da audiência remota. Não há restrição processual sobre o assunto. Nem mesmo sobre dados de saúde. E aqui é

²⁴⁶ BAUMAN, Zygmunt. Modernidade Líquida. Tradução Plínio Dentzien. 1ª ed. Rio de Janeiro: Zahar, 2021. p. 40.

²⁴⁷ MENSI, Maurizio. Caratteristiche e criticità della comunicazione da remoto in tema di giustizia. 23 de setembro de 2020. Disponível em: <https://www.amministrazioneincammino.luiss.it/wp-content/uploads/2020/09/MENSI.pdf>. Acesso em: 09 jun 2024.

importante explicar, pois dados de saúde são entendidos como dados pessoais sensíveis, de acordo com a lei geral de proteção de dados. Isso pode fazer repensar sobre a publicidade de processos que tratam de questões de saúde, por exemplo.

Desse modo, como diversos países, a Itália passou a utilizar audiências por plataformas para dar continuidade à prestação jurisdicional. Assim, se observa a mesma problemática de vulnerabilidade, relatada acima quando se abordou sobre o sistema do Brasil, de dados pessoais por conter um banco de dados advindos das referidas audiências.

L'emergenza sanitaria ha rappresentato una sfida soprattutto ai due primi profili, anche se occorre riconoscere come la comunicazione da remoto, lungi dal qualificarsi come una limitazione del principio dell'Open Justice, in realtà sia stata un mezzo per continuare ad assicurare durante l'emergenza l'accesso alla giustizia e la fruizione dei servizi ad essa inerenti. Il che ci ricorda come la qualità e l'efficienza, insieme all'indipendenza, siano elementi essenziali di ogni sistema giudiziario, fondamentali in quanto alla base dello Stato di diritto e dei valori sui quali si fonda l'Unione europea. Disporre di sistemi giudiziari efficienti è infatti fondamentale per la piena attuazione del diritto europeo²⁴⁸²⁴⁹.

Observa-se que a permissão quanto ao uso de audiências remotas está em consonância com a eficiência, independência que são elementos do sistema judiciário, fundamentos do Estado de Direito e estão em conformidade com os valores da União Europeia. É o que relata o professor Mensi.

²⁴⁸ MENSI, Maurizio. Caratteristiche e criticità della comunicazione da remoto in tema di giustizia. 23 de setembro de 2020. Disponível em: <https://www.amministrazioneincammino.luiss.it/wp-content/uploads/2020/09/MENSI.pdf>. Acesso em: 09 jun 2024.

²⁴⁹ Tradução livre: A emergência sanitária representou um desafio especialmente para os dois primeiros perfis, embora deva ser reconhecido que a comunicação remota, longe de ser qualificada como uma limitação do princípio da Justiça Aberta, foi na verdade um meio para continuar a garantir durante a emergência o acesso à justiça e o uso de serviços relacionados. O que nos lembra como a qualidade e a eficiência, juntamente com a independência, são elementos essenciais de qualquer sistema judicial, fundamentais porque sustentam o Estado de direito e os valores em que se baseia a União Europeia. Ter sistemas judiciais eficientes é, de facto, fundamental para a plena implementação do direito europeu.

Dessa forma, a reflexão é de que sempre será urgente debater sobre privacidade e proteção de dados. Principalmente por se viver na intitulada sociedade da informação em um ciberespaço²⁵⁰, como bem preceituam Castells²⁵³ e Lévy²⁵⁴.

É importante observar que o desenvolvimento tecnológico é crescente e constante. Não haverá retrocesso no que diz respeito a tecnologia, a dita sociedade da informação, muito menos sobre o ciberespaço. Tudo isso precisa ser pensado repetidamente à luz da extraterritorialidade. Essa característica é a válvula motriz para o insistente debate sobre proteção de dados a nível global.

A problemática do tratamento de dados pelo judiciário é uma dentre as tantas que precisam ser constantemente repensadas e não sendo somente um problema local, daquele país. As audiências por videoconferência são utilizadas corriqueiramente em processos judiciais, quando possível ou sugerido, em se tratando de Brasil, por exemplo, conforme autorizado em lei.

No Brasil, como visto, há a opção do juízo 100% digital. Isso se traduz sobre a possibilidade de haver um processo completamente virtualizado. E, nesse contexto, é preciso pensar sobre as repercussões e cautelas a serem tomadas para minimizar a possibilidade de causar danos às partes envolvidas.

Realizar audiência por videoconferência é saber que, além dos dados coletados de forma escrita, como ata virtual ou chat de conversa da plataforma, também ocorrem os armazenamentos de imagens, dentre tantas outras possíveis informações. Isso porque, após a realização do ato, as mídias ficam armazenadas nos arquivos digitais dos tribunais.

²⁵⁰ Expressão originalmente criada por William Gibson em 1984 que expressou uma visão científica inspirada no mito ou alegoria da Caverna de Platão, uma realidade presa ao metaverso. Depois passou a ser utilizada por Lévy como ambiente global.

²⁵¹ PIMENTEL, Alexandre Freire. Tratado de direito e Processo Tecnológico. Vol. II. Big Data, Justiça 4.0 e a digitalização da processualização, ciberespaço, metaverso, legal design e visual Law: o Direito Processual Tecnológico. Ed. Publius. Recife, 2023. p. 191.

²⁵² SALDANHA, Paloma Mendes. **PRIVACIDADE E VIGILÂNCIA: A COVID-19 COMO JUSTIFICATIVA E A SOCIEDADE COMO FRUTO DA COLHEITA DIGITAL**. In book: Pensar a PANDEMIA: perspectivas críticas para o enfrentamento da crise (pp.430-444). Publisher: Tirant Lo Blanch. Disponível em: https://www.researchgate.net/publication/370099717_PRIVACIDADE_E_VIGILANCIA_A_COVID-19_COMO_JUSTIFICATIVA_E_A_SOCIEDADE_COMO_FRUTO_DA_COLHEITA_DIGITAL. Acesso em: 16 jun 2024. p. 429.

²⁵³ CASTELLS, Manuel. A sociedade em rede. A era da informação: Economia, Sociedade e Cultura. Vol I, Ed. Paz & Terra. 2020.

²⁵⁴ LÉVY, Pierre. Cibercultura. Tradução Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

Uma vez coletados e armazenados em ambientes digitais, encontram-se na internet. Acessíveis de qualquer lugar do mundo. Portanto, vulneráveis não só no Brasil, mas em qualquer lugar. Assim como também estão vulneráveis os dados coletados na Itália e qualquer outro país que realize essa tarefa.

Tudo isso significa que as plataformas, sistemas e modos de operação dos tribunais precisam investir constantemente no maior nível de segurança possível. A segurança pode estar associada tanto aos softwares, quanto à preparação da equipe que realiza as operações nas audiências, armazenando e tratando os dados pessoais.

O professor Alexandre Freire Pimentel denomina, em sua obra, de “big data jurisdicional” o grande volume de informações processuais. Ele demonstra a preocupação sobre a adequação do judiciário brasileiro à legislação de proteção de dados.

Interessa, também, investigar se os meios de proteção de dados pessoais adotados pelo judiciário, além de estarem em conformidade com a legislação de regência, são realmente aptos e eficientes para ensejar uma efetiva proteção contra a sua coleta, tratamento e uso indevidos, em especial pelas empresas privadas que prestam serviços ao judiciário no ambiente da prática de atos processuais telepresenciais, bem como digitalização de autos físicos, busca de informações em sítios oficiais dos tribunais, armazenamento em nuvens etc.

O big data jurisdicional, portanto, está inserido num ambiente mais amplo (big data universal) e é constituído pelos dados armazenados em data centers ou depositados em nuvens digitais dos tribunais e do Conselho Nacional de Justiça, que passou a utilizar os serviços da Amazon Web Services (AWS) para essa finalidade. Esses dados também são captados, estocados e minerados por terceiros estranhos ao judiciário, a partir de consultas públicas virtuais realizadas nos autos dos processos e em publicações das decisões jurisdicionais e decisões administrativas nos diários da justiça eletrônico, as quais são realizadas por algoritmos sentinelas programados para esse específico desiderato²⁵⁵.

Essa preocupação com a proteção do sistema é visualizada no texto do prof. Mensi:

A ciò si aggiunge la necessità di proteggere sistemi, reti e dati dagli attacchi informatici, tenendo conto che le vulnerabilità dei due sistemi, in presenza e in modalità digitale (vale dire mediante la trasmissione di dati) sono completamente diverse. Il che significa che occorre tutelare sistemi e reti garantendo integrità ai dati che vi sono veicolati e conservati, in primis tramite il rispetto delle norme vigenti in tema di protezione dei dati personali (il regolamento UE 2016/679 e il codice in materia di protezione dei dati personali, d.lgs. n. 196/2003) e sicurezza cibernetica (d. lgs. n. 65/2018 e legge n. 133/2019)²⁵⁶.

²⁵⁵ PIMENTEL, Alexandre Freire. Tratado de Direito e Processo Tecnológico. Vo. II. Big Data, Justiça 4.0 e a digitalização da processualização. Ciberespaço, Metaverso, Legal Design e Visual Law: O direito Processual Tecnológico. Ed. Publius, Recife. 2023. p. 112-113.

²⁵⁶ Tradução livre: A isto acrescenta-se a necessidade de proteger sistemas, redes e dados contra ataques cibernéticos, tendo em conta que as vulnerabilidades dos dois sistemas, em presença e em modo digital (ou seja, através da transmissão de dados) são completamente diferentes. O que significa que é necessário proteger os sistemas e as redes, garantindo a integridade dos dados que aí são transmitidos e armazenados, principalmente através do cumprimento da regulamentação em vigor sobre a protecção de dados pessoais (Regulamento UE 2016/679 e o código sobre a protecção de dados pessoais). dados

Assim como ele afirma que o uso de ferramentas traz a garantia do acesso à justiça e cumpre os preceitos fundamentais do Estado de Direito, ele sustenta que o uso das ferramentas não deve abolir os meios tradicionais. Isso porque, há os cidadãos que não tem o acesso à internet e meios tecnológicos e para eles precisa ser mantido o direito de acesso à justiça.

Ainda assim, como citado o trecho acima, o autor explica que é necessário proteger o sistema, as redes, os dados contra os ataques cibernéticos. Ele explica que a vulnerabilidade do sistema físico é diferente do digital. Afirma que é necessário garantir a integridade dos dados que são veiculados e armazenados de modo que atenda os preceitos do GDPR e as normas de segurança cibernética (Decreto legislativo nº. 65/2018 e lei nº. 133/2019).

Aqui é importante explicar sobre a vulnerabilidade cibernética. Trata-se de uma fragilidade que os dados pessoais estão submetidos no ambiente virtual. Em se tratando de realização de audiências por videoconferência, essa vulnerabilidade também pode ser identificada. Como dito acima, as mídias são passíveis de acesso caso a segurança não esteja garantida.

A vulnerabilidade dos dados pessoais que aqui se traz, diz respeito ao fato de que uma vez esses dados colocados no espaço virtual sem os devidos protocolos de segurança, ficam passíveis de serem violados. A insegurança dos sistemas e das condutas acerca da coleta, tratamento e armazenamento possibilita o acesso facilitado de hackers a essas informações, deixando os titulares desprotegidos e impotentes diante dos possíveis danos que podem ocorrer.

O espaço virtual onde são armazenadas as informações é um espaço em que se pode ter invasões e roubos de dados. É essa vulnerabilidade que traz preocupação no que diz respeito aos armazenamentos de dados pelo judiciário decorrentes das audiências remotas.

Ressalte-se que sobre a responsabilidade do poder público, aqui tratando-se de poder judiciário, pode-se atribuir a responsabilidade civil quanto ao dano que venha ocorrer em razão de roubo ou vazamento de dados coletados em audiências remotas. O art. 42 da LGPD traz o dever do controlador ou operador de reparar quando causar dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados.

personais). dados pessoais, Decreto Legislativo n.º 196/2003) e segurança cibernética (Decreto Legislativo n.º 65/2018 e lei n.º 133/2019).

Os agentes de tratamento apenas deixarão de ser responsabilizados civilmente, conforme previsto no art. 43 da LGPD, se provarem não ter realizado o tratamento de dados, se o dano decorrer de culpa exclusiva do titular ou de terceiros, ou se não tiver havido violação aos termos da LGPD. A própria lei se encarrega, assim, de estabelecer as causas excludentes de responsabilidade aplicáveis à matéria, cumprindo assumir, portanto, que os aludidos agentes respondem objetivamente pelos danos causados, eis que não cogita a LGPD de verificação de culpa ou dolo como elementos necessários à caracterização do dever de reparar²⁵⁷.

As reflexões tecidas neste tópico precisam partir de alguns pressupostos. O primeiro deles é o fato de que a existência do ciberespaço elimina os limites territoriais, como afirmado acima sobre a extraterritorialidade. Essa reafirmação se dá porque a problemática discutida sobre proteção de dados deixa de ser local e passa a ser global.

Com a afirmação sobre a eliminação dos limites territoriais concebidos a partir do uso da rede mundial de computadores, o professor Pimentel entende que:

(...)A mundialização da rede, nesse aspecto ontológico, requer do poder judiciário uma atuação consentânea com essa realidade, no sentido de fazer atuar o ordenamento jurídico interno nos seus limites territoriais para coibir qualquer violação ou ameaça de violação a direito ocorrida na rede, ainda que no exterior, recorrendo a meios igualmente tecnológicos para proteger direitos subjetivos²⁵⁸.

Acredita-se que a regulação interna do judiciário deve ocorrer e deve ser constante. Buscando acompanhar os avanços tecnológicos. Cada órgão tem a responsabilidade de trabalhar na eliminação das dificuldades sobre proteção de dados em suas atividades. Regulamentar especificamente é uma tarefa minuciosa e precisa se realizar pelo próprio órgão judiciário, pois ele é o executor das tarefas judicantes, incluído aqui os fiscalizadores, como o CNJ.

Entretanto, entende-se que a regulamentação no ordenamento interno pode e deve caminhar em consonância com a construção de uma compreensão mais próxima dos direitos humanos. A proposta é de uma sociedade não só conectada tecnologicamente, mas também sobre humanidade. A preocupação deve seguir o sentido de proteção de direito fundamental, como é identificada a proteção dos dados pessoais.

Sobre as vulnerabilidades dos dados, podem ser criadas rotinas de segurança, protocolos a serem seguidos e, do ponto de vista informático, criação de camadas de segurança, bem como a possibilidade de criptografia das informações pessoais.

²⁵⁷ GODINHO, Adriano Marteleto; NETO, Genésio Rodrigues Queiroga; TOLÊDO, Rita Cássia Morais. A responsabilidade civil pela violação a dados pessoais. **Revista IBERC**, v. 3, n. 1, 2020. Disponível em: <https://revistaiberc.responsabilidadecivil.org/iberc/article/view/105/78>. Acesso em: 17 out 2024.

²⁵⁸ PIMENTEL, Alexandre Freire. Tratado de Direito e Processo Tecnológico. Vo. II. Big Data, Justiça 4.0 e a digitalização da processualização. Ciberespaço, Metaverso, Legal Design e Visual Law: O direito Processual Tecnológico. Ed. Publius, Recife. 2023. p. 212.

Entretanto, é necessário que a medida adotada preserve o princípio da transparência e a publicidade processual. Apesar de existirem várias formas possíveis para proteger o sistema judiciário contra invasão de hackers, sabe-se que uma proteção que garanta segurança absoluta não é possível do ponto de vista tecnológico. Isso porque, tecnologia é um ramo que está sempre sendo aprimorado e, infelizmente, as técnicas maliciosas também seguem em desenvolvimento.

O que se faz necessário é que o trabalho para proteger os dados não cesse. Os treinamentos e as medidas de segurança precisam estar em constante aprimoramento para que se diminuam os riscos de violação do direito a proteção dos dados pessoais. Além disso, o acompanhamento por meio de relatórios e análise sobre possíveis vulnerabilidades cibernéticas. Isso permite atualização de sistemas que estejam em conformidade com os avanços dos desafios frente a proteção de dados.

Além disso, é importante pensar sobre a problemática da vulnerabilidade cibernética no judiciário em um cenário globalizado e hiperconectado. Como já explicado em outros momentos, o que é colocado em meio digital é passível de acesso de qualquer lugar físico. Dessa forma, trata-se de um problema que precisa ser discutido sob várias perspectivas.

Uma regulamentação nacional pode não ser suficiente, tendo em vista que a dinâmica de fluxo de informações não está ligada geograficamente. Se faz necessário um debate global, tal como ocorrem com outros temas de interesse de todos os países.

As informações não estão registradas em papel, estão em armazenamentos digitais. Isso quer dizer que a probabilidade de acesso aos dados pessoais coletados se torne possível de qualquer lugar físico que seja, bastando o acesso à internet.

Sobre instrumentos normativos a nível global, pode parecer uma ideia complexa, pois exige a adesão de todos os países. Entretanto, a Organização das Nações Unidas²⁵⁹ aprovou por consenso resolução sobre governança da inteligência artificial, com objetivo de criar um mundo mais seguro e equitativo. Tal resolução é um exemplo de debate a nível global frente aos avanços tecnológicos e as problemáticas que advenham das novas conjunturas.

²⁵⁹ ONU. Organização das Nações Unidas. ONU adota por consenso resolução para reger a inteligência artificial. Disponível em: <https://news.un.org/pt/story/2024/03/1829446>. Acesso em: 14 jun 2024.

O professor Pimentel²⁶⁰ entende que a escala jurídica da mundialização é utopia. Exigiria um sistema em que houvesse uma autoridade mundial como a Organização das Nações Unidas ou estipulação por tratados internacionais globais, dentre outros pontos.

Todavia, o que se defende aqui é iniciar o debate a nível global para uma convergência de entendimento sobre proteção de dados pessoais. Considerando o ponto de vista da dignidade da pessoa humana. O que incluiria o trabalho do poder público dentre as situações em que ocorrem o fluxo de dados.

Nesse raciocínio, não há mais como separar o assunto como sendo de apenas um país, pois trata-se de um banco de informações que está acessível em ambiente digital e isso é globalizado. Dessa forma, o cerne da problemática deixa de ser local. A comunicação, o acesso à informação e a dados não estão mais relacionados a um grupo, uma cidade ou um país. É uma questão que reverbera para o globo.

A presente pesquisa, portanto, se propôs a trazer uma pequena amostra do que ocorre em dois países, Itália e Brasil, e, especificamente, em duas cidades, Recife e Itália, Pisa no âmbito processual judicial, especificamente sobre as audiências remotas e o armazenamento dos dados pessoais que nela são coletados. Não se traz contabilidade de informações a nível numérico e gráfico, servem para exemplificar e trazer pontos para debates e direcionar a pesquisa sobre o que precisa ser trabalhado.

Seguindo esse sentido, o estudo faz pensar sobre uma harmonização global sobre proteção de dados, isso porque uma problemática que abrange todos os países enseja um trabalho em coletivo. Dessa forma, entendeu-se necessário remeter-se ao estudo desenvolvido por McLuhan²⁶¹. Ele traz o ideal de uma aldeia global. De uma convergência, uma só comunidade, uma só tribo.

Nossa civilização especializada e fragmentada. baseada na estrutura centro-margem, subitamente está experimentando uma reunificação instantânea de todas as suas partes mecanizadas num todo orgânico. Este é o mundo novo da aldeia global.

²⁶⁰ PIMENTEL, Alexandre Freire. Tratado de Direito e Processo Tecnológico. Vo. II. Big Data, Justiça 4.0 e a digitalização da processualização. Ciberespaço, Metaverso, Legal Design e Visual Law: O direito Processual Tecnológico. Ed. Publius, Recife. 2023. p. 212.

²⁶¹ MCLUHAN, Marshall. Os meios de comunicação como extensões do homem. Tradução Décio Pignatari. Ed. Cultrix. São Paulo. Disponível em: https://edisciplinas.usp.br/pluginfile.php/352425/mod_resource/content/1/MCLUHAN%2C%20Marshall%20-%20Os%20Meios%20de%20Comunicac%CC%A7a%CC%83o%20como%20Extenso%CC%83es%20do%20Homem.pdf. Acesso em 08 jun 2024.

Castro e Delfim debatem o conceito trazido por McLuhan sobre Aldeia Global. O conceito de que o mundo estaria interligado em uma cultura unificada por meio da tecnologia, para muitos não faz sentido. Isso porque, as pessoas contrárias entendem que esse momento que é falado por McLuhan²⁶² é o agora, a partir do momento em que começou a existir a internet e a aldeia global não aconteceu como previsto.

O filósofo Marshall McLuhan cunhou, na década de 60 do século passado, o polêmico conceito de aldeia global para descrever um mundo em que todos estariam interligados em uma cultura unificada por meio da tecnologia. Meio século depois, muitos acreditam que esse tempo já chegou graças à internet. Vinícius Pereira, professor da Universidade Estadual do Rio de Janeiro (UERJ), discorda de tal visão. Na abertura do Seminário 100 anos McLuhan, nesta quinta 10, ele defendeu que a utopia concebida pelo canadense está longe de ser alcançada²⁶³.

O professor ao abordar esse ideal, causou uma impressão utópica para alguns. Muitos não acreditam nessa ideia de unificação. Talvez, como afirmando mais acima, se o pensamento for sobre a perspectiva de que haja uma homogeneidade, unicidade, padrão, conceitos e cultura iguais, sim, se torna utópico. Os próprios autores acima referenciados relatam essa oposição.

Todavia, com o cenário atual, acredita-se na necessidade de um debate a nível global urgente. O que se pretende dizer é que, em matéria de privacidade e de proteção de dados, é necessário haver uma convergência a nível macro. Isso refletirá em todas as relações sociais globais, sejam elas interpessoais, nacionais ou internacionais.

Dugnani²⁶⁴ elaborou um artigo que traz uma perspectiva mais realista para a condição da atualidade. Em seu texto sobre meios de comunicação e aldeia global, ele reflete sobre a interculturalidade. O que significa dizer uma harmonia, considerando as diferenças culturais, sociais, etc.

²⁶² Ainda que o estudioso McLuhan tenha modificado seu entendimento sobre aldeia global em sua obra “do Clichê ao Arquétipo” é importante trazer a reflexão anterior que favorece a um ideal de aldeia global.

²⁶³ CASTRO, Flavio; DELFIN, Cristiane. A internet não é a aldeia global de McLuhan. Professores reunidos em encontro de debates pelos 100 anos do filósofo canadense questionaram uso do termo criado por Marshall McLuhan para descrever a realidade atual. Disponível em: <https://www.unbciencia.unb.br/humanidades/48-comunicacao/212-a-internet-nao-e-a-aldeia-global-de-mcluhan-dizem-especialistas>. Acesso em: 08 jun 2024.

²⁶⁴ DUGNANI, Patrício. Meios de comunicação e Aldeia Global: globalização, desglobalização e interculturalidade. 2022. Disponível em: https://www.researchgate.net/profile/Patricio-Dugnani/publication/361680536_Meios_de_comunicacao_e_Aldeia_Global_Globalizacao_desglobalizacao_ao_e_interculturalidade/links/62bf53290bf6950edea25713/Meios-de-comunicacao-e-Aldeia-Global-Globalizacao-desglobalizacao-e-interculturalidade.pdf. Acesso em 08 jun 2024.

Ele não desconsidera por total o ideal de Aldeia Global, como trazido por McLuhan. Entretanto, faz considerações sobre a necessidade de se pensar sobre esse debate global, considerando as diferenças.

Por causa disso, para compreender melhor o conceito é preciso entendê-la como um sistema, ou seja, formada por vários elementos que a compõem, mas que não se desenvolvem de maneira independente, mas sim, de maneira convergente. Nesse sentido, a interculturalidade se assemelha muito à comunicação, por sua estrutura sistêmica, assim como são ideias entrelaçadas, pois uma, na verdade, se compõem na relação com a outra: as culturas, e, conseqüentemente, as relações entre elas, se constituem através da comunicação, enquanto a comunicação se organiza, a partir das relações sociais inseridas num processo cultural. Por isso, a interculturalidade, ou seja, o pensamento intercultural, é expressa pelo seu componente estruturante: a comunicação intercultural²⁶⁵.

Ele discute sobre a globalização, considerando que a interculturalidade precisa ser compreendida como um sistema. Os elementos dessa interculturalidade precisam seguir de maneira convergente. Precisa ser entendido como um estudo e como uma ação comunicativa.

Como ação comunicativa, a relação entre culturas, mediadas, agora, principalmente, pelos meios digitais e globalizantes, pode ser estudada, para que se criem estratégias que possibilitem o desenvolvimento do contato, e, a consequente mistura de culturas. Essas misturas entre culturas, as quais, com o avanço tecnológico dos meios, já tem sido produzida durante a existência humana, não ocorrem, em grande parte das vezes, de maneira justa, equilibrada e pacífica, mas sim de maneira hierárquica, etnocêntrica e violenta.(...)

Ou seja, pensando a interculturalidade como estudo, ou como ação comunicativa, é importante ressaltar um preceito desse pensamento que se busca desenvolver na Pósmodernidade: ressaltar as semelhanças entre as culturas. Por isso, observar no que as culturas se assemelham, pode ser uma estratégia de aproximação entre elas, tendo em vista que, com o advento dos meios digitais, acelerou-se o processo de trocas entre culturas locais, aumentando, também, a velocidade, tanto do processo de mistura entre culturas, quanto o surgimento, ou melhor, o ressurgimento de uma resposta contrária e preconceituosa na forma de discursos polarizados, do resgate de visões etnocêntricas, do preconceito, e mesmo, da violência.

Ele entende que os estudos interculturais podem ser uma opção para esse momento inevitável de mistura de culturas. Ele considera ainda, nesse contexto, as teorias de McLuhan, entretanto, entendendo que o mundo não está exatamente como foi elaborado pelo filósofo da aldeia global.

Ao mesmo tempo, em outro artigo, Dugnani discute o paradoxo da desglobalização, de protecionismo, fechamento de fronteiras e o movimento das comunicações digitais que tendem a ser mais globalizantes, ampliando os contatos. Em seu texto, aborda o que ele entende ser

²⁶⁵ DUGNANI, Patricio. Meios de comunicação e Aldeia Global: globalização, desglobalização e interculturalidade. 2022. Disponível em: https://www.researchgate.net/profile/Patricio-Dugnani/publication/361680536_Meios_de_comunicacao_e_Aldeia_Global_Globalizacao_desglobalizacao_e_interculturalidade/links/62bf53290bf6950edea25713/Meios-de-comunicacao-e-Aldeia-Global-Globalizacao-desglobalizacao-e-interculturalidade.pdf. Acesso em 08 jun 2024.

uma desglobalização dos sistemas políticos em contraponto com a globalização dos meios de comunicação.

Com esta reflexão, apresenta-se o movimento complexo e paradoxal de desglobalização dos sistemas políticos e de globalização dos meios de comunicação, para buscar compreender esse impasse que amplia as incertezas e as tensões entre os grupos humanos da sociedade em âmbito mundial²⁶⁶.

Ainda nessa análise global, convém comentar a pós-modernidade, momento atual, tratada por Stuart Hall. No entendimento dele estão surgindo novas identidades, o indivíduo moderno não tem as mesmas características do indivíduo de outrora. Ele chama de “crise de identidade”.

A questão da identidade está sendo extensamente discutida na teoria social. Em essência, o argumento é o seguinte: as velhas identidades, que por tanto tempo estabilizaram o mundo social, estão em declínio, fazendo surgir novas identidades e fragmentando o indivíduo moderno, até aqui visto como um sujeito unificado. A assim chamada “crise de identidade” é vista como parte de um processo mais amplo de mudança, que está deslocando as estruturas e processos centrais das sociedades modernas e abalando os quadros de referência que davam aos indivíduos uma ancoragem estável no mundo social²⁶⁷.

Ele complementa que as sociedades modernas são, portanto, por definição, sociedades de mudança constante, rápida e permanente. Nesse sentido, afirma que essa é a principal distinção entre a sociedade “tradicional” e a sociedade “moderna”²⁶⁸.

Castells, ao comentar sobre as transformações que a sociedade passou e passa, ele afirma que:

Devido a essas tendências, houve também a acentuação de um desenvolvimento desigual, desta vez não apenas entre o norte e o sul, mas entre os seguimentos e territórios dinâmicos das sociedades em todos os lugares e aqueles que correm risco de tornar-se irrelevantes sob a perspectiva da lógica do sistema. Na verdade, observamos a liberação paralela de forças produtivas consideráveis da revolução informacional e a consolidação de buracos negros de miséria humana na economia

²⁶⁶ DUGNANI, Patricio. Globalização e desglobalização: outro dilema da Pós-Modernidade (Globalization and deglobalization: another dilemma of Post-Modernity). Revista Famecos, Porto Alegre, v. 25, n. 2, p. 1-14, maio, junho, julho e agosto de 2018: ID27918. DOI: <http://dx.doi.org/10.15448/1980-3729.2018.2.27918>. Acesso em: 08 jun 2024.

²⁶⁷ HALL, Stuart. A identidade cultural na pós-modernidade. tradução Tomaz Tadeu da Silva, Guaracira Lopes Louro-11. ed. -Rio de Janeiro: DP&A, 2006. Disponível em: https://leiaarqueologia.wordpress.com/wp-content/uploads/2018/02/kupdf-com_identidade-cultural-na-pos-modernidade-stuart-hallpdf.pdf. Acesso em: 08 jun 2024, p. 7.

²⁶⁸ HALL, Stuart. A identidade cultural na pós-modernidade. tradução Tomaz Tadeu da Silva, Guaracira Lopes Louro-11. ed. -Rio de Janeiro: DP&A, 2006. Disponível em: https://leiaarqueologia.wordpress.com/wp-content/uploads/2018/02/kupdf-com_identidade-cultural-na-pos-modernidade-stuart-hallpdf.pdf. Acesso em: 08 jun 2024, p. 14.

global, quer em Burking Faso, South Bronx, Kammagasaki, Chiapas, quer em La Courneuve²⁶⁹.

Ele relata a desigualdade no desenvolvimento global, mostrando que a dinamicidade, forças de produção e, em contrapartida, identifica a miséria humana na economia global. Essa afirmação faz pensar sobre a distância que se está a respeito de haver um parâmetro mínimo a nível de mundo. Ele relata sobre a sociedade da informação e sociedade informacional, o que em tudo estão relacionados com os dados espalhados no ciberespaço.

Sobre isso, pode-se entender que já houve um passo, ainda que incipiente, quando da elaboração da Convenção 108+ que foi idealizada pela União Europeia, mas que tem signatários de países não membros. A proposta da convenção é essa convergência a nível global sobre proteção de dados.

Inclusive, ao trazer a diferença entre Sociedade da informação e Sociedade informacional, elucida sobre como ocorre o funcionamento da sociedade na atualidade:

Gostaria de fazer uma distinção analítica entre as noções de “sociedade da informação” e “sociedade informacional” com consequências similares para economia da informação e economia informacional. O termo sociedade da informação enfatiza o papel da informação na sociedade. Mas afirmo que informação, em seu sentido mais amplo, por exemplo, como comunicação de conhecimentos, foi crucial e todas as sociedades, inclusive à Europa medieval que era culturalmente estruturada intelectual (ver Southern 1995). Ao contrário, o termo informacional indica o atributo de uma forma específica de organização social em que a geração, o processamento e a transmissão da informação tornam-se as fontes fundamentais de produtividade e poder devido às novas condições tecnológicas surgidas nesse período histórico (...) ²⁷⁰.

É importante refletir sobre a sociedade informacional, sem desmerecer a expressão anterior. Isso porque, a informacional descreve a condução da organização social. Ele ressalta que a forma como se lida com informação fundamenta a produtividade e poder. Nesse sentido, dado é informação. A circulação é instantânea em razão da velocidade tecnológica. Daí a preocupação sobre a inserção desses dados no ambiente virtual.

Sobre uma visão generalista, uma vez que se instalam nos bancos virtuais, os dados não estão apenas sob os cuidados de quem tem a responsabilidade para tal. Na verdade, a responsabilidade continua, o dever de zelar permanece, entretanto, não existe um meio absolutamente seguro de proteção.

²⁶⁹ CASTELLS, Manuel. A sociedade em rede. A era da informação: Economia, Sociedade e Cultura. Vol I, Ed. Paz & Terra. 2020. p. 62.

²⁷⁰ CASTELLS, Manuel. A sociedade em rede. A era da informação: Economia, Sociedade e Cultura. Vol I, Ed. Paz & Terra. 20120. p. 30

Essa discussão é necessária. Compreender que uma vez que os dados estão postos em rede, estão expostos a riscos, são vulneráveis. E Castells demonstra a preocupação sobre as diferenças entre países, pois entende ser fonte da desigualdade.

O fato de países e regiões apresentarem diferenças quanto ao momento oportuno de dotarem seu povo de acesso ao poder da tecnologia representa fonte crucial de desigualdade em nossa sociedade²⁷¹.

Lévy traz seu pensamento sobre conhecimento e informação. Para ele, não são “imateriais” e sim desterritorializados. Esse pensamento tem peso para o debate sobre sociedade da informação, tratamento de dados pessoais e sociedade em sua estrutura global.

Precisamente: o conhecimento e a informação não são “imateriais” e sim desterritorializados; longe de estarem exclusivamente presos a um suporte privilegiado, eles podem viajar. Mas informações e conhecimentos tampouco são “materiais”. A alternativa do material e do imaterial vale apenas para substâncias, coisas, ao passo que a informação e o conhecimento são da ordem do acontecimento ou do processo²⁷².

Esse posicionamento reforça a necessidade de olhar os processos e procedimentos do cotidiano social com uma cautela diferente das realizadas em sistemas anteriores. Quando o zelo sobre as informações estava restrito a documentos em papel ou armazenamentos em gavetas, os níveis de proteção eram de outra ordem.

Lévy esclarece o que significa registrar informação. Quando são feitos no ciberespaço se tornam exploráveis. Aqui ele fala sobre riqueza. Ele mostra que essa disponibilidade se torna constante, ao passo que há consumidores e coprodutores de informações. Uma dinâmica cíclica.

Todo ato registrável cria efetivamente ou virtualmente informação, ou seja, numa economia da informação, riqueza. Ora, o ciberespaço é por excelência o meio em que os atos podem ser registrados e transformados em dados exploráveis. Por isso o consumidor de informação, de transação ou dispositivos de comunicação não cessa, ao mesmo tempo, de produzir uma informação virtualmente cheia de valor. O consumidor não apenas se torna coprodutor de informação que consome, mas é também produto cooperativo dos “mundos virtuais” nos quais evolui, bem como agente de visibilidade do mercado para os que exploram os vestígios de seus atos no ciberespaço²⁷³.

²⁷¹ CASTELLS, Manuel. A sociedade em rede. A era da informação: Economia, Sociedade e Cultura. Vol I, Ed. Paz & Terra. 2016. p. 90.

²⁷² LÉVY, Pierre. O que é virtual? Tradução de Paulo Nevez. São Paulo: Editora 34, 2ª edição, 2017. p.56.

²⁷³ LÉVY, Pierre. O que é virtual? Tradução de Paulo Nevez. São Paulo: Editora 34, 2ª edição, 2017. p.63

Ao abordar inteligências coletivas, Lévy explica que o ciberespaço oferece estrutura de cooperação. Há um contexto comum, reconhecimento mútuo dos indivíduos e dos grupos por meio da atividade da comunicação.

Segundo modalidades ainda primitivas, mas que se aperfeiçoam ano a ano, o ciberespaço oferece instrumentos de construção cooperativa de um contexto comum em grupos numerosos e geograficamente dispersos. A comunicação se desdobra aqui em toda sua dimensão pragmática. Não se trata mais apenas de uma difusão ou de um transporte de mensagens, mas de uma interação no seio de uma situação que cada um contribui para modificar ou estabilizar, de uma negociação sobre significações, de um processo de reconhecimento mútuos dos indivíduos e dos grupos via atividade de comunicação²⁷⁴.

O acompanhamento dos avanços e o constante repensar sobre as formas de se relacionar são necessidades. Estagnar na idealização de que o virtual não tem riscos, que é algo a parte da vida é padecer em um erro. O virtual faz parte da sociedade, é somente uma mais um outro espaço onde se pode interagir. Nesse sentido, Lévy se posiciona sobre o que é a virtualidade:

A virtualidade não tem absolutamente nada a ver com aquilo que a televisão mostra sobre ela. Não se trata de modo algum de um mundo falso ou imaginário. Ao contrário, a virtualização é a dinâmica mesma do mundo comum, é aquilo através do qual compartilhamos uma realidade. Longe de circunscrever o reino da mentira, o virtual é precisamente o modo de existência de que surgem tanto a verdade como a mentira²⁷⁵.

Tanto as reflexões de Castells, quanto as de Lévy demonstram com clareza o que significa estar em uma sociedade pós-moderna de Hall. Eles apresentam os novos riscos, as novas possibilidades, benefícios. Eles apresentam a realidade, alertam para o que se deve pensar e como se deve agir no agora.

Devemos antes de tentar acompanhar e dar sentido à virtualização, inventando ao mesmo tempo uma nova arte de hospitalidade. A mais alta moral dos nômades deve tornar-se, neste momento de grande desterritorialização, uma nova dimensão estética, o próprio traço da criação. A arte, e portanto a filosofia, a política e a tecnologia que ela inspira e atravessa, deve opor uma virtualização requalificante, inclusiva e hospitaleira à virtualização pervertida que exclui e desqualifica.

Preste atenção à interpelação desta arte, desta filosofia, desta política inédita: “seres humanos pessoas daqui e de toda parte, vocês são arrastados no grande movimento da desterritorialização, vocês que são enxertados no hipercorpo da humanidade e cuja pulsação ecoa as gigantescas pulsações deste hipercorpo, vocês que pensam reunidos e dispersos entre o hipercórtex das nações, vocês que vivem capturados, esquarterados, nesse imenso acontecimento do mundo que não cessa de voltar a si e de recriar-se, vocês são jogados vivos no virtual, vocês são pegos nesse enorme salto que nossa espécie efetua em direção à nascente do fluxo do ser, sim, no núcleo mesmo desse estranho turbilhão, vocês estão em sua casa. Bem-vindos à nova morada do gênero humano. Bem-vindos aos caminhos do virtual”²⁷⁶.

²⁷⁴ LÉVY, Pierre. O que é virtual? Tradução de Paulo Nevez. São Paulo: Editora 34, 2ª edição, 2017. p.114

²⁷⁵ LÉVY, Pierre. O que é virtual? Tradução de Paulo Nevez. São Paulo: Editora 34, 2ª edição, 2017. p.148

²⁷⁶ LÉVY, Pierre. O que é virtual? Tradução de Paulo Nevez. São Paulo: Editora 34, 2ª edição, 2017. p. 150.

O movimento da desterritorialização, constantemente referenciado nesse trabalho, é das problemáticas sobre vulnerabilidade dos dados. Lévy, ao falar sobre essa realidade, esclarece que não haverá um retorno para um antes. Ele diz que o mundo não cessa de recriar-se. É o que ele chama de casa, a nova moradia do gênero humano.

As reflexões feitas até aqui demonstram a necessidade do pensar em coletivo. Os autores citados se complementam, abordam a atualidade, trazendo a sua ótica e sobre como há vários caminhos a surgir. São reflexões que quando estudadas, percebe-se a visualização no cotidiano. São várias as perspectivas que se pode ter a partir da leitura atenta das obras aqui trazidas.

Proteção de dados é a grande mina no atual contexto e é também uma infinidade de possibilidades. A união das nações sobre como conduzir tal questão pode ser um direcionamento plausível e com alguns resultados positivos.

Modelar o ciberespaço é trazer muitas tarefas a serem constantemente pensadas e, a depender, realizadas, colocadas em prática. Os dados são riquezas, como são as informações e estão postos neste ciberespaço. A ideia da Aldeia Global não pode ser completamente desconsiderada. Ao menos a reflexão acerca de um debate global pode ser assemelhada ao ideal de aldeia global. Apesar das diferenças conceituais, culturais entre nações, existir uma convergência pode aumentar a possibilidade de proteção do humano que é o principal ator em sociedade.

Doneda, ao abordar o tema de privacidade e proteção de dados, explica que a falta de uma definição âncora sobre o que venha a ser privacidade. Essa afirmação corrobora com a ideia do porquê não se ter a construção de conceito fechado como garantia. Acredita-se que a compreensão sobre os riscos da vulnerabilidade e um olhar sob viés da dignidade da pessoa humana, como fundamentado mais acima, poderá trazer sentido para o ciberespaço.

A verdade é que a falta de uma definição “âncora” que reflita uma consolidação do seu tratamento semântico, não é um problema próprio da doutrina brasileira; tome-se por exemplo a doutrina norte americana, que conta com um vocábulo consolidado (privacy, fortalecido com o reconhecimento do right to privacy) que, no entanto, faz referência a um vasto número de situações, muitas das quais o jurista brasileiro (ou qualquer outro da tradição de civil law) não relacionaria com a privacidade.

Preferimos afirmar, portanto, que a indefinição quanto ao conteúdo do direito à privacidade deve ser tomada mais como uma característica intrínseca da matéria do

que um defeito ou obstáculo. Talvez uma “definição” do que seja privacidade não seja propriamente a principal questão a ser enfrentada²⁷⁷.

O entendimento do professor Doneda é que definição simples de conceito não seja o cerne do problema. Privacidade pode ser compreendido de formas diferentes, como debatido em capítulos anteriores desse trabalho.

O que se propõe não é estabelecer letras fechadas para dar nome a nível mundial. Isso poderia ser dito como utópico. O que se diz é sobre um debate global sobre uma cultura, sobre o que venha a ser proteger os dados. Saber o porquê de ter que pensar sobre esse tema. Algo continuação da Convenção 108.

Dessa forma, deve-se pensar nas diferenças intrínsecas ao ser humano quando se fala em etnias, países e culturas diferentes. Não se almeja uniformidade. Não seria tampouco razoável que fosse assim estabelecido.

O prof. Bolzan *et al* trazem uma reflexão importante sobre proteção à privacidade dos indivíduos na atualidade:

Assim, deve ser feita uma pergunta: como é possível proteger a privacidade em pleno século XXI se a confiança é atribuída somente a instrumentos feitos para lidar com problemas inaugurados no século XVI? É possível afirmar, *mutatis mutandis*, que o imaginário equivocado sobre os limites e possibilidades do marco civil da Internet sofrem da mesma miopia da Lei 13.709/2018, a Lei Geral de Proteção de Dados do Brasil²⁷⁸.

Mais uma vez o professor Doneda explica que a natureza e valores precisam ser levados em consideração. É um debate complexo. Mas se faz necessário levantá-lo com uma maior amplitude. Ele explica o seguinte:

Levar em conta a natureza e o valor conferido à esfera privada em determinadas sociedades, de todo modo, é indispensável para realizar a valoração de sua configuração atual. A ela correspondem funções diversas em gênero e amplitude, funções que hoje devem ser conhecidas para adequá-las ou não ao momento²⁷⁹.

Dessa forma, a complexidade humana enfrenta os desafios advindos dos avanços e transformações tecnológicas. O pensamento sobre a sociedade acontece de outra ordem. Há o físico e o virtual, e a vida acontece com os dois, pois os dois são reais.

²⁷⁷ DONEDA, Danilo. Da Privacidade à proteção de dados pessoais. Ed. Revista dos Tribunais. 3ª edição. Formato E-book. 2021. p. 101 - 103.

²⁷⁸ DE MORAIS, Jose Luis Bolzan et al. DEMOCRACIA, FLUXO DE DADOS E SOCIEDADE EM REDE: LIMITES DE PROTEÇÃO E CONTROLE ESTATAL A PARTIR DA LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA. *Revista Jurídica*, v. 3, n. 70, p. 770-791, 2022. Disponível em: <https://revista.unicuritiba.edu.br/index.php/RevJur/article/view/2913/pdf>.

²⁷⁹ DONEDA, Danilo. Da Privacidade à proteção de dados pessoais. Ed. Revista dos Tribunais. 3ª edição. Formato E-book. 2021. p.114.

Paloma Mendes Saldanha, em seu artigo, traz considerações sobre a coleta de dados pessoais na sociedade hiperconectada. Em suas reflexões, traz diversas problemáticas advindas do ciberespaço, no que tange a dados pessoais.

Diante das análises feitas por ela, só há o fortalecimento da necessidade de um desenvolvimento tecnológico com o olhar da dignidade da pessoa humana. Em sua pesquisa, com o propósito de estudar a relação entre vigilância e dados pessoais, ela demonstra a preocupação que tem sobre o Brasil a respeito do uso dos dados na conjuntura de uma sociedade da informação.

Nesse sentido, ela reforça que o senso de coletividade não tem sido o norte da sociedade e que se faz necessário refletir sobre a trajetória histórica humana, olhando para as coletas de dados já realizadas e os respectivos propósitos. Ela traz questionamento sobre o que é ou não necessário ser feito com a aflição do caminho que se tem seguido a respeito do tratamento de dados pessoais.

Essas e várias outras reflexões percorrem o cotidiano das pessoas que se debruçam a estudar a proteção de dados pessoais não como mera preocupação, mas como visualização de que o Estado democrático de Direito existente, até que se prove o contrário, no Brasil pode estar sendo ameaçado pelo desenvolvimento tecnológico realizado por mãos erradas que não visualizam os dados pessoal como extensão da personalidade dos seres humanos. Mas unicamente como pontos de informação que geram lucro e criam oportunidades de negócios com novos produtos e serviços²⁸⁰.

O olhar que a professora Paloma traz sobre as consequências de os dados pessoais estarem disponíveis faz pensar sobre os riscos e as vulnerabilidades do cidadão. São reflexões necessárias que corroboram com a preocupação desenvolvida nessa pesquisa sobre como são tratados os dados pessoais pelo judiciário.

Complementando o raciocínio acima referenciado, as considerações de Almeida e Barzotto sobre um vazamento ou tratamento indevido de dados pessoais são no sentido de que em ocorrendo tal episódio pode gerar danos imensuráveis. Isso porque a velocidade do fluxo de informações, com o uso da tecnologia, é imediata o que faz dar acesso aos dados pessoais a

²⁸⁰ SALDANHA, Paloma Mendes. **PRIVACIDADE E VIGILÂNCIA: A COVID-19 COMO JUSTIFICATIVA E A SOCIEDADE COMO FRUTO DA COLHEITA DIGITAL**. In book: Pensar a PANDEMIA: perspectivas críticas para o enfrentamento da crise (pp.430-444). Publisher: Tirant Lo Blanch. Disponível em: https://www.researchgate.net/publication/370099717_PRIVACIDADE_E_VIGILANCIA_A_COVID-19_COMO_JUSTIFICATIVA_E_A_SOCIEDADE_COMO_FRUTO_DA_COLHEITA_DIGITAL. Acesso em: 16 jun 2024.

quem não esteja autorizado, o que pode gerar danos que atinjam a dignidade do titular dessas informações.

Um vazamento ou o tratamento indevido de dados pessoais expõem a pessoa física e agride a sua dignidade. É algo que qualquer ser humano não deseja e teme, pois os resultados e os danos que podem gerar a partir do uso indevido de dados pessoais são sérios em uma sociedade interligada e informatizada, onde a cada dia a velocidade da informação está mais rápida e sem limites geográficos. Não querer isso para mim, em uma sociedade fraterna (Constituição Federal, preâmbulo), faz-me não desejar o mesmo para o outro, que é um “outro eu”²⁸¹.

Assim, considerando a concepção da sociedade da informação, dados pessoais são uma das principais preocupações frente aos novos modos de comunicação e constante metamorfose da tecnologia. Assim como toda a sociedade, o poder judiciário precisa acompanhar a remodelação social às suas atividades, seja por meio de normativas ou políticas de adequação a uma proteção de dados, tendo em vista que está inserido nesse modelo de sociedade atual.

A segurança da informação não se restringe a uma única ação e sim um conjunto delas que são adotadas por aqueles que lidam com dados. Essa segurança precisa ser adotada estrategicamente para evitar ameaças, roubos, danos e perdas dos dados. É feita através de um conjunto de processos de forma sincronizada para blindar as informações. Isso se traduz em gestão de riscos que envolvem vários fatores, como análise de vulnerabilidade, formas de controle, fontes de ameaça, entre outros.

Trata-se de um processo que exige o trabalho tanto do setor de tecnologia da informação, quanto dos servidores que trabalham com a coleta, tratamento e armazenamento dos dados. Não adianta ter uma ferramenta de proteção muito bem pensada e os servidores responsáveis não seguirem um rito de segurança.

É importante falar sobre os pilares da segurança da informação. O primeiro deles é a confidencialidade, que quer dizer que as informações sigilosas sejam acessadas apenas por pessoas autorizadas, do contrário pode levar a danos como vazamento, roubos, etc.

Outro pilar é a integridade, que se traduz na garantir de que os dados não serão alterados. Para isso, é determinada a licença para de cada pessoa que irá acessar os dados. Na sequência, o pilar da disponibilidade, que atribui a pessoas específicas o acesso aos dados, ocorrendo alguma invasão, haverá de ter a indisponibilidade.

²⁸¹ ALMEIDA, Isaac Nogueira de; BARZOTTO, Luciane Cardoso. Proteção de dados nos tribunais brasileiros: os principais temas da LGPD. Disponível em: <https://publicar.claec.org/index.php/editora/catalog/download/68/68/754?inline=1>. Acesso em: 09 jun 2024.

Já a irretratabilidade, outro pilar, significa que não há como negar a autoria de um arquivo fornecido pela instituição, autoria de quem realizou a ação ou modificou (não repúdio), trata-se de uma proteção. E, por fim, o da autenticidade que prevê o registro de todas as informações armazenadas ou alteradas e por quem foi realizadas as ações. A deficiência na senha, leitura digital, reconhecimento facial é falha na autenticidade.

É importante que haja uma política da segurança da informação. Nela estão todas as diretrizes a serem seguidas por todos os envolvidos nos procedimentos de coleta, tratamento e armazenamento de dados das audiências. O texto do Docusign apresenta todas as orientações sobre conceito e procedimentos a serem adotados²⁸².

A respeito das alternativas que podem ser tomadas pelos tribunais quanto a responsabilidade sobre a segurança da informação sobre os dados pessoais coletados durante as audiências remotas, pode-se citar o uso de criptografias. O que significa dizer que os dados ficam armazenados de modo indecifrável, apenas aquelas pessoas que tenham a senha poderão acessar tais informações.

Trata-se de uma medida de proteção contra ataque cibernéticos. Além disso, importante investir no treinamento dos servidores e orientações a respeito dos procedimentos que devem ser realizados para garantir a proteção dos dados. Apresentar o funcionamento das tecnologias de modo que se torne viável a utilização segura nas rotinas de audiências²⁸³.

De acordo com o *Guidelines for cybersecurity*, citada por Coelho e Araújo, as regras ISSO/IEC 27032 (2012) e a ISSO/IEC 27002(2005) afirmam que²⁸⁴:

A norma ISO/IEC 27032 (2012) Guidelines for cybersecurity (Diretrizes para a segurança cibernética), alinhada com o "espírito" de segurança da informação inerente à família das normas internacionais 27000, define segurança cibernética como preservação da confidencialidade, da integridade e da disponibilidade da informação no espaço cibernético (ISO/IEC 27032,2012).

²⁸² DOCUSIGN. Segurança da informação: conceito, função e como proteger dados sigilosos. 8 dez 2022. Disponível em: <https://www.docusign.com/pt-br/blog/seguranca-da-informacao#:~:text=Tenha%20um%20plano%20de%20conting%C3%Aancia&text=Logo%2C%20essa%20estrat%C3%A9gia%20preventiva%20precisa,fique%20inativa%20por%20muito%20tempo..> Acesso em: 24 jul 2024.

²⁸³ AWARI. Como garantir a segurança da informação e proteção de dados: dicas essenciais para proteger suas informações. 10 ago 2023. Disponível em: <https://awari.com.br/como-garantir-a-seguranca-da-informacao-e-protecao-de-dados-dicas-essenciais-para-proteger-suas-informacoes/>. Acesso em 24 jul 2024.

²⁸⁴ BARBOSA, Juliana Souza et al. A proteção de dados e segurança da informação na pandemia COVID-19: contexto nacional. **Research, Society and Development**, v. 10, n. 2, p. e40510212557-e40510212557, 2021. Apud Coelho, F. E.S., Araújo, L. G. S. (2013). Gestão da Segurança da Informação NBR 27001 e 27002. Escola Superior de Redes.

Já a norma ISO/IEC 27002 (2005), afirma que a segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizando os riscos e maximizando o retorno sobre os investimentos e as oportunidades de negócio. A segurança da informação é obtida como resultado da implementação de um conjunto de controles, compreendendo políticas, processos, procedimentos, estruturas organizacionais e funções de hardware e software.

Assim, de acordo com as medidas de segurança, uma das ações que devem ser seguidas pelos servidores, estão: o uso de senhas fortes, a troca periódica de senhas, autenticação de dois fatores, pois esta aumenta a camada de proteção fornecendo código por aplicativo ou outra forma de informação.

Além disso, os tribunais precisam manter os dispositivos atualizados. Isso significa dizer que as manutenções das máquinas e todas as ferramentas devem estar sempre atualizadas quanto as novas versões existentes. Importante que haja backups dos dados em outro espaço para garantir que as informações estejam protegidas caso haja alguma invasão e prejudique a segurança dos dados armazenados pelo tribunal.

E, por fim, a política sobre conscientização a partir de treinamentos precisa ser executada com constância. Orientação sobre as operações e medidas realizadas a serem e informações dadas aos titulares dos dados coletados precisam fazer parte de um protocolo criado para garantir a segurança dos dados e a informação a seus titulares.

Portanto, minimizar os riscos a que os dados coletados em audiência remota, em um ambiente virtual estão suscetíveis, é de responsabilidade do Poder Judiciário, considerando uma análise sobre tudo que vem sendo estudado nesse trabalho. Assim, cabe ao judiciário desenvolver mecanismos e soluções de forma permanente que acompanhem os avanços tecnológicos.

CONSIDERAÇÕES FINAIS

Considerando o contexto da Pós-Modernidade, intitulado momento atual da sociedade, em que estão imersas as transformações tecnológicas da sociedade da transformação, o presente trabalho buscou analisar o contexto de proteção de dados no judiciário. Para isso, fez-se um estudo sobre o tema em uma perspectiva global, mas desenvolvendo um exame sob a ótica localizada, quando direciona a pesquisa para análise normativa de dois países, Brasil e Itália.

Com o intuito de construir o trabalho partindo de um ponto comum entre os países, desenhou-se o trabalho a partir do maior para o menor. Ou seja, do regulamento europeu, nascedouro de regras sobre proteção de dados até chegar nas regras de cada país.

Dessa forma, consistiu-se em esmiuçar a origem do tema de proteção de dados, tratando-o desde compreensão conceitual até vigência do texto normativo. Com isso, o trabalho analisou privacidade desde seus primeiros sinais de existência, inclusive adentrando sobre a perspectiva de outras nações sobre o que se entende a respeito do tema.

A pesquisa se propõe a discutir sobre o tema proteção de dados com viés o viés processual judicial. E, no contexto de que a tecnologia está cada vez mais sendo propulsora dos debates e transformações e influenciando todas as áreas da sociedade, designou-se a análise para a coleta, tratamento e armazenamento de dados nas audiências por videoconferência.

Assim, partiu-se de um ponto considerado comum a nível mundial sobre a abordagem de proteção de dados, estudando sobre a posição da Europa no cenário mundial. Dessa forma, buscou-se falar sobre o protagonismo da União Europeia e explicar o seu posicionamento perante outras nações. Isso porque, o GDPR tornou-se exemplo para elaboração outras normas sobre o direito de proteção de dados pessoais em outros países.

O primeiro capítulo examinou a dimensão do posicionamento da UE não só em matéria de proteção de dados, mas sobre a regulamentação em outras matérias. Isso demonstra a importância e influência que reflete em outros Estados, definindo-a como *Modelador de Normas* e sendo, assim, uma tendência no mundo.

Nessa realidade atual, é importante destacar que a extraterritorialidade que é tema central ao se tratar de tecnologia e sociedade. As relações internacionais têm um outro formato a partir do uso da internet. Para isso surgem as novas regulamentações e formas de condução das atividades a nível global.

De fato, a União Europeia tem liderado o espaço ao considerar como ponto fundamental a proteção dos dados pessoais dos seus cidadãos nas negociações internacionais. Nesse sentido, demonstra uma solidez no que diz respeito a compreensão sobre o direito fundamental de proteção de dados pessoais.

O olhar é direcionado para a dignidade da pessoa humana, antes de qualquer outra perspectiva. Nesse diapasão, faz parte das tratativas em que a Europa esteja envolvida que as transações de dados pessoais de seus cidadãos estejam em consonância com os preceitos do

regulamento europeu. Dessa forma, mantém a preservação do direito fundamental e o respeito à dignidade das pessoas.

Portanto, para construir o entendimento no trabalho de tese, no primeiro tópico do capítulo 1, conduziu-se a pesquisa para a análise sobre a elaboração *do General Data Regulation Protection* – GDPR, desde seu nascimento. Nesse sentido, foram debatidos os conceitos e entendimentos sobre privacidade da UE fazendo uma análise de outras perspectivas sobre o mesmo tema em outros Estados.

Isso porque se tornou importante demonstrar que há olhares diferentes para o mesmo tema. Como trabalhado, privacidade é utilizada sob perspectivas diferentes entre os EUA e Europa, por exemplo. Isso significa dizer que grandes discrepâncias sobre o conceito ou entendimento acerca do tema podem afetar as relações internacionais.

Nesse sentido, a União Europeia considera essencial que os dados pessoais de seus cidadãos estejam protegidos. De modo que, aqueles países, que não compreendam proteção de dados da mesma maneira que a EU, podem ter dificuldades no que diz respeito as tratativas internacionais.

Por conseguinte, corroborando com a construção do entendimento sobre o tema, o último tópico do primeiro capítulo abordou privacidade e publicidade. Demonstrando a importância de ambos e a necessidade do equilíbrio entre eles nos casos concretos.

Sobre privacidade, o trabalho buscou trazer o seu nascedouro e o seu significado. Depois explicou-se a sua relação com proteção de dados. Ficando compreendido que privacidade e proteção de dados não são a mesma coisa.

A proteção de dados está no conceito de privacidade. Esse último é bastante abrangente, podendo abranger outras searas da vida do indivíduo. Por exemplo, a vida privada, que não necessariamente tem a ver com dados pessoais.

O segundo capítulo buscou-se desenvolver uma análise sobre o arcabouço normativo do ponto de vista processual entre dois países: Itália e Brasil. O objetivo foi analisar as produções normativas posteriores a vigência dos regulamentos de proteção de dados para cada nação. Foi feita análise sobre as normas que envolvem o processo eletrônico de um modo geral, bem como uma pesquisa sobre a regulamentação de audiências remotas e adjacências.

Além disso, analisou-se como era o estado normativo dos países antes do surgimento das regulamentações. A Itália, como país membro da União Europeia, foi analisada antes da

vigência do regulamento, com o intuito de demonstrar o lado pioneiro sobre proteção de dados que essa nação apresenta sobre a matéria. Isso porque outros países já haviam sinalizado a preocupação sobre regras em matéria de proteção de dados, entretanto, a Itália foi a primeira que elaborou um Código de Proteção de Dados.

Dessa forma, foi significativo analisar as normas anteriores, bem como posteriores ao regulamento europeu. O direcionamento da análise foi em relação às regras sobre processo judicial. Especificamente sobre uso de tecnologia em processo com o propósito de buscar a regulamentação da audiência por videoconferência.

Como já explicado, a Itália tem sistema processual semelhante ao do Brasil, justificando o estudo sobre esse país. Além disso, o seu pioneirismo sobre proteção de dados foi outro fator que justificou o estudo sobre esse Estado. A existência do Código de proteção de dados antes do surgimento do regulamento europeu demonstra que houve interesse em regulamentar a matéria delimitada ao seu espaço.

A outra análise foi sobre o funcionamento brasileiro sobre o antes da LGPD e o após essa lei. Mais uma vez para demonstrar como o país visualizava o direito a proteção de dados antes de surgir uma norma específica e como se apresentou após a vigência da lei protetiva.

Dessa forma, analisou-se o Marco Civil da Internet, Código de Processo Civil, Constituição Federal, Código de Defesa do Consumidor e demais resoluções e orientações do Conselho Nacional de Justiça (incluindo os regulamentos do CNJ que foram elaborados após a LGPD).

A partir da análise dos dois ordenamentos jurídicos, no que diz respeito as regras processuais e uso de tecnologia, o terceiro capítulo trouxe dados empíricos. Examinou-se relatórios disponibilizados pelos portais institucionais dos tribunais e demais instituições fiscalizatórias e regulatórias do judiciário.

Isso porque, foi necessário compreender se o trabalho do judiciário está adequado às exigências da lei de proteção de dados de cada um dos países. Para isso, se fez necessário identificar a existência de relatórios de acompanhamento anual do judiciário, bem como projetos de aperfeiçoamento quanto aos novos desafios surgidos.

Além disso, foi enviado um questionário com perguntas relacionadas ao cotidiano da realização de audiência por videoconferência tanto para o Tribunal de Justiça do Estado de

Pernambuco, quanto para o *Tribunale di Pisa*. As perguntas foram elaboradas todas em consonância com as exigências legais.

O objetivo do questionário, como já explicado, não foi de trazer uma visão generalista e considerar que todos os tribunais trabalham da mesma forma. O propósito foi trazer, de forma exemplificativa, o que acontece no cotidiano desses tribunais para fomentar o debate e direcionar outras futuras pesquisas. Até o presente momento não houve resposta dos tribunais a que foram direcionados os questionários.

Por fim, o último tópico trouxe uma reflexão sobre a sociedade pós-moderna e as nuances tecnológicas e o novo modo de viver. Analisou que transformações e todos os desdobramentos estão presentes em todas as áreas da sociedade, assim como também estão no poder judiciário.

Entendeu-se assim, que a vulnerabilidade não pode ser mais compreendida como algo pontual e de responsabilidade apenas de determinada instituição, estado ou país. Compreende-se que na sociedade da informação e no ciberespaço não há mais uma separação específica.

A partir da disposição dos dados pessoais no espaço virtualizado, eles já estão em outra conjuntura que não é mais aquela dos arquivos físicos, em uma sala e trancados por uma chave física. Os desafios são outros, variados e transformados a todo instante. Dessa forma, o aperfeiçoamento da segurança digital em todos os âmbitos sociais se torna necessário.

O estudo desenvolvido nesse trabalho demonstra que o judiciário apresenta uma busca aprimoramento constante, ao passo que o avanço tecnológico acontece. Entretanto, precisa haver um trabalho mais incisivo diante do estágio em que se encontram. Isto é, o cotidiano do judiciário precisa estar mais próximo do idealizado pela regulamentação de proteção de dados.

Foram identificados e analisados relatórios de acesso público. Entretanto, as informações apenas trazem os tópicos que serviram de métrica para avaliação dos próprios tribunais ou dos órgãos fiscalizadores. Não demonstram maiores detalhes sobre a adequação à legislação pertinente no que diz respeito ao cotidiano das audiências remotas.

O planejamento apresentado pelo tribunal brasileiro para 2024 traz passo a passo a que se propõe concretizar para melhorar a prestação jurisdicional. A título de exemplo, estão previstos cursos sobre vários conteúdos de capacitação sobre matérias que envolvem a tecnologia.

Todavia, poderia ser contributivo a elaboração de manual de rotinas no judiciário que esteja associado e adequado às exigências legais. Como por exemplo, procedimentos que devem ser adotados para garantia de adequação à lei geral de proteção de dados nas varas judiciárias. Além disso, explicações precisam ser disponibilizadas com menos tecnicidade sobre proteção de dados para o público em geral, tornando as informações mais claras e compreensíveis para o jurisdicionado que não compreende os termos jurídicos.

Tais medidas podem vir a ser elaboradas em conjunto com a academia e a sociedade civil, além de equipe multidisciplinar, trazendo um conjunto de informações completo e que atenda às necessidades sociais. O envolvimento de universidades, estudantes, pesquisadores, professores e profissionais da área podem elaborar trabalhos com qualidade que auxiliem o judiciário e a população no desenvolvimento de projetos para adequação à legislação.

Além disso, considerando que as mídias das audiências ficam armazenadas nos arquivos digitais do tribunal, seria congruente um procedimento inicial explicativos para o público em geral sobre a coleta, tratamento e armazenamento dos dados pessoais. Tal medida pode ser realizada pelo assistente de audiência, pelo juiz ou alguém responsável por essa tarefa. Etapa essa que pode ser elaborada no planejamento acima proposto.

Nesse sentido, uma orientação, explicação sobre as coletas, o porquê que estão sendo realizadas, explicando o propósito desse ato e como serão armazenados os dados pessoais decorrentes das audiências remotas. Além do mais, se faz necessário dar informação a respeito da imagem gerada na audiência que ficará gravada no acervo do tribunal, assim como todas as demais informações.

Além disso, a reciclagem dos serventuários acerca do conhecimento sobre medidas de segurança, atualização legislativa e mudança de rotinas precisam ser constantes. Portanto, criação de treinamentos sobre os regulamentos e de medidas as serem adotadas na rotina judiciária.

É necessário que haja sempre o alerta, para aqueles que lidam com as informações, sobre os riscos e sobre a hipótese de vazamento de dados e a responsabilidade do tribunal sobre esse ocorrido. Como já dito, não existe segurança absoluta do ponto de vista tecnológico, as transformações e avanços são constantes e não existe uma ferramenta que possa garantir proteção plena. Entretanto o constante investimento com treinamentos e medidas adequadas podem minimizar os riscos.

A persistência dos ataques de ransomware é uma das principais tendências de ameaças para o cenário cibernético de 2024. Após um breve declínio em 2022, os ataques desse tipo tiveram um retorno exponencial em 2023, mostrando a adaptabilidade dos hackers maliciosos por trás dessas investidas digitais. A capacidade de sequestrar dados importantes e exigir resgates financeiros continua sendo uma estratégia lucrativa para cibercriminosos, desafiando as defesas digitais.

Para enfrentar essa persistência é importante ter uma constante atualização de backups, proporcionando uma linha de defesa contra a perda de dados. Além disso, investir em treinamentos para os colaboradores é essencial, pois a conscientização e preparação dos membros da equipe são armas poderosas na prevenção e resposta eficiente a ataques de ransomware. À medida que esses ataques evoluem, a adoção de uma postura proativa e a implementação de medidas de proteção são imprescindíveis para garantir a segurança e continuidade das operações empresariais²⁸⁵.

Os ransomware é um software malicioso, um malware. Suas ameaças são realizadas a partir de criptografia. Assim, o hacker coleta dados essenciais e os transforma em reféns para que possa obrigar a organização a pagar pelo retorno deles.

O ransomware é um tipo de software malicioso, uma espécie de malware, que emprega criptografia para ameaçar as organizações. Ou seja, o hacker utiliza essa tecnologia para criptografar os dados essenciais de um usuário ou de uma empresa e depois, exigem um resgate para liberar o acesso. Sendo assim, eles conseguem manter os dados confidenciais na posição de refém e obrigam as organizações a pagarem valores altos pelo retorno e segurança dos seus dados.

(...)Esse tipo de ataque tira proveito do fato que alguns setores não estão preparados para suportar a falta de determinado sistema. Alguns ataques de ransomware são capazes até de manter redes inteiras como reféns. Dessa forma, eles conseguem deixar as organizações “sem saída”. Elas podem escolher entre pagar pelo resgate ou tomar medidas para mitigar os danos e restaurar as operações. Mas, de qualquer forma, o custo é muito alto e os danos são significativos²⁸⁶.

Dentre as sugestões para proteger as informações estão: backups recorrentes, treinamento, autenticação de dois fatores, uso de redes seguras, programas e sistemas atualizados. Entende-se que quanto maior o nível de segurança, menor se torna a vulnerabilidade.

Ademais, importante frisar que os dados, ainda que coletados pelo judiciário, uma vez digitais, estão no ciberespaço. Isso quer dizer que o Judiciário não tem controle absoluto sobre o que acontece com as informações, mas tem responsabilidade sobre as medidas adotadas para evitar riscos futuros. Esse controle absoluto quer dizer que diante dos avanços tecnológicos, também avançam os artifícios de invasores cibernéticos.

²⁸⁵ CONTACTA SEGURANÇA DIGITAL. CYBER SECURITY. Tendência de segurança cibernética para 2024. Disponível em: <https://www.contacta.com.br/tendencias-de-seguranca-cibernetica-para-2024/#:~:text=Resili%C3%Aancia%20cibern%C3%A9tica:%20A%20resili%C3%Aancia%20cibern%C3%A9tica%20%C3%A9%20uma,garantem%20uma%20prote%C3%A7%C3%A3o%20absoluta%20contra%20amea%C3%A7as%20cibern%C3%A9ticas>. Acesso em: 30 jul 2024.

²⁸⁶ CONTACTA SEGURANÇA DIGITAL. Ransomware: como se prevenir contra esse ataque. Disponível em: https://www.contacta.com.br/ransomware-como-se-prevenir-contra-esse-ataque/?link_interno=post-26-12-23&ancora=ransomware. Acesso em 30 jul 2024.

Durante a pesquisa foi sinalizado que o banco de dados do judiciário brasileiro é bastante extenso, isso porque são inúmeros processos judicializados anualmente. Considerando a complexidade humana e o porte das cidades estudadas²⁸⁷. Isso torna a responsabilidade mais complexa. Além disso, o controle foge das questões geográficas, como já falado quando comentado sobre a extraterritorialidade.

Importante ressaltar, nesse contexto, que o Tribunal de Justiça do Estado de Pernambuco teve um percentual de 97,1% de casos novos eletrônicos, a partir do Relatório Justiça em Números 2023. Além disso, o percentual de processos do TJPE cresceu linearmente, de 89% passou para 98% (gráfico fig. 124 do relatório), como informa o referido relatório:

O percentual de processos que ingressa eletronicamente no Poder Judiciário tem crescido linearmente, em curva acentuada, desde 2012. Na série histórica apresentada na Figura 121, é possível constatar que a curva do primeiro grau está acima da do segundo grau em todo o Programa de transformação digital e atuação inovadora 177 período, havendo maior aproximação entre os indicadores em 2022 devido à grande evolução na virtualização dos processos de segundo grau. A avaliação detalhada por tribunal e instância está disposta na Figura 124²⁸⁸.

Dessa forma, os dados pessoais coletados em audiência por videoconferência não são apenas uma questão unicamente do judiciário. Trata-se de um desafio de todos os judiciários ou qualquer outro setor que tenha funcionamento no ciberespaço.

Isso quer dizer que esses dados pessoais decorrentes de processo estão a menos de 1 (um) segundo em qualquer local do mundo. Basta um computador, internet e acesso livre ou conhecimento cibernético e todos os dados podem estar sob a posse de pessoas erradas.

Essa reflexão traz à tona, portanto, o ideal de um debate global sobre proteção de dados. A pesquisa citou alguns autores que conversam sobre essa temática, trazendo o destaque para Aldeia Global de McLuhan. Polêmico porque trazia uma visão ideal com características impossíveis de concretização.

Entretanto, não se deve desconsiderar a proposta apresentada pelo autor acima. Talvez o pensamento de uma padronização global não seja alcançável. Mas o debate global na busca

²⁸⁷ BRASIL. Conselho Nacional de Justiça. Relatório Justiça em Números 2023. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2023/08/justica-em-numeros-2023.pdf>. Acesso em: 14 jun 2024. Importante observar que esse relatório informa a possibilidade de utilização de nuvem, inclusive provida por pessoa jurídica de direito privado. Além disso, explica a existência do CODEX, que é uma plataforma nacional que consolida bases de dados processuais, e, em agosto de 2023 já existiam 171 milhões de processos armazenados.

²⁸⁸ BRASIL. Conselho Nacional de Justiça. Relatório Justiça em Números 2023. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2023/08/justica-em-numeros-2023.pdf>. Acesso em: 14 jun 2024.

dos pontos convergentes parece ser uma possibilidade plausível, pois não há uma vida isolada em cada país.

Dessa forma, pode-se criar uma cultura global de proteção de dados e sua expansão naturalmente refletiria em cada setor da sociedade. Assim, há de ter um crescimento enquanto sociedade, aumentando o comprometimento com desenvolvimento e o respeito à dignidade da pessoa humana.

No que diz respeito a problemática da vulnerabilidade dos dados pessoais coletados nas audiências remotas, entende-se que esteja incluído nessa aldeia global. Em se tratando de medidas a serem adotadas por tribunais, se faz necessário a criação de barreiras de proteção. Como vem sendo debatido nessa pesquisa, a criação de senhas fortes (incluindo mudança periódica), constantes atualizações de sistemas e treinamento dos serventuários seriam medidas básicas a serem adotadas no cotidiano das audiências.

O contacta segurança digital traz as tendências de segurança digital para 2024. Dentre elas, cita a resiliência cibernética, que seria a continuidade das atividades e operações de forma eficaz mesmo após um ataque.

A resiliência cibernética é uma das principais tendências em segurança cibernética para 2024, destacando a crescente necessidade de preparação para recuperação pós-ataque. Reconhecendo que mesmo as medidas de segurança mais robustas não garantem uma proteção absoluta contra ameaças cibernéticas, a resiliência cibernética concentra-se na habilidade de uma organização em continuar suas operações de forma eficaz após uma violação.

Essa tendência reconhece que nenhum sistema de segurança é infalível, mesmo com os avanços tecnológicos. Em vez de focar exclusivamente na prevenção, a resiliência cibernética direciona seus esforços para a preparação e resposta eficaz após um incidente. As organizações estão começando a entender que é crucial não apenas se proteger contra ameaças, mas também garantir a capacidade de se recuperar rapidamente caso uma violação ocorra. Para fortalecer a resiliência cibernética, as empresas estão investindo em práticas proativas, como desenvolvimento de planos de resposta a incidentes, treinamento contínuo de pessoal, implementação de tecnologias de detecção avançada e a criação de estratégias de continuidade de negócios. Essa abordagem não apenas ajuda a limitar os danos causados por um ataque, mas também a garantir a continuidade das operações, mantendo a confiança dos clientes e parceiros²⁸⁹.

Além disso, o referido texto traz como ponto importante a segurança adaptável. Seria a capacidade de se ajustar às ameaças. Trata-se de uma resposta proativa que antecipa e neutraliza as ameaças.

²⁸⁹ CONTACTA SEGURANÇA DIGITAL. ZTNA: o que é zero Trust Network Access. Disponível em: https://www.contacta.com.br/conheca-sobre-o-modelo-de-seguranca-zero-trust-network-access/?link_interno=post-26-12-23&ancora=ztna. Acesso em: 30 jul 2024.

Outra sugestão é abordagem zero trust. Essa abordagem exige autenticação constantemente validada durante toda a sessão. Essa expressão se traduz na confiança zero. Por isso a necessidade de autenticação de identidade sendo executada de forma constante. Exige monitoramento e verificação sempre e nunca confiar. Seria monitoramento do comportamento dos usuários na movimentação de dados²⁹⁰.

Outro ponto ressaltado é o da governança de dados. Espera-se que em 2024 haja uma crescente conscientização sobre a administração dos dados. E nesse contexto, portanto, são os processos e práticas para garantir a segurança da informação.

A implementação eficaz dessa estratégia envolve a definição de políticas claras, a aplicação de controles de acesso rigorosos, a criptografia adequada e a monitoramento constante para identificar e responder rapidamente a qualquer ameaça potencial. Assim, a tendência da governança de dados reflete a necessidade de estabelecer práticas sólidas que garantam a segurança dos dados em um cenário cibernético dinâmico²⁹¹.

Desse modo, respondendo à pergunta de pesquisa objetivo do estudo: A Itália e o Brasil estão adequados às suas respectivas regulamentações sobre proteção de dados no que tange a realização de audiência por videoconferência? Pode-se afirmar que a partir da análise dos relatórios, das normas e, principalmente, das respostas aos questionários, a pesquisa demonstra que o TJPE e o *Tribunale di Pisa* ainda não estão totalmente adequados às suas respectivas legislações de proteção de dados no que tange à realização de audiências por videoconferência.

Embora o TJPE demonstre maior preocupação com a proteção de dados, com a existência de política específica, treinamentos e restrição de acesso aos dados, a ausência de um protocolo específico para videoconferências e a falta de clareza na comunicação com os titulares dos dados apontam para a necessidade de aprimoramento.

O *Tribunale di Pisa*, por sua vez, apresenta um cenário mais preocupante, com a falta de treinamento para os servidores, a ausência de medidas de segurança robustas para o armazenamento das gravações e a falta de transparência na comunicação com os titulares dos dados.

²⁹⁰ CONTACTA SEGURANÇA DIGITAL. ZTNA: o que é zero Trust Network Access. Disponível em: https://www.contacta.com.br/conheca-sobre-o-modelo-de-seguranca-zero-trust-network-access/?link_interno=post-26-12-23&ancora=ztna. Acesso em: 30 jul 2024.

²⁹¹ CONTACTA SEGURANÇA DIGITAL. Tendências de segurança Cibernética para 2024. Disponível em: <https://www.contacta.com.br/tendencias-de-seguranca-cibernetica-para-2024/#:~:text=Resili%C3%Aancia%20cibern%C3%A9tica:%20A%20resili%C3%Aancia%20cibern%C3%A9tica%20%C3%A9%20uma.garantem%20uma%20prote%C3%A7%C3%A3o%20absoluta%20contra%20amea%C3%A7as%20cibern%C3%A9ticas>. Acesso em: 30 jul 2024.

Portanto, a hipótese inicial de que ambos os países estejam adequados não se confirma, sendo necessária a elaboração e implementação de medidas mais eficazes para garantir a proteção dos dados pessoais em audiências por videoconferência. Além disso, manter o cumprimento dos princípios e regras contidas nos regulamentos, que podem ser atendidas aprimorando condutas, criação de protocolo padrão, acompanhamento pelos órgãos jurisdicionais através de relatórios (detalhados e que esclareçam tudo que esteja ligado a coleta de dados pessoais, proporcionando a melhoria), elaborando cartilhas informativas, entre outras.

Portanto, as medidas que precisam ser adotadas pelo poder judiciário são aquelas de acesso rigoroso, com criptografia e monitoramento constante das ações referentes aos dados coletados. Trata-se de práticas sólidas que venham trazer segurança dos dados no cenário cibernético, o que vem a incluir também o uso de inteligência artificial entre as ferramentas, considerando que esta também é utilizada nos ciberataques.

Referências

AIELLO, Giuseppe Francesco. La protezione dei dati personali dopo il trattato di Lisbona: natura e limiti di um diritto fondamentale <disomogeneo> alla luce della nuova proposta di General Data Protection Regulation. Disponível em: <https://www.rivisteweb.it/doi/10.4478/81757>. Acesso em 25 mar 2024.

ALMEIDA, Isaac Nogueira de; BARZOTTO, Luciane Cardoso. Proteção de dados nos tribunais brasileiros: os principais temas da LGPD. Disponível em: <https://publicar.claec.org/index.php/editora/catalog/download/68/68/754?inline=1>. Acesso em: 09 jun 2024.

ARAUJO, Marilene Pereira; DOS SANTOS, Maria Celeste Cordeiro Leite. O tempo e o espaço. Fragmentos do marco civil da internet: paradigmas de proteção da dignidade humana. **Revista Brasileira de Políticas Públicas**, v. 7, n. 3, p. 159-183, 2017.

ARNAUDO, Daniel. O Brasil e o Marco Civil da Internet. **Igarapé Institute**, 2017. Disponível em: https://d1wqtxts1xzle7.cloudfront.net/53233066/igarape_o-brasil-e-o-marco-civil-da-internet-libre.pdf?1495467259=&response-content-disposition=inline%3B+filename%3DO_Brasil_e_o_Marco_Civil_da_Internet_O_E.pdf&Expires=1729134079&Signature=Wobw5zOqxLqsTn8wXC1oIgOS0EkuRePmFqIJ~7xPIeqHIYWnglmeFZCH0y0aj7ikTPHcb0lBA8lU3krZ5lGzYmvER0yHoygbOIVKE0SnkQUl6OtJUIUofOY2jLxomEk1EgyhdJmqIIlDcbD-j2o4~8hHuQVnsAm-rIUUATUSaVP8UAsWCr4YLEaKlkaBRB4C9K7zo8US0QUx6-BJH6EypSD5rFEoPHa~Lm0MT4tf7os75UKXF3RyYuYueTk52gFKpTX9tci7iOhYHiCkCaEW9KT26hteEM5T3FBwtZYQgDbniIPnIGHsVp67H2dd7FkStnmNrx4OHUroa8tzLBWn6WA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA. Acesso em: 16 out 2024.

AWARI. Como garantir a segurança da informação e proteção de dados: dicas essenciais para proteger suas informações. 10 ago 2023. Disponível em: <https://awari.com.br/como-garantir-a-seguranca-da-informacao-e-protecao-de-dados-dicas-essenciais-para-proteger-suas-informacoes/>. Acesso em 24 jul 2024.

BALDONI, Roberto et al. Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici. 2018.

BARBOSA, Juliana Souza et al. A proteção de dados e segurança da informação na pandemia COVID-19: contexto nacional. **Research, Society and Development**, v. 10, n. 2, p. e40510212557-

e40510212557, 2021. Apud Coelho, F. E.S., Araújo, L. G. S. (2013). Gestão da Segurança da Informação NBR 27001 e 27002. Escola Superior de Redes.

BAUMAN, Zygmunt. Modernidade Líquida. Tradução Plínio Dentzien. 1ª ed. Rio de Janeiro: Zahar, 2021.

BENDIEK, Annegret; RÖMER, Magnus (2019): Externalizing Europe: the global effects of European data protection, Digital Policy, Regulation and Governance, ISSN 2398-5046, Emerald, Bingley, Vol. 21, Iss. 1, pp. 32-43, <https://doi.org/10.1108/DPRG-07-2018-0038>. Disponível em: <https://www.econstor.eu/bitstream/10419/210482/1/Full-text-article-Bendiek-et-al-Externalizing-Europe.pdf>. Acesso em: 15 mar 2024.

BERTI, Ricardo. ZURMELE, Franco. Giustizia digitale, gli aspetti privacy delle udienze da remoto: ecco le regole. Le udienze da remoto stanno permettendo alla Giustizia di proseguire la propria attività nonostante l'emergenza coronavirus. Tuttavia, come sottolineato dal Garante della privacy con una lettera al Ministero della Giustizia, non mancano fronti critici sul versante data protection. Pubblicato il 22 mag 2020. Disponível em: <https://www.agendadigitale.eu/documenti/giustizia-digitale/giustizia-digitale-gli-aspetti-privacy-delle-udienze-da-remoto-ecco-le-regole/>. Acesso em 17 maio 2024.

BIONI, Bruno Ricardo. RIELLI, Mariana. Data Privacy Brasil. Comissão Mista da Medida Provisória nº. 869, de 2018 Segunda Audiência Pública. Tema: Tratamento de dados pela Administração Pública e Proteção de Dados relativos à defesa e segurança pública. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento/download/01cdc9cc-4e64-4a40-a32b-cbad84777b05>, acesso em 14 mar 2024.

BONFANTI, Angelica. Big Data e polizia predittiva: riflessione in tema di protezione del diritto alla privacy e dei dati personali. Disponível em: <https://hdl.handle.net/2434/605891>. Acesso em: 31 mar 2024.

BRADFORD, Anu. The Brussels Effect, Northwestern University Law Review, Vol. 107, p. 1, 2012; Columbia Law & Economics Working Paper No. 533 (2012). Available at: https://scholarship.law.columbia.edu/faculty_scholarship/1966. Acesso em: 24 jun 2024.

BRASIL. Conselho Nacional de Justiça. Plataforma Emergencial de videoconferência para atos processuais. Disponível em: <https://www.cnj.jus.br/plataforma-videoconferencia-nacional/>. Acesso em: 29 abril 2024.

BRASIL. ANPD. Guia orientativo. Hipóteses legais de tratamento de dados pessoais. Legítimo interesse. Fev/2024. p. 15. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf. Acesso em 23 jul 2024.

BRASIL. Código de Defesa do Consumidor. Lei nº. 8.078 de 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm#:~:text=LEI%20N%C2%BA%208.078%2C%20DE%2011%20DE%20SETEMBRO%20DE%201990.&text=Disp%C3%B5e%20sobre%20a%20prate%C3%A7%C3%A3o%20do%20consumidor%20e%20d%C3%A1%20outras%20provid%C3%AAs.&text=Art.,da%20Constitui%C3%A7%C3%A3o%20Federal%20e%20art. Acesso em: 20 abril 2024.

BRASIL. Conselho Nacional de Justiça. Disponível em: <https://paineisanalytics.cnj.jus.br/single/?appid=a89ef492-f81e-4679-a58f-f7caa7452d82&sheet=740707b2-b87f-4ac0-a185-b430f855e682&lang=pt-BR&opt=cursel&select=clearall>. Acesso em 08 maio 2024.

BRASIL. Conselho Nacional de Justiça. Disponível em: <https://www.cnj.jus.br/sobre-o-cnj-3/>. Acesso em: 27 maio 2024.

BRASIL. Conselho Nacional de Justiça. iGovTIC-JUD – Resultado Geral. Disponível em: https://paineisanalytics.cnj.jus.br/single/?appid=36047c1e-acf8-4030-8474-78a20bae7c96&sheet=fb1b4d86-5d2f-4ac5-a4fd-345065ec8bd4&lang=pt-BR&theme=cnj_theme&opt=ctxmenu. Acesso em: 29 maio 2024.

BRASIL. Conselho Nacional de Justiça. Levantamento de Governança, Gestão e Infraestrutura de TIC do Poder Judiciário. iGovTIC-JUD 2023. Resultado Geral. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2023/10/relatorio-geral-do-igovtic-jud-2023-2023-09-27-v2.pdf>. Acesso em 29 maio 2024.

BRASIL. Conselho Nacional de Justiça. Recomendação nº. 73 de 20 de agosto de 2020. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3432>. Acesso em: 07 jun 2024.

BRASIL. Conselho Nacional de justiça. Recomendação orienta tribunais sobre proteção de dados. 27/08/2020. Agência de Notícias. Disponível em: <https://www.cnj.jus.br/recomendacao-orienta-tribunais-sobre-protecao-de-dados/>. Acesso em 07 jun 2024.

BRASIL. Conselho Nacional de Justiça. Relatório Justiça em Números 2023. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2023/08/justica-em-numeros-2023.pdf>. Acesso em: 14 jun 2024. Importante observar que esse relatório informa a possibilidade de utilização de nuvem, inclusive provida por pessoa jurídica de direito privado. Além disso, explica a existência do CODEX, que é uma plataforma nacional que consolida bases de dados processuais, e, em agosto de 2023 já existiam 171 milhões de processos armazenados.

BRASIL. Conselho Nacional de Justiça. Relatório Justiça em Números 2023. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2023/08/justica-em-numeros-2023.pdf>. Acesso em: 14 jun 2024.

BRASIL. Conselho Nacional de Justiça. Resolução nº. 372 de 12 fevereiro de 2021. Dispõe sobre Gestão da Informação e de Demandas Judiciais; Gestão e Organização Judiciária. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3742>. Acesso em 16 maio 2024.

BRASIL. Conselho Nacional de Justiça. Resultado do Questionário de TIC. Disponível em: <https://www.cnj.jus.br/tecnologia-da-informacao-e-comunicacao/comite-nacional-de-gestao-de-tecnologia-da-informacao-e-comunicacao-do-poder-judiciario/resultado-do-questionario-de-tic/>. Acesso em: 29 maio 2024.

BRASIL. Conselho Nacional de Justiça. Tratamento de dados pessoais na consulta de jurisprudência: desafios e perspectivas. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2022/02/tratamento-dados-pessoais-consulta-jurisprudencia30-11-21.pdf>. Acesso em: 29 maio 2024.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 abril 2024.

BRASIL. Decreto Lei nº 3.689 de 3 de outubro de 1941. Código de Processo Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 29 abril 2024.

BRASIL. Lei 10.406 de 10 de janeiro de 2002. Código Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm. Acesso em 23 abril 2024.

BRASIL. Lei 12.527 de 18 de novembro de 2011. Lei de Acesso à Informação. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm#:~:text=Regula%20o%20acesso%20a%20informa%C3%A7%C3%B5es,de%201991%3B%20e%20d%C3%A1%20outras. Acesso em 21 de abril de 2024.

BRASIL. Lei 13.105 de março de 2015. Código de Processo Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/113105.htm. Acesso em: 07 maio 2024.

BRASIL. Lei nº. 12.865 de abril de 2014. Marco Civil da Internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 21 abril 2024.

BRASIL. Lei nº. 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 30 abril 2024.

BRASIL. Portaria nº. 61 de 31 de março de 2020. Institui a plataforma emergencial de videoconferência para realização de audiências e sessões de julgamento nos órgãos do Poder Judiciário, no período de isolamento social, decorrente da pandemia do Covid-19. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3266>. Acesso em: 29 abril 2024.

BRASIL. Resolução 317 de abril de 2020 do Conselho Nacional de Justiça. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3302#:~:text=Disp%C3%B5e%20sobre%20a%20realiza%C3%A7%C3%A3o%20de,Coronav%C3%ADrus%2C%20e%20d%C3%A1%20outras%20provid%C3%A2ncias>. Acesso em: 30 abril 2024.

BRASIL. Resolução nº. 105 de 06 de abril de 2010 do Conselho Nacional de Justiça. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/166>. Acesso em: 30 abril 2024.

BRASIL. Resolução nº. 222 de maio de 2016 do Conselho Nacional de Justiça. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/atos-normativos?documento=2283>. Acesso em 30 abril 2024.

BRASIL. Resolução nº. 337 de 29 de setembro de 2020 do Conselho Nacional de Justiça. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3498>. Acesso em: 30 abril 2024.

BRASIL. Resolução nº. 345 de 9 de outubro de 2020 do Conselho Nacional de Justiça. Disponível em: <https://atos.cnj.jus.br/files/original175500202010145f873b7482503.pdf>. Acesso em: 8 maio 2024.

BRASIL. Resolução nº. 370 de 28/01/2021. Tecnologia da Informação E Comunicação; Gestão da Informação e de Demandas Judiciais; Gestão e Organização Judiciária. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3706>. Acesso em: 29 maio 2024.

BRASIL. Superior Tribunal de Justiça. **Direito ao esquecimento não justifica obrigação de excluir notícia de site, decide Terceira Turma.** Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/08032022-Direito-ao-esquecimento-nao-justifica-obrigacao-de-excluir-noticia-de-site--decide-Terceira-Turma.aspx#:~:text=Direito%20ao%20esquecimento%20incompat%C3%ADvel%20com%20a%20Constitui%C3%A7%C3%A3o&text=Todavia%2C%20a%20ministra%20observou%20que,o%20entendimento%20firmado%20pelo%20STJ..> Acesso em: 15 out 2024.

BRASIL. Tribunal de Justiça do Estado de Pernambuco. Plano de capacitação de TIC. Secretaria de tecnologia da informação e comunicação – SETIC. Disponível em: <https://portal.tje.jus.br/documents/d/transparencia/05-plano-de-capacitacao-2024-setic-pdf-1->. Acesso em 11 jun 2024

BRASIL. Tribunal de Justiça do Estado de Pernambuco. Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC. Disponível em: <https://portal.tje.jus.br/documents/d/transparencia/02-pdtic-2024-2026-1->. Acesso em: 11 jun 2024.

BRASIL. Tribunal de Justiça do Estado de Pernambuco. Portal da Transparência. Disponível em: <https://portal.tje.jus.br/web/transparencia/gestao/lei-geral-de-protecao-de-dados-lgpd/formulario>. Acesso em: 11 jun 2024.

CANNIZZARO, Enzo. Il diritto dell'integrazione europea: l'ordinamento dell'Unione. 2ª ed, Giappichelli, Torino 2017.

CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf, acesso em 02/03/2024.

CASTELLS, Manuel. A sociedade em rede. A era da informação: Economia, Sociedade e Cultura. Vol I, Ed. Paz & Terra. 2016. p. 90.

CASTRO, Aldo Aranha de. A busca pela efetividade do acesso à justiça por meio da tutela provisória no direito processual civil brasileiro e da tutela cautelar no sistema italiano. I Encontro Virtual do CNPEDI. Acesso à Justiça I. Coordenadores: Juvêncio Borges Silva e Luiz Fernando Bellinetti. Florianópolis, 2020. Disponível em: <http://site.conpedi.org.br/publicacoes/olpbq8u9/ag5bl345/6YJcO6R9Pr32Q7fz.pdf>. Acesso em 14 out 2024. p. 198-199.

CASTRO, Flavio; DELFIN, Cristiane. A internet não é a aldeia global de McLuhan. Professores reunidos em encontro de debates pelos 100 anos do filósofo canadense questionaram uso do termo criado por Marshall McLuhan para descrever a realidade atual. Disponível em: <https://www.unbcienca.unb.br/humanidades/48-comunicacao/212-a-internet-nao-e-a-aldeia-global-de-mcluhan-dizem-especialistas>. Acesso em: 08 jun 2024.

CATALETA, Anna. GDPR, um bilancio dei primi tre anni di applicazione: effetti, traguardi e prossimi step. Disponível em: <https://www.agendadigitale.eu/sicurezza/privacy/gdpr-un-bilancio-dei-primi-tre-anni-di-applicazione-effetti-traguardi-e-prossimi-step/>. 2021. Acesso em 16 mar 2024.

CISO Adviso. Ataque ao TSE desviou R\$ 1,2 mi a uma empresa terceirizada de TI. 29/04/2024. Disponível em: <https://www.cisoadvisor.com.br/ataque-ao-tse-desviou-r-12-mi-uma-empresa-terceirizada-de-ti/>. Acesso em: 18 jul 2024.

COMISSÃO EUROPEIA. Disponível em: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-commission_pt#:~:text=Tem%20a%20responsabilidade%20exclusiva%20de,e%20do%20Conselho%20da%20UE., acesso em 07/03/2024.

CONCILIO, Emanuela. Atti Giudiziare e tutela dei dati personali (nota a TAR Lazio, Sez. III, 1° febbraio 2021, n. 579. Disponível em: <https://www.giustiziainsieme.it/it/diritto-e-processo-amministrativo/1641-atti-giudiziari-e-tutela-dei-dati-personali-nota-a-tar-lazio-sez-iii-1-febbraio-2021-n-580>. Acesso em: 30 mar 2024.

CONTACTA SEGURANÇA DIGITAL. CYBER SECURITY. Tendência de segurança cibernética para 2024. Disponível em: <https://www.contacta.com.br/tendencias-de-seguranca-cibernetica-para-2024/#:~:text=Resili%C3%Aancia%20cibern%C3%A9tica:%20A%20resili%C3%Aancia%20cibern%C3%A9tica%20%C3%A9%20uma,garantem%20uma%20prote%C3%A7%C3%A3o%20absoluta%20contra%20amea%C3%A7as%20cibern%C3%A9ticas>. Acesso em: 30 jul 2024.

CONTACTA SEGURANÇA DIGITAL. Tendências de segurança Cibernética para 2024. Disponível em: <https://www.contacta.com.br/tendencias-de-seguranca-cibernetica-para-2024/#:~:text=Resili%C3%Aancia%20cibern%C3%A9tica:%20A%20resili%C3%Aancia%20cibern%C3%A9tica%20%C3%A9%20uma,garantem%20uma%20prote%C3%A7%C3%A3o%20absoluta%20contra%20amea%C3%A7as%20cibern%C3%A9ticas>. Acesso em: 30 jul 2024.

CONTACTA SEGURANÇA DIGITAL. ZTNA: o que é zero Trust Network Access. Disponível em: https://www.contacta.com.br/conheca-sobre-o-modelo-de-seguranca-zero-trust-network-access/?link_interno=post-26-12-23&ancora=ztna. Acesso em: 30 jul 2024.

CONTACTA SEGURANÇA DIGITAL. Ransomware: como se prevenir contra esse ataque. Disponível em: https://www.contacta.com.br/ransomware-como-se-prevenir-contra-esse-ataque/?link_interno=post-26-12-23&ancora=ransomware. Acesso em 30 jul 2024.

CONVENÇÃO 108/1981. Disponível em: <https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2>, acesso em 01/03/2024.

CONVENÇÃO 108+. Convenção para a proteção das pessoas relativamente ao tratamento de dados de carácter pessoal. Disponível em: <https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2#:~:text=A%20presente%20Conven%C3%A7%C3%A3o%20tem%20por,do%20direito%20%C3%A0%20vida%20privada>. Acesso em: 23 jun 2024.

GUIMARÃES, Glayder Daywerth Pereira et al. O princípio da publicidade dos atos processuais civis e o direito fundamental à proteção de dados pessoais: diretrizes para uma balize entre os direitos no Brasil. **Revista de Direito Magis**, v. 1, n. 2, 2022. Disponível em: <https://periodico.agej.com.br/index.php/revistamagis/article/view/17/15>. Acesso em: 17 out 2024.

COUNCIL OF EUROPE. Data Protection. Parties. Disponível em: <https://www.coe.int/en/web/data-protection/convention108/parties>. Acesso em 24 jun 2024.

DE MIRANDA, Wallace Vieira; ZAGANELLI, Juliana Costa. Marco civil da internet e política pública de transparência: uma análise da e-democracia e do compliance público. **Revista Brasileira de Políticas Públicas**, v. 7, n. 3, p. 633-646, 2017.

DE MORAIS, Jose Luis Bolzan et al. DEMOCRACIA, FLUXO DE DADOS E SOCIEDADE EM REDE: LIMITES DE PROTEÇÃO E CONTROLE ESTATAL A PARTIR DA LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA. **Revista Jurídica**, v. 3, n. 70, p. 770-791, 2022. Disponível em: <https://revista.unicritiba.edu.br/index.php/RevJur/article/view/2913/pdf>.

DE TARSO BRANDÃO, Paulo; BOUMANN, Gabrielle Amado. A INSERÇÃO DIGITAL DE QUALIDADE COMO DIREITO FUNDAMENTAL NA ERA DE HIPERCONECTIVIDADE: O DIREITO A ACESSAR DIREITOS. **Revista de Direito, Governança e Novas Tecnologias**, v. 7, n. 2, p. 91-112, 2021.

DECLARAÇÃO UNIVERSAL SOBRE OS DIREITOS DO HOMEM. Disponível em: <https://brasil.un.org/pt-br/91601-declara%C3%A7%C3%A3o-universal-dos-direitos-humanos>, acesso em 02/03/2024.

DECRETO LEGISLATIVO 30 giugno 2003, n. 196. Codice in materia di protezione dei dati personali. Disponível em: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2003-07-29&atto.codiceRedazionale=003G0218. Acesso em: 05 abril 2024.

DECRETO LEGISLATIVO, 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali. Disponível em: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2003-07-29&atto.codiceRedazionale=003G0218. Acesso em 19 abril 2024.

DOCUSIGN. Segurança da informação: conceito, função e como proteger dados sigilosos. 8 dez 2022. Disponível em: <https://www.docuSign.com/pt-br/blog/seguranca-da-informacao#:~:text=Tenha%20um%20plano%20de%20conting%C3%Aancia&text=Logo%2C%20essa%20estrat%C3%A9gia%20preventiva%20precisa,fique%20inativa%20por%20muito%20tempo..> Acesso em: 24 jul 2024.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico: Journal of Law**, v. 12, n. 2, p. 91-108, 2011.

DONEDA, Danilo. Da Privacidade à proteção de dados pessoais. Ed. Revista dos Tribunais. 3ª edição. Formato E-book. 2021.

DONEDA, Danilo. Um Código da Proteção de Dados Pessoais na Itália. Disponível em: <https://egov.ufsc.br/portal/sites/default/files/anexos/29727-29743-1-PB.pdf>. Acesso em 05 abril 2024.

DONEDA, Danilo. Um código para a proteção de dados pessoais na Itália. **Revista Trimestral de Direito Civil**, p. 117, 2003.

DUGNANI, Patricio. Globalização e desglobalização: outro dilema da Pós-Modernidade (Globalization and deglobalization: another dilemma of Post-Modernity). *Revista Famecos*, Porto Alegre, v. 25, n. 2, p. 1-14, maio, junho, julho e agosto de 2018: ID27918. DOI: <http://dx.doi.org/10.15448/1980-3729.2018.2.27918>. Acesso em: 08 jun 2024.

DUGNANI, Patrício. Meios de comunicação e Aldeia Global: globalização, desglobalização e interculturalidade. 2022. Disponível em: https://www.researchgate.net/profile/Patricio-Dugnani/publication/361680536_Meios_de_comunicacao_e_Aldeia_Global_Globalizacao_desglobalizacao_e_interculturalidade/links/62bf53290bf6950edea25713/Meios-de-comunicacao-e-Aldeia-Global-Globalizacao-desglobalizacao-e-interculturalidade.pdf. Acesso em 08 jun 2024.

EURONEWS. O que significa uma lei de vigilância dos EUA para a privacidade dos dados europeus. 01/06/2024. Disponível em: <https://pt.euronews.com/next/2024/06/01/o-que-significa-uma-lei-de-vigilancia-dos-eua-para-a-privacidade-dos-dados-europeus>. Acesso em: 23 jun 2024.

EUROPEAN CONVENTION ON HUMAN RIGHTS. Disponível em: <https://www.coe.int/en/web/human-rights-convention>, acesso em 02/03/2024.

EUROPEAN DATA PROTECTION SUPERVISOR. The History of The General Data Protection Regulation. Disponível em: https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en. Acesso em: 17 mar 2024.

EUROPIAN COMISSION. **COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Exchanging and Protecting Personal Data in a Globalised World**. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN>. Acesso em 28 mar 2024.

FACHINETTI, Aline Fuke. CAMARGO, Guilherme. Convenção 108 +: o tratado de proteção de dados e a relevância do tema para o Brasil. 04/07/2021. Disponível em: <https://www.conjur.com.br/2021-jul-04/opinio-convencao-108-relevancia-protecao-dados/>. Acesso em: 23 jun 2024.

FEDRECHESKI, Geovane. Entenda como a GDPR, a LGPD e NIST ajudam na proteção de dados pessoais. 05/07/2023. Disponível em: <https://www.alura.com.br/artigos/gdpr-lgpd-nist-ajudam-protecao-dados-pessoais>. Acesso em: 21 jun 2024.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. Privacidade e lei geral de proteção de dados pessoais. **Revista de Direito Brasileira**, v. 23, n. 9, p. 284-301, 2019. Disponível em: <https://indexlaw.org/index.php/rdb/article/view/5343/4545>. Acesso em: 17 out 2024.

FROSINI, Tommaso Edoardo et al. Il costituzionalismo nella società tecnologica. **Giurcost. org, Liber Amicorum per Pasquale Costanzo**, v. 25, 2020. Il Costituzionalismo nella società tecnologica. Disponível em: <https://dirittodiinternet.it/wp-content/uploads/2021/12/afro.pdf>. Acesso em 17 mar 2024.

GALLO, Veronica. MULA, Davide. USA, come sta cambiando l'approccio alla privacy: la grande svolta. 2021. Disponível em: <https://www.agendadigitale.eu/sicurezza/privacy/dal-diritto-alla-solitudine-alla-protezione-dei-dati-come-cambia-lapproccio-alla-privacy-negli-usa/>. Acesso em: 16 mar 2024.

GREENLEAF, Graham. Global Data Privacy Laws 2023: International standards stall, but UK disrupts. 2023. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4530145, acesso em 14 mar 2024.

GODINHO, Adriano Marteleto; NETO, Genésio Rodrigues Queiroga; TOLÊDO, Rita Cássia Moraes. A responsabilidade civil pela violação a dados pessoais. **Revista IBERC**, v. 3, n. 1, 2020. Disponível em: <https://revistaiberc.responsabilidadecivil.org/iberc/article/view/105/78>. Acesso em: 17 out 2024.

HALL, Stuart. A identidade cultural na pós-modernidade. tradução Tomaz Tadeu da Silva, Guaracira Lopes Louro-11. ed. -Rio de Janeiro: DP&A, 2006. Disponível em: https://leiaarqueologia.wordpress.com/wp-content/uploads/2018/02/kupdf-com_identidade-cultural-na-pos-modernidade-stuart-hallpdf.pdf. Acesso em: 08 jun 2024.

HAN, Byung-Chul. Sociedade da transparência. Trad. Lucas Machado. Petrópolis, RJ: Vozes, 2017.

ITÁLIA. Consiglio Nazionale Forense. Presso il Ministero della Giustizia. Proposta di Protocollo per udienze civili tramite collegamento da remoto – art. 83 lett. f, D.L. 18/2020. Disponível em:

<https://www.consiglionazionaleforense.it/documents/20182/677549/Protocollo+per+udienze+civili.pdf/56847321-9706-4347-a14b-2c9bcee3a089>. Accesso em: 15 jun 2024.

ITÁLIA. Consiglio Superiore della Magistratura. Disponível em: <https://www.csm.it/web/csm-internet/csm/attribuzioni-e-funzionamento>. Accesso em: 28 maio 2024.

ITÁLIA. Consiglio Superiore della Magistratura. Disponível em: <https://www.csm.it/web/csm-internet/csm/attribuzioni-e-funzionamento>. Accesso em: 28 maio 2024.

ITÁLIA. Decreto 21 febbraio 2011, n°. 44. Regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale, delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2, del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010 n. 24. (11G0087) (GU Serie Generale n.89 del 18-04-2011). Disponível em: <https://www.gazzettaufficiale.it/eli/id/2011/04/18/011G0087/sg>. Accesso em: 28 maio 2024.

ITÁLIA. Decreto Legge 28 ottobre 2020, n°. 137. Ulteriori misure urgenti in materia di tutela della salute, sostegno ai lavoratori e alle imprese, giustizia e sicurezza, connesse all'emergenza epidemiologica da Covid-19. (20G00166) (GU Serie Generale n.269 del 28-10-2020). Disponível em: <https://www.gazzettaufficiale.it/eli/id/2020/10/28/20G00166/sg>. Accesso em: 15 maio 2024.

ITÁLIA. Decreto Legislativo 10 agosto 2018, n. 101. Disponível em: <https://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg>. Accesso em 25 abril 2024.

ITÁLIA. Decreto Legislativo de 18 maggio 2018, n° 51. Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio. (18G00080) (GU Serie Generale n.119 del 24-05-2018). Disponível em: <https://www.gazzettaufficiale.it/eli/id/2018/05/24/18G00080/sg>. Accesso em 15 maio 2024.

ITÁLIA. Decreto Legislativo de 30 de giugno 2003, n. 196. Codice in Materia di Protezione dei Dati Personali. Disponível em: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2003-07-29&atto.codiceRedazionale=003G0218. Accesso em 25 mar 2024.

ITÁLIA. Decreto-Legge 17 marzo 2020, n°. 18. Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19. (20G00034). Disponível em: https://www.gazzettaufficiale.it/atto/stampa/serie_generale/originario. Accesso em: 15 maio 2024.

ITÁLIA. La Costituzione della Repubblica Italiana. Disponível em: https://www.cortecostituzionale.it/documenti/download/pdf/Costituzione_della_Repubblica_italiana.pdf. Accesso em 25 abril 2024.

ITÁLIA. Ministero della Giustizia. Circolare 31 maggio 2019 - Regolamento generale sulla protezione dei dati (regolamento ue 2016/679) - valutazione d'impatto sulla protezione dei dati (cd. dpia) - istruzioni operative e modulistica. Disponível em: https://www.giustizia.it/giustizia/it/mg_1_8_1.page?contentid=sdc194013&previouspage=mg_1_8. Accesso em: 28 maio 2024.

ITÁLIA. Ministero della Giustizia. Protezione dei dati personali. Disponível em: <https://www.giustizia.it/giustizia/page/it/privacy>. Accesso em: 14 jun 2024.

ITÁLIA. DECRETO DEL PRESIDENTE DELLA REPUBBLICA 13 febbraio 2001, n. 123. Regolamento recante disciplina sull'uso di strumenti informatici e telematici nel processo civile, nel processo amministrativo e nel processo dinanzi alle sezioni giurisdizionali della Corte dei Conti. Disponível em: <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:presidente.repubblica:decreto:2001-02-13;123!vig>. Accesso em: 17 out 2024.

ITÁLIA. Portale dei Servizi Telematici del Ministero della Giustizia. Disponível em: https://pst.giustizia.it/PST/resources/cms/documents/SPECIFICHE_TECNICHE_DM_44_2011REV_04.01.24.pdf. Acesso em: 17 maio 2024.

ITÁLIA. Portale dei Servizi Telematici del Ministero della Giustizia. Disponível em: https://pst.giustizia.it/PST/resources/cms/documents/20231213DGSIATribunaleOnline_SpecificheTecniche_signed.pdf. Acesso em: 17 maio 2024.

ITÁLIA. Portale dei Servizi Telematici del Ministero della Giustizia. Disponível em: https://pst.giustizia.it/PST/resources/cms/documents/m_dg.DOG07.09122023.0007511.ID_Regole_Tecniche_Udienze_da_remoto_signed.pdf. Acesso em: 17 maio 2024.

ITÁLIA. Provvedimento. REGOLE TECNICHE ED OPERATIVE IN MATERIA DI SVOLGIMENTO DELLE UDIENZE IN VIDEOCONFERENZA E FIRMA DIGITALE DEI PROVVEDIMENTI DEL GIUDICE NEI GIUDIZI DINANZI ALLA CORTE DEI CONTI. Disponível em: <https://www.corteconti.it/Download?id=ae08f022-9d8d-4782-b521-61fd0f262749>. Acesso em: 17 maio 2024.

Legge n. 675 del 31 dicembre 1996 – Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. Disponível em: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/28335>. Acesso em 05 abril 2024.

Lei de Inteligência Artificial da União Europeia entra em vigor. Publicado em 06 de agosto de 2024. Disponível em: <https://www.tozzinifreire.com.br/boletins/lei-de-inteligencia-artificial-da-uniao-europeia-entra-em-vigor>. Acesso em: 15 out 2024.

LÉVY, Pierre. Cíbercultura. Tradução Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

LÉVY, Pierre. O que é virtual? Tradução de Paulo Nevez. São Paulo: Editora 34, 2ª edição, 2017.

LGPD/DF. Disponível em: <https://lgpd.df.gov.br/historico/>. Acesso em 16 mar 2024.

LIMA, Caio Cesar Carvalho; MONTEIRO, Renato Leite. Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada. **AtoZ: novas práticas em informação e conhecimento**, v. 2, n. 1, p. 60-76, 2013.

MAGRANI, Eduardo. *Democracia conectada: a internet como ferramenta de engajamento político – democrático*. Curitiba: Juruá, 2014. p.165

MAGRANI, Eduardo. Ética e privacidade na era da hiperconectividade. Rio de Janeiro: Konrad Adenauer Stiftung, 2018. P. 15-16. Apud DE TARSO BRANDÃO, Paulo; BOUMANN, Gabrielle Amado. A INSERÇÃO DIGITAL DE QUALIDADE COMO DIREITO FUNDAMENTAL NA ERA DE HIPERCONECTIVIDADE: O DIREITO A ACESSAR DIREITOS. **Revista de Direito, Governança e Novas Tecnologias**, v. 7, n. 2, p. 91-112, 2021.

MAGRINI, Eduardo. Entre dados e robôs: ética e privacidade na era da hiperconectividade / Eduardo Magrani. — 2. ed. — Porto Alegre: Arquipélago Editorial, 2019.

MARTINES, Francesca. Conteúdo abordado em sala de aula em 26 mar 2024. Università di Pisa, Itália.

MARTORANA, Marco. Giustizia digitale e data protection, ecco gli impatti privacy dei processi da remoto. pubblicato il 3 giu 2020. Disponível em: <https://www.agendadigitale.eu/documenti/giustizia-digitale/giustizia-digitale-e-data-protection-ecco-gli-impatti-privacy-dei-processi-da-remoto/>. Acesso em: 17 maio 2024.

MASCHII, Andrea. New Rules on Italian Civil Proceedings: A step forward in improving the italian court system. Disponível em: <https://portolano.it/en/newsletter/litigation-arbitration/new-rules-on-italian-civil-proceedings-a-step-forward-in-improving-the-italian-court-system> Acesso em 16 maio 2024.

MCLUHAN, Marshall. Os meios de comunicação como extensões do homem. Tradução Décio Pignatari. Ed. Cultrix. São Paulo. Disponível em: https://edisciplinas.usp.br/pluginfile.php/352425/mod_resource/content/1/MCLUHAN%2C%20Marshall%20-%20Os%20Meios%20de%20Comunicac%CC%A7a%CC%83o%20como%20Extenso%CC%83es%20do%20Homem.pdf. Acesso em 08 jun 2024.

MENSI, Maurizio. Caratteristiche e criticità della comunicazione da remoto in tema di giustizia. 23 de setembro de 2020. Disponível em: <https://www.amministrazioneincammino.luiss.it/wp-content/uploads/2020/09/MENSI.pdf>. Acesso em: 09 jun 2024.

MERLA, Lara. Droni, privacy e tutela dei dati personali. **Informatica e diritto**, v. 25, n. 1, p. 29-45, 2016. Disponível em: http://www.ittig.cnr.it/EditoriaServizi/AttivitaEditoriale/InformaticaEDiritto/IeD_2016_01_Merla.pdf. Acesso em 07 abril 2024.

MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. **RJLB, Ano**, v. 5, p. 781-809, 2019.

MONT'ALVERNE, Tarin Cristino Frota; LIMA, Maria Cecília Girão Veras. The European Union as a Norm Shaper on Biodiversity Protection. **Veredas do Direito**, v. 20, p. e202569, 2023.

MOTA, Fabrício. Proteção de dados é a evolução de privacidade. Disponível em: <https://www.serpro.gov.br/lcpd/noticias/protacao-dados-evolucao-privacidade>. Acesso em 17 mar 2024. ONU Brasil. Rede Brasil do Pacto Global quer mais empresas alinhadas aos objetivos globais. Disponível em: <https://brasil.un.org/pt-br/83698-rede-brasil-do-pacto-global-quer-mais-empresas-alinhadas-aos-objetivos-globais>. Acesso em: 30 mar 2024.

ONU. Organização das Nações Unidas. ONU adota por consenso resolução para reger a inteligência artificial. Disponível em: <https://news.un.org/pt/story/2024/03/1829446>. Acesso em: 14 jun 2024.

OSERVATORIO CYBERSECURITY & DATA PROTECTION. **GDPR e Privacy, cos'è e come cambia per il trattamento e la protezione dei dati. La protezione dei dati, prima e dopo l'introduzione del General Data Protection Regulation**. Disponível em: <https://blog.osservatori.net/gdpr-privacy-protezione-dati-personali>. Acesso em: 23 abril 2024.

PAGLIA, Ricardo. TALENTI, Alfredo. Riforma del processo civile, la nuova disciplina dell'udienza cartolare. 10 febbraio 2023. Disponível em: <https://nplusrdiritto.ilsole24ore.com/art/riforma-processo-civile-nuova-disciplina-udienza-cartolare-AECtykC>. Acesso em: 17 maio 2024.

PIMENTEL, Alexandre Freire. Tratado de direito e Processo Tecnológico. Vol. II. Big Data, Justiça 4.0 e a digitalização da processualização, ciberespaço, metaverso, legal design e visual Law: o Direito Processual Tecnológico. Ed. Publius. Recife, 2023. p. 191.

PINHEIRO, Patrícia Peck. Proteção de dados pessoais. Comentários à Lei n. 13.709/2018. 4ª ed. Saraiva, 2023, p. 6.

PIZZETTI, Franco. Privacy. Condice privacy italiano dopo il Gdpr: come leggerlo e applicarlo ex decreto 101/2018. 14 set 2018. Disponível em: <https://www.agendadigitale.eu/sicurezza/privacy/gdpr-pizzetti-i-consigli-per-leggere-e-applicare-bene-il-decreto-101-2018-dal-19-settembre/>. Acesso em: 25 abril 2024.

PIZZETTI, Franco. Privacy. Condice privacy italiano dopo il Gdpr: come leggerlo e applicarlo ex decreto 101/2018. 14 set 2018. Disponível em: <https://www.agendadigitale.eu/sicurezza/privacy/gdpr-pizzetti-i-consigli-per-leggere-e-applicare-bene-il-decreto-101-2018-dal-19-settembre/>. Acesso em: 25 abril 2024.

REIS, Lucas. Regulamentação Europeia sobre Inteligência Artificial: o que uma liderança de marketing precisa saber. A versão final da regulamentação possui 272 páginas e ele influenciará a atuação da maior parte das companhias do mundo. Disponível em: <https://www.meioemensagem.com.br/proxima/regulamentacao-europeia-sobre-inteligencia-artificial-o-que-uma-lideranca-de-marketing-precisa-saber>. Acesso em 01 abril 2024.

RODOTÀ, Stefano. Riservatezza. 10ª edição. Treccani, 2023, p. 69-70.

RODOTÀ, Stefano. *Tecnologie e diritti*, Bologna, Il Mulino, 2021(ed. digit.: 2021, doi: 10.978.8815/367778, Capitolo primo: La privacy tra individuo e collettività, pp. 23-41, doi capitolo: 10.1401/9788815367778/c1). Disponível em: <https://www.darwinbooks.it/doi/10.978.8815/367778/page/28>. Acervo Biblioteca UNIPI. Acesso em: 26 mar 2024

RUGANI, Gabriele. I FLUSSI DI DATI PERSONALI DALL'UE VERSO PAESI TERZI, TRA ESPANSIONE DEL COMMERCIO E PERSONAL DATA PROTECTION. 2022. Tese de Doutorado. 2022.

SALDANHA, Paloma Mendes. **PRIVACIDADE E VIGILÂNCIA: A COVID-19 COMO JUSTIFICATIVA E A SOCIEDADE COMO FRUTO DA COLHEITA DIGITAL**. In book: Pensar a PANDEMIA: perspectivas críticas para o enfrentamento da crise (pp.430-444). Publisher: Tirant Lo Blanch. Disponível em: https://www.researchgate.net/publication/370099717_PRIVACIDADE_E_VIGILANCIA_A_COVID-19_COMO_JUSTIFICATIVA_E_A_SOCIEDADE_COMO_FRUTO_DA_COLHEITA_DIGITAL. Acesso em: 16 jun 2024P. 429.

SALDANHA, Paloma Mendes. **PRIVACIDADE E VIGILÂNCIA: A COVID-19 COMO JUSTIFICATIVA E A SOCIEDADE COMO FRUTO DA COLHEITA DIGITAL**. In book: Pensar a PANDEMIA: perspectivas críticas para o enfrentamento da crise (pp.430-444). Publisher: Tirant Lo Blanch. Disponível em: https://www.researchgate.net/publication/370099717_PRIVACIDADE_E_VIGILANCIA_A_COVID-19_COMO_JUSTIFICATIVA_E_A_SOCIEDADE_COMO_FRUTO_DA_COLHEITA_DIGITAL. Acesso em: 16 jun 2024.

SECURITY REPORT. Tribunal de Justiça do Pará sofre ataque cibernético. Disponível em: <https://securityleaders.com.br/tribunal-de-justica-do-para-sofre-ataque-cibernetico/>. Acesso em 14 jun 2024.

SILVA, Carlos Alberto. O elo mais fraco da segurança da informação. Pessoas representam o maior desafio. Oliveira MG, 2015. Livro digital. P. 92-93.

SILVA, Rennan Gonçalves; DA SILVA, Lucas Gonçalves; DE OLIVEIRA SILVA, Karen Thaiany Puresa. Impacto da LGPD na legitimação dos atos judiciais sob o prisma do princípio da publicidade. **Revista Direito & Paz**, v. 1, n. 46, p. 234-248, 2022. Disponível em: <https://revista.unisal.br/lo/index.php/direitoepaz/article/view/1651/657>. Acesso em: 17 out 2024.

SORO, Antonello. Là libertà e il suo limite. Una riflessione sul diritto alla privacy a partire dalla sentenza Roe v. Wade. Disponível em: <https://www.giustiziainsieme.it/it/diritto-e-innovazione/2396-la-liberta-e-il-suo-limite-una-riflessione-sul-diritto-alla-privacy-a-partire-dalla-sentenza-roe-v-wade>. Acesso em: 30 mar 2024.

SPAGNOLO, Antonio G. Il Regolamento Europeu sulla protezione dei dati personale: implicazioni pela ricerca scientifica. *Medicina e Morale*, 2018, Vol.67 (2), p.151-157. Disponível em: <https://web.p.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=0&sid=db0cf330-f25f-486d-b286-7a6475feec75%40redis>. Acervo da Biblioteca da UNIPI. Acesso em 25 mar 2024.

STORELLI, Filomena Marianna. Processo Telematico e da Remoto: l'udienza è smart. 04/05/2020. In *IusItinere Revista Giuridica*. Disponível em: <https://www.iusinitinere.it/processo-telematico-e-da-remoto-ludienza-e-smart-27530>. Acesso em: 15 jun 2024.

STORELLI, Filomena Marianna. Processo Telematico e da Remoto: l'udienza è smart. 04/05/2020. In *IusItinere Revista Giuridica*. Disponível em: <https://www.iusinitinere.it/processo-telematico-e-da-remoto-ludienza-e-smart-27530>. Acesso em: 15 jun 2024.

TECNOBLOG. STJ sofre ataque hacker e suspende atividades por uma semana. Disponível em: <https://tecnoblog.net/noticias/stj-sofre-ataque-hacker-e-suspende-atividades-por-uma-semana/>. Acesso em: 18 jul 2024.

TIGRINO, Andrea. Procedimento Penale e diffusione dei dati personali. Stato dell'arte e quesiti posti dalla riforma Cartabia. Rivista di Diritto dei Media. Disponível em: <https://www.medialaws.eu/rivista/procedimento-penale-e-diffusione-dei-dati-personali-stato-dellarte-e-quesiti-posti-dalla-riforma-cartabia/>. Acesso em 01 mar 2024.

TRATADO DE LISBOA. Disponível em: <https://www.parlamento.pt/europa/Paginas/TratadodeLisboa.aspx>, acesso em 02/03/2024.

TRATADO SOBRE O FUNCIONAMENTO DA UNIÃO EUROPEIA. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF, acesso em 02/03/2024.

UFRN. Evolução Histórica da Proteção de Dados e o Direito à Privacidade. Disponível em: <https://obdi.ccsa.ufrn.br/2020/09/24/evolucao-historica-da-protecao-de-dados-e-o-direito-a-privacidade/>. Acesso em: 05 abril 2024.

UNIÃO EUROPEIA. Acesso à informação. Disponível em: https://european-union.europa.eu/principles-countries-history/principles-and-values/access-information_pt. Acesso em: 08 jul 2024.

UNIÃO EUROPEIA. Carta de Direitos Fundamentais. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 06 jul 2024.

UNIÃO EUROPEIA. Carta dos Direitos Fundamentais da União Europeia. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em 23 mar 2024.

UNIÃO EUROPEIA. Convenzione del Consiglio d'Europa sulla Accesso ai documenti ufficiali (STCE no. 205). Trata-se de instrumento jurídico internacional vinculante que reconhece o direito geral de acesso a documentos públicos. Disponível em: <https://www.coe.int/it/web/conventions/full-list?module=treaty-detail&treaty-num=205>.

UNIÃO EUROPEIA. Convenzione Europea dei Diritti dell'Uomo. Disponível em: https://presidenza.governo.it/CONTENZIOSO/contenzioso_europeo/documentazione/Convention_ITA.pdf. Acesso em: 25 abril 2024.

UNIÃO EUROPEIA. Council of Europe. Department for the Execution of judgments of the European Court of Human Rights. DG1. Thematic Factsheet. September 2022. Disponível em: <https://rm.coe.int/tfs-personal-data-protection-eng/1680a811ea>. Acesso em: 08 jul 2024.

UNIÃO EUROPEIA. Council of Europe. Convenção 108+. Disponível em: <https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2>. Acesso em: 06 jul 2024.

UNIÃO EUROPEIA. Departamento temático dos Direitos dos Cidadãos e dos Assuntos Constitucionais do Parlamento Europeu. Proteção de dados pessoais. Disponível em: <https://www.europarl.europa.eu/factsheets/pt/sheet/157/protecao-dos-dados-pessoais>. Acesso em 22 mar 2024.

UNIÃO EUROPEIA. **Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche).** Disponível em: <https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A32002L0058>. Acesso em: 06 jul 2024.

UNIÃO EUROPEIA. Diretiva 95/46/EC do Parlamento Europeu e Conselho, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>. Acesso em 28 mar 2024.

UNIÃO EUROPEIA. Este regulamento constitui uma medida essencial para reforçar os direitos fundamentais das pessoas na era digital e facilitar a atividade comercial, mediante a clarificação das normas aplicáveis às empresas e aos organismos públicos no mercado único digital. Proteção de Dados na UE. Disponível em: [https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_pt#:~:text=Regulamento%20\(UE\)%202016%2F679,23%20de%20maio%20de%202018](https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_pt#:~:text=Regulamento%20(UE)%202016%2F679,23%20de%20maio%20de%202018). Acesso em: 22 mar 2024.

UNIÃO EUROPEIA. European Commission. The 2023 EU Justice Scoreboard. Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions COM(2023) 309. Disponível em: https://commission.europa.eu/document/download/db44e228-db4e-43f5-99ce-17ca3f2f2933_en?filename=Justice%20Scoreboard%202023_0.pdf&prefLang=it. Acesso em 10 jun 2024.

UNIÃO EUROPEIA. European Commission. The 2023 EU Justice Scoreboard. Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions COM(2023) 309. Disponível em: https://commission.europa.eu/document/download/db44e228-db4e-43f5-99ce-17ca3f2f2933_en?filename=Justice%20Scoreboard%202023_0.pdf&prefLang=it. Acesso em 10 jun 2024.

UNIÃO EUROPEIA. European Commission. The 2023 EU Justice Scoreboard. Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions COM(2023) 309. Disponível em: https://commission.europa.eu/document/download/db44e228-db4e-43f5-99ce-17ca3f2f2933_en?filename=Justice%20Scoreboard%202023_0.pdf&prefLang=it. Acesso em 11 jun 2024.

UNIÃO EUROPEIA. European Commission. The 2023 EU Justice Scoreboard. Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions COM(2023) 309. Disponível em: https://commission.europa.eu/document/download/db44e228-db4e-43f5-99ce-17ca3f2f2933_en?filename=Justice%20Scoreboard%202023_0.pdf&prefLang=it. Acesso em 11 jun 2024.

UNIÃO EUROPEIA. European Commission. The 2023 EU Justice Scoreboard. Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions COM(2023) 309. Disponível em: https://commission.europa.eu/document/download/db44e228-db4e-43f5-99ce-17ca3f2f2933_en?filename=Justice%20Scoreboard%202023_0.pdf&prefLang=it. Acesso em 11 jun 2024.

UNIÃO EUROPEIA. European Commission. The 2023 EU Justice Scoreboard. Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions COM(2023) 309. Disponível em: https://commission.europa.eu/document/download/db44e228-db4e-43f5-99ce-17ca3f2f2933_en?filename=Justice%20Scoreboard%202023_0.pdf&prefLang=it. Acesso em 11 jun 2024.

UNIÃO EUROPEIA. European Commission. The 2023 EU Justice Scoreboard. Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions COM(2023) 309. Disponível em: https://commission.europa.eu/document/download/db44e228-db4e-43f5-99ce-17ca3f2f2933_en?filename=Justice%20Scoreboard%202023_0.pdf&prefLang=it. Acesso em 11 jun 2024.

UNIÃO EUROPEIA. EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE (CEPEJ). Toolkit for supporting the implementation of the Guidelines on how to drive change towards Cyberjustice.

UNIÃO EUROPEIA. EUROPEAN DATA PROTECTION SUPERVISOR. DATA PROTECTION. Disponível em: [HTTPS://WWW.EDPS.EUROPA.EU/DATA-PROTECTION/DATA-PROTECTION_EN](https://www.edps.europa.eu/data-protection/data-protection_en). Acesso em: 21 JUN 2024.

UNIÃO EUROPEIA. European Ombudsman. Acesso Público aos documentos do Provedor de Justiça Europeu. 16/11/2020. Disponível em: <https://www.ombudsman.europa.eu/en/office/publicregister/pt>. Acesso em: 08 jul 2024.

UNIÃO EUROPEIA. General Data Protection Regulation. Art. 45. Disponível em: **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE)**. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679>. Acesso em: 20 jun 2024.

UNIÃO EUROPEIA. Parlamento Europeu. Proteção de dados. Disponível em: https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf. Acesso em: 06 jul 2024.

UNIÃO EUROPEIA. Proteção de dados e respeito a vida privada são Direitos fundamentais. Presente no texto sobre Proteção de dados da União Europeia. Proteção de dados pessoais. Disponível em: <https://www.europarl.europa.eu/factsheets/pt/sheet/157/ptecao-dos-dados-pessoais>. Acesso em 30 mar 2024.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE)**. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>. Acesso em: 21 jun 2024.

UNIÃO EUROPEIA. Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho relativo a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32018R1725>. Acesso em: 23 mar 2024.

UNIÃO EUROPEIA. Regulamento Inteligência Artificial: Parlamento aprova legislação histórica. Disponível em: <https://www.europarl.europa.eu/news/pt/press-room/20240308IPR19015/regulamento-inteligencia-artificial-parlamento-aprova-legislacao-historica>. Acesso em: 01 abril 2024.

UNIÃO EUROPEIA. Tratado de Nice. EUR-Lex. Access to European Union Law. Tratado de Nice. Síntese do Tratado de Nice. Disponível em: <https://eur-lex.europa.eu/PT/legal-content/summary/treaty-of-nice.html>. Acesso em: 21 jun 2024.

UNIÃO EUROPEIA. **Tratado que institui a Comunidade Europeia (Versão consolidada 2002)**. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:12002E/TXT>. Acesso em 21 jun 2024.

UNITED NATIONS. Universal Declaration of Human Rights. Disponível em: <https://www.un.org/en/about-us/universal-declaration-of-human-rights>. Acesso em: 21 jun 2024.

VOGLER, John; STEPHAN, Hannes R. The European Union in global environmental governance: leadership in the making?. International Environmental Agreements: Politics, Law and Economics, [Utrecht, The Netherlands], v. 7, n. 4, p. 389-413, 2007, APUD LIMA, Maria Cecília Girão Veras; MATIAS, João Luís Nogueira. Os efeitos extraterritoriais do regulamento antidesmatamento da União Europeia no Brasil. **Revista CEJ, Brasília, Ano XXVII**, n. 85, p. 47-54, 2023. Disponível em: <file:///C:/Users/Aline/Downloads/2791-Texto%20do%20artigo-7770-1-10-20231116.pdf>. Acesso em: 14 out 2024.

Anexos

Ofício

Ao Tribunal de Justiça do Estado de Pernambuco Comitê de Governança de Tecnologia da Informação e Comunicação

Excelentíssimo Senhor Doutor Desembargador Presidente do Comitê de Governança de Tecnologia da Informação e Comunicação Alexandre Freire Pimentel,

Com os devidos cumprimentos, venho encaminhar o pedido de informações, todas para fins de pesquisa no Doutorado do Programa de Pós-Graduação em Direito da Universidade Católica de Pernambuco e da Universidade de Pisa – Itália, a respeito da adequação do Tribunal de Justiça do Estado de Pernambuco à Lei Geral de Proteção de Dados e demais regulamentações, quando da realização de audiências por videoconferência. As informações serão utilizadas única e exclusivamente para fins de contribuição que agregarão a pesquisa desenvolvida na Tese de Doutorado com tema de privacidade e proteção de dados pessoais. Desse modo, as informações a serem analisadas e estudadas seguem a partir dos seguintes questionamentos:

1. Os servidores (controladores, operadores e encarregados pelo tratamento dos dados pessoais) do Tribunal de Justiça de Pernambuco recebem treinamento sobre a Lei Geral de Proteção de Dados e demais regulamentos e resoluções pertinentes ao tema?
2. Há política de proteção de dados estabelecida no âmbito do Tribunal de Justiça do Estado de Pernambuco?
3. Durante a realização das audiências por videoconferência, no Tribunal de Justiça de Pernambuco, ocorre a coleta de dados pessoais dos participantes, sejam partes, servidores, juízes, membros do Ministério Público, testemunhas ou qualquer outra pessoa participante?
4. Em havendo a referida coleta de dados, como esta é realizada? De forma oral, imagens de documentos, escritas em chat ou outro meio? As pessoas são cientificadas do propósito da coleta, segurança e demais orientações pertinentes ao ato praticado?
5. Como se dá o armazenamento das gravações de audiência por videoconferência no âmbito do Tribunal de Justiça de Pernambuco? O servidor(a) responsável segue algum critério específico?
6. Por quanto tempo as gravações ficam armazenadas nos arquivos do Tribunal?
7. Quais critérios de segurança e proteção das gravações? Há exigência de protocolos específicos, como uso de senhas, treinamento específico?
8. A realização das audiências é feita por qualquer servidor do setor/vara?
9. Qualquer servidor do setor/vara tem acesso ao armazenamento das gravações?

Reitero que os questionamentos acima sinalizados são para fins de pesquisa acadêmica/científica e análise de acordo com trabalho desenvolvido no Doutorado.

Na oportunidade, reitero os protestos de elevada e estima consideração.

Aline Taraziuk Nicodemos

Doutoranda do Programa de Pós-Graduação da Universidade Católica de Pernambuco e da Universidade de Pisa, Itália

Alla Corte di Pisa – Ministero della Giustizia
Presidente Dott.ssa Beatrice Dani

Con i dovuti saluti, mi permetto di inoltrare la richiesta di informazioni, tutte a scopo di ricerca per il Dottorato presso l'Università di Pisa e il Programma di Post-Laurea in Diritto dell'Università Cattolica di Pernambuco-Brasile, riguardo l'adeguamento del Tribunale di Pisa al Regolamento Europeo sulla protezione dei dati e altre normative, in occasione della realizzazione di udienze tramite videoconferenza.

Le informazioni saranno utilizzate unicamente ai fini di contribuire alla ricerca sviluppata nella Tesi di Dottorato, sotto la guida della Professoressa Francesca Martines, associata di diritto dell'Unione Europea, Dipartimento di Giurisprudenza dell'Università di Pisa e del Professore Alexandre Freire Pimentel, docente nella linea di ricerca di Diritto Digitale dell'Università Cattolica di Pernambuco e Giudice del Tribunale di Giustizia dello Stato di Pernambuco.

Il tema del lavoro riguarda la privacy e la protezione dei dati personali (L'uso di piattaforme di comunicazione digitale per la realizzazione di udienze tramite videoconferenza: la raccolta e il trattamento dei dati da parte del potere giudiziario brasiliano e italiano e la conformità con le rispettive normative).

In questo modo, le informazioni da analizzare e studiare derivano dai seguenti quesiti:

1. I dipendenti (responsabili, incaricati e addetti al trattamento dei dati personali) del Tribunale di Pisa ricevono formazione sul Regolamento Europeo sulla protezione dei dati e su altre normative e risoluzioni pertinenti al tema?

2. Esiste una politica di protezione dei dati stabilita nell'ambito del Tribunale di Pisa?

3. Durante lo svolgimento delle udienze tramite videoconferenza nel Tribunale di Pisa, avviene la raccolta di dati personali dei partecipanti, siano essi parti, dipendenti, giudici, membri del Ministero Pubblico, testimoni o qualsiasi altra persona partecipante?

4. Nel caso di suddetta raccolta di dati, come viene effettuata? Verbalmente, tramite immagini di documenti, scritti in chat o altri mezzi? Le persone sono informate dello scopo della raccolta, della sicurezza e di altre istruzioni pertinenti all'atto compiuto?

5. Come avviene l'archiviazione delle registrazioni delle udienze tramite videoconferenza nell'ambito del Tribunale di Pisa? Il/la responsabile segue qualche criterio specifico? 6. Per quanto tempo le registrazioni rimangono archiviate nei file del Tribunale?

7. Quali sono i criteri di sicurezza e protezione delle registrazioni? È richiesta l'adozione di protocolli specifici, come l'uso di password, formazione specifica?

8. La realizzazione delle udienze è effettuata da qualsiasi dipendente del settore/sezione?

9. Qualsiasi dipendente del settore/sezione ha accesso all'archiviazione delle registrazioni? Ribadisco che i quesiti sopra indicati sono a scopo di ricerca accademica/scientifica e analisi secondo il lavoro sviluppato nel Dottorato. Colgo l'occasione per rinnovare i miei più distinti saluti e considerazione.

Aline Taraziuk Nicodemos
Dottoranda dell'Università di Pisa e del Programma di Post-Laurea dell'Università
Cattolica di Pernambuco – Brasile

E-mail Tribunal de Justiça do Estado de Pernambuco

**Ofício ao Comitê de Governança de Tecnologia da Informação e Comunicação
TJPE**

Aline Taraziuk Nicodemos <aline.nicodemos@phd.unipi.it>

Seg, 01/04/2024 17:02

Para: alexandre.pimentel@tjpe.jus.br <alexandre.pimentel@tjpe.jus.br>

1 anexos (2 MB)

Ofício ao Tribunal Aline.pdf; Boa tarde, Excelentíssimo Senhor Doutor Presidente do Comitê de Governança de Tecnologia da Informação e Comunicação do Tribunal de Justiça do Estado de Pernambuco,

Com os devidos cumprimentos, venho, por meio deste e-mail encaminhar o ofício, que segue em anexo, dirigido a esse Comitê, para fins de pesquisa, solicitar informações a respeito dos procedimentos adotados por esse Tribunal no que diz respeito à Proteção de dados Pessoais e audiências por videoconferência.

Os dados serão utilizados para fins de pesquisa na Tese de doutorado desenvolvida por mim, aluna da Universidade Católica de Pernambuco e a Universidade de Pisa, Itália.

Cordialmente,

Aline Taraziuk Nicodemos

Doutoranda UNICAP e UNIFI

23/07/2024, 11:45 Email – Aline Taraziuk Nicodemos – Outlook
<https://outlook.office.com/mail/sentitems/id/AAQkADc2MjQ0ZjU4LWNhMTktNGM3MS1hYTRkLWNiMWRiNzhmM2Q0MgAQACTgxTtQqnBOiWdk...>

Ricerca sulla conformità del sistema giudiziario - Dottorato di Ricerca

Aline Taraziuk Nicodemos <aline.nicodemos@phd.unipi.it>

Sex, 19/04/2024 10:32

Para: tribunale.pisa@giustizia.it <tribunale.pisa@giustizia.it> Cc: Francesca Martines <francesca.martines@unipi.it>

1 anexos (2 MB)

Tribunale di Pisa IT..pdf;

Buongiorno, Dott.ssa Presidente Beatrice Dani.

Sono una studentessa di Dottorato di ricerca in Giurisprudenza presso l'Università di Pisa in cotutela con l'Università Cattolica del Pernambuco, Brasile, ho come Direttrice della ricerca la Professoressa Francesca Martines, che è ci legge in copia. Sto conducendo una ricerca sulla conformità del sistema giudiziario, in particolare nello svolgimento di udienze tramite videoconferenza, al regolamento sulla protezione dei dati e desidererei ottenere alcune informazioni istituzionali dal Tribunale di Pisa, come ho già richiesto al Tribunale in Brasile. Ho allegato a questa e-mail un documento con il tema della ricerca (privacy e protezione dei dati) e le domande che vorrei porre a questa istituzione. Le risposte saranno analizzate e inserite nel lavoro di Tesi soltanto a scopo di ricerca e costituiranno un contributo prezioso per lo sviluppo della mia ricerca.

Ringrazio anticipatamente per la disponibilità.

Aline Taraziuk Nicodemos

Dottoranda di ricerca in giurisprudenza

23/07/2024, 11:46 Email – Aline Taraziuk Nicodemos – Outlook
<https://outlook.office.com/mail/sentitems/id/AAQkADc2MjQ0ZjU4LWNhMTktNGM3MS1hYTRkLWNiMWRiNzhmM2Q0MgAQAPle%2BivxEDIEtIM...>

Questionario - Dottorato di Ricerca in giurisprudenza - Studentessa Nicodemos Aline

Aline Taraziuk Nicodemos <aline.nicodemos@phd.unipi.it>

Qua, 19/06/2024 07:11

Para: tribunale.pisa@giustizia.it <tribunale.pisa@giustizia.it> Cc: Francesca Martines <francesca.martines@unipi.it>

Gentilissima Presidente dott.ssa Dani,

Sono una studente del dottorato di ricerca in giurisprudenza presso l'Università di Pisa e l'Universidade Católica de Pernambuco in regime dicotutela, sotto la supervisione della Professoressa Francesca Martines, che è in copia. Sto studiando la protezione dei dati nel processo giudiziario, con particolare attenzione alle udienze in videoconferenza. Ho inviato un questionario al Tribunale di Pisa a metà aprile con alcune domande le cui risposte potrebbero integrare la mia ricerca. Sto completando la stesura del testo e la data di discussione è prossima. Poiché le risposte possono veramente incidere positivamente sui risultati della mia tesi Le chiederei gentilmente se sarebbe possibile - compatibilmente con le esigenze di lavoro del suo ufficio - riuscire ad ottenere nei prossimi giorni le risposte al questionario. Queste mi permetterebbero di consegnare il testo della tesi alla fine del mese.

La ringrazio moltissimo per la sua cortese attenzione

Cordiali saluti.

Aline Nicodemos

23/07/2024, 11:46 Email – Aline Taraziuk Nicodemos – Outlook
<https://outlook.office.com/mail/sentitems/id/AAQkADc2MjQ0ZjU4LWNhMTktNGM3MS1hYTRkLWNiMWRiNzhmM2Q0MgAQAGEozIj%2FUgBBoM...>

Questionario - Doutorado em Direito - Estudante Aline Nicodemos

Aline Taraziuk Nicodemos <aline.nicodemos@phd.unipi.it>

Qua, 19/06/2024 07:18

Para: alexandre.pimentel@tjpe.jus.br <alexandre.pimentel@tjpe.jus.br>

Exmo. Sr. Dr. Alexandre Freire Pimentel,

Sou estudante de doutorado em Direito na Universidade de Pisa e na Universidade Católica de Pernambuco em regime de cotutela. Estou estudando a proteção de dados no processo judicial, com particular atenção às audiências por videoconferência. Enviei um questionário ao Tribunal de Justiça do Estado de Pernambuco em abril com algumas perguntas cujas respostas poderiam integrar minha pesquisa. Estou completando a redação do texto e a data de defesa está próxima. Como as respostas podem realmente impactar positivamente os resultados da minha tese, pediri gentilmente se seria possível - compativelmente vossos compromissos institucionais - obter nos próximos dias as respostas ao questionário. O prazo para entregar o texto da tese é até o final do mês de junho.

Agradeço muitíssimo pela sua cortês atenção.

Cordiais saudações.

Aline Nicodemos

23/07/2024, 11:47 Email – Aline Taraziuk Nicodemos – Outlook

<https://outlook.office.com/mail/sentitems/id/AAQkADc2MjQ0ZjU4LWNhMTktNGM3MS1hYTRkLWNiMWRiNzhmM2Q0MgAQAJY4Q4wm0RNHv0A...>

Ricerca sulla conformità del sistema giudiziario - Dottorato di Ricerca - Aline Taraziuk Nicodemos - Outlook - Google Chrome

about:blank

Excluír Arquivar Denunciar Resposta Resposta a todos Encaminhar Aplicar zoom

Ricerca sulla conformità del sistema giudiziario - Dottorato di Ricerca

privacy...IVILE.docx privacy...ENALE.docx

BP Beatrice Pellegrinelli <beatrice.pellegrinelli@giustizia.it>
Para: Aline Taraziuk Nicodemos
Cc: Beatrice Dani <beatrice.dani@giustizia.it>; Angela D'aniello <angela.daniello02@giustizia.it>; Beatrice Dani <beatrice.dani@giustizia.it>; Francesca Martines
Qui, 01/08/2024 05:22

Você respondeu em Qua. 14/08/2024 15:55

Esta mensagem está em Italiano Traduzir para o Português (Brasil) Nunca traduzir do Italiano

privacy - SEZIONE CIVILE.docx 17 KB privacy - SEZIONE PENALE.d... 17 KB

2 anexos (34 KB) Salvar tudo no OneDrive - University of Pisa Baixar tudo

Iniciar a responder com: Grazie mille! Ricevuto. Grazie!

Buongiorno,
dando seguito alla richiesta di informazioni avanzata dalla dott.ssa Nicodemos, si provvede ad inoltrare le risposte del Tribunale di Pisa.
Rimanendo a disposizione per eventuali precisazioni o chiarimenti, si porgono cordiali saluti.

Dott.ssa Beatrice Pellegrinelli
Funzionario Ufficio per il Processo
Tribunale di Pisa
Tel. 050 513615

Pesquisar 18:53 15/10/2024

Fwd: Questionário Tratamento de Dados TJPE - Aline Nicodemos - Outlook - Google Chrome

about:blank

Excluír Arquivar Denunciar Resposta Aplicar zoom Lido / Não lido Categorizar Sinalizar/ Remover sinalizador Imprimir

Fwd: Questionário Tratamento de Dados TJPE

AS Alexandre Freire Pimentel <alexandrefreirepimentel@gmail.com>
Para: Você
Qua, 28/08/2024 14:21

----- Forwarded message -----
De: JULIANA SOUZA CARVALHO CASIMIRO <juliana.casimiro@tjpe.jus.br>
Data: qua, 28 de ago. de 2024, 11:10
Subject: ENC: Questionário Tratamento de Dados TJPE
To: ALEXANDRE FREIRE PIMENTEL <alexandrefreirepimentel@gmail.com>, alexandrefreirepimentel@gmail.com <alexandrefreirepimentel@gmail.com>

Bom dia Prof.,
segue resposta da encarregada de dados quanto ao questionário de Aline.
Att.,
Juliana Casimiro

De: ELIS BEZERRA DE MENDONÇA OLIVEIRA <elis.oliveira@tjpe.jus.br>
Enviado: quarta-feira, 28 de agosto de 2024 11:04
Para: JULIANA SOUZA CARVALHO CASIMIRO <juliana.casimiro@tjpe.jus.br>
Assunto: RE: Questionário Tratamento de Dados TJPE

Bom dia, Juliana.
Envio a seguir as respostas ao questionário. Espero que seja útil.
Qualquer esclarecimento, mantenho-me a disposição.
Atenciosamente,
Elisa Oliveira
Encarregada de Proteção de dados - TJPE.

1. Os servidores (controladores, operadores e encarregados pelo tratamento dos dados pessoais) do Tribunal de Justiça de Pernambuco recebem treinamento sobre a Lei Geral de Proteção de Dados e demais regulamentos e resoluções pertinentes ao tema? **sim. Periodicamente a ESMAPE oferece cursos sobre proteção de dados, LGPD e segurança da informação.**

Pesquisar 18:55 15/10/2024