ATHENAS REVISTA DE DIREITO, POLÍTICA E FILOSOFIA

SEGURANÇA DA INFORMAÇÃO NO JUDICIÁRIO BRASILEIRO: Desafios, possibilidades e riscos impostos pelo hackeamento de dados

INFORMATION SECURITY IN THE BRAZILIAN JUDICIARY: Challenges, possibilities and risks imposed by data hacking

Edilene Lôbo[1]
Ana Lúcia Ribeiro Mól[2]

RESUMO: Recentemente tem-se constatado um crescimento acentuado dos ataques cibernéticos às plataformas digitais dos tribunais brasileiros, demonstrando a vulnerabilidade dos seus sistemas eletrônicos e os perigos que podem advir dessas situações. Nesse contexto, ganha relevo a análise da segurança da informação e os impactos consideráveis que sua violação gera nos direitos e garantias fundamentais, especialmente quando a atuação de *hackers* atinge atividades essenciais do Estado, como é o caso da jurisdição. A análise dessa temática, embasada no método dedutivo e em pesquisa bibliográfica, constitui o objetivo principal do presente estudo, que concluiu pela inevitabilidade da aplicação dos instrumentos tecnológicos no exercício da atividade jurisdicional, especialmente a par do uso acentuado dos algoritmos como fórmulas capazes de possibilitar economia e celeridade à prestação dos serviços judiciais, mas não ignora a necessidade de se repensar a segurança cibernética, a partir da adoção de medidas preventivas para que haja alguma contenção na ação dos saqueadores de dados e informações. As consequências relacionadas à possibilidade de divulgação, remoção ou modificação de informações processuais, com violação de direitos e garantias previstos no texto constitucional, além dos visíveis prejuízos à soberania nacional, denotam a relevância da pesquisa.
PALAVRAS-CHAVE: Tecnologia; jurisdição; ataque cibernético; hackeamento de dados; Tribunais Brasileiros.

ABSTRACT: Recently, there has been a marked increase in cyber attacks on the digital platforms of Brazilian courts, demonstrating the vulnerability of their electronic systems and the dangers that can arise from these situations. In this context, the analysis of information security and the considerable impacts that its violation generates on fundamental rights and guarantees stands out, especially when the performance of hackers affects essential activities of the State, as is the case of jurisdiction. The analysis of this theme, based on the deductive method and on bibliographic research, constitutes the main objective of the present study, which concluded by the inevitability of the application of technological instruments in the exercise of judicial activity, especially along with the accentuated use of algorithms as formulas capable of enabling economy and speed in the provision of judicial services, but it does not ignore the need to rethink cyber security, from the adoption of preventive measures so that there is some restraint in the action of data and information looters. The consequences related to the possibility of disclosing, removing or modifying procedural information, with violation of rights and guarantees provided for in the constitutional text, in addition to the visible damage to national sovereignty, denote the relevance of the research.
KEYWORDS: Technology; jurisdiction; cyber attack; data hacking; Brazilian Courts.

[1] Doutora em Direito Processual (PUC/MG). Mestra em Direito Administrativo (UFMG). Especialista em Processo Penal (UCLA). Professora do PPGD *Stricto Sensu* da Universidade de Itaúna. Professora Convidada da Pós-Graduação em Processo Eleitoral da PUC/MG. Advogada. Email: edilenelobo@yahoo.com.br. ORCID:https://orcid.org/0000-0003-4043-0286. Curriculo Lattes: http://lattes.cnpq.br/6348105561410653.
[2] Doutoranda em Proteção dos Direitos Fundamentais da Universidade de Itaúna (UIT). Mestre em Direito Processual (PUC/MG). Professora da Universidade Estadual de Montes Claros (UNIMONTES). Procuradora do Município de Montes Claros-MG. ORCID: https://orcid.org/0000-0002-3486-0215. E-mail: anaribeiromol@gmail.com. Currículo Lattes: http://lattes.cnpq.br/1686178234063670.

INTRODUÇÃO

Nos últimos anos, os tribunais brasileiros têm sido alvo de ataques *hackers*, com paralisação dos sistemas e suspensão de acesso aos sítios eletrônicos, gerando repercussões relevantes na prática de atos processuais. Tais eventos não deixam de tumultuar o exercício da função jurisdicional, causando transtornos institucionais e, por consequência, à população, que é a destinatária final dessa atividade estatal.

Essa constatação levanta a necessidade de se discutir a questão da segurança da informação, a utilização indevida das ferramentas tecnológicas e os impactos dessas intercorrências quando são atingidas as bases de dados dos órgãos do Judiciário.

A contextualização dessa temática perpassa pela análise da aplicação das novas tecnologias pelos órgãos públicos no Brasil, em especial pelos tribunais, a revelar a inevitabilidade de incorporação dos parâmetros estabelecidos pela revolução digital nessa seara, como decorrência da própria transformação da sociedade e dos seus vários setores, implementada pela incorporação dos avanços tecnológicos em todas as relações interpessoais.

Nesse sentido, verifica-se que as plataformas digitais, os sistemas de telecomunicações e o uso da inteligência artificial são realidades atualmente indissociáveis do exercício da jurisdição e demandam a necessidade de compatibilizá-las com a preservação dos direitos e garantias previstos e consagrados no texto constitucional em vigor.

Contudo, a par do proveito que pode resultar de sua utilização para a concretização dessa função estatal, especialmente no que se refere ao aumento da produtividade do Judiciário e da prática de atos processuais em menor espaço de tempo, tem-se a possibilidade de exposição e sequestro de dados e, ainda, a interferência no próprio exercício da jurisdição em situações de ameaça e efetivo ataque cibernético aos sistemas dos tribunais, como se tem visto recorrentemente no Brasil.

A partir dessa perspectiva, o presente estudo busca analisar as consequências decorrentes da vulnerabilidade da segurança da informação dos órgãos jurisdicionais e tem como intuito, em última instância, apontar a necessidade de se repensar as medidas preventivas que devem girar em torno da proteção dos dados e dos serviços

judiciais, especialmente quando se trata de função do Estado essencial à soberania nacional e, ainda, à concretização das garantias estabelecidas na Constituição para a cidadania: a jurisdição.

Com vistas a enfrentar os objetivos propostos, metodologicamente, a pesquisa bibliográfica, amparada em legislação, obras nacionais e estrangeiras, realiza-se, num primeiro momento, a partir de estudo descritivo sobre as recentes tecnologias utilizadas pelo Judiciário, mostrando que, apesar de sua tradição discursiva e humana, essa função estatal tem-se valido de cabedal de mecanismos tecnológicos na sua atividade precípua. Em seguida, como lócus de discussão da problemática da pesquisa, são abordados os ataques cibernéticos sofridos pelos tribunais brasileiros, demonstrando-se a instabilidade desses sistemas de informação e os riscos que daí podem advir para os direitos dos usuários desses serviços.

1. AS CONQUISTAS TECNOLÓGICAS A SERVIÇO DA ATIVIDADE JURISDICIONAL

Desde a década de 70, tem-se constatado o avanço da criação e desenvolvimento de novas tecnologias, com reflexos de relevo na estrutura econômica, social e cultural em níveis planetários (WERTHEIN, 2000). A globalização, atrelada ao uso das ferramentas digitais e da *internet*, tem potencializado essas mudanças, que ocorrem numa rapidez de difícil mensuração, redefinindo as ideias de tempo e lugar até então tidas como consolidadas (PÉREZ LUÑO, 2014).

A inevitabilidade das transformações operadas pela revolução digital, como não poderia deixar de ser, vem alcançando, especialmente nos últimos anos, a ciência jurídica e suas formas de aplicação. Nesse contexto, a possibilidade de se realizar múltiplas atividades de forma célere, muitas vezes de modo simultâneo e instantâneo, não passou despercebida pelo Judiciário.

Seguindo a tendência mundial e constatada de forma interdisciplinar nos vários setores da sociedade, os avanços tecnológicos alcançam essa função do Estado a passos largos, a ponto de se revelar inexorável o caminhar em direção a um mundo novo. As *lawtechs* ou *legaltechs*, entendidas como ferramentas que buscam simplificar e acelerar os atos praticados na seara jurídica numa extensão maior do que se efetivados do modo tradicional, já são indissociáveis do cotidiano forense (SALMERÓN-MANZANO, 2021).

Basta constatar que os autos físicos cederam lugar aos autos eletrônicos, com economia de recursos financeiros e de espaço, de um lado, e na busca pela garantia da eficiência, de outro. A partir desse progresso, constata-se que os dados dos procedimentos instaurados perante o Judiciário passaram a se hospedar em nuvens, inseridos numa rede digital que exige a aplicação de novas e múltiplas tecnologias para a sua utilização. Em decorrência dessa circunstância, atualmente tem-se a disponibilidade dos autos a todo momento e em qualquer lugar, sendo suficiente, para tanto, o acesso com as qualificações exigidas para a utilização dos sistemas eletrônicos pertinentes.

É de se ressaltar que a concretização do processo eletrônico avulta-se, claramente, como um marco na ruptura de um sistema tradicionalmente material e analógico, para outro em que imperam os meios digitais. A partir de então, não se olvida que o operador do direito necessariamente precisa, como condição *sine qua non* para o exercício de suas atribuições, deter razoável conhecimento tecnológico, o que já faz parte da sua atuação rotineira. Porém, não se pode dizer o mesmo dos cidadãos representados nesses variados processos, ainda mais quando desponta, a par da constatação que 55 milhões de brasileiros não têm pleno acesso à tecnologia (IDEC; LOCOMOTIVA, 2021), uma nova modalidade de escassez ou analfabetismo no campo digital.

A tendência para a utilização da *internet* e dos avanços tecnológicos no processo tem sido encorpada pela ampliação dessas vias para a prática de atos processuais, que, até pouco tempo, não se pensavam críveis para além dos limites territoriais do fórum.

Hoje se tem como realidade a realização de sessões de julgamento de recursos pela via *on-line*, o mesmo acontecendo com audiências de conciliação, e mesmo de instrução, não obstante as dificuldades de acesso constatadas na prática, em grande parte pela restrição de parcela da população brasileira ao uso das novas tecnologias, com graves prejuízos aos interessados no processo.

O uso dessa via foi potencializado pela necessidade de isolamento social e da redução da aglomeração de pessoas imposta pela pandemia do coronavírus, que fez com que fossem tomadas medidas urgentes e necessárias à continuidade da função jurisdicional, haja vista tratar-se de um serviço essencial e, portanto, insuscetível de interrupção. As plataformas digitais passaram a ser utilizadas para que os julgamentos e as audiências ocorressem em tempo real e de forma remota por videoconferência.

Apesar de ter ganhado força no momento atual, certo é que aquela possibilidade já se encontrava prevista no Código de Processo Civil (BRASIL, 2015), e, quanto ao processo eletrônico, na Lei n.º 11.419, de 19 de dezembro de 2006 (BRASIL, 2006), que preconizaram a realização de uma série de atos processuais nesse formato.

A par dos atos que devam ser assim praticados como decorrência natural da virtualização dos autos, inclusive aqueles de comunicação processual, como citações, intimações e cartas, deve-se destacar que o Código de Processo Civil permitiu que certos meios de prova, como o depoimento pessoal e a oitiva de testemunhas, fossem produzidos por quaisquer mecanismos de transmissão de sons e imagens em tempo real.

É dizer, o que se tem visto hoje, como aplicação corriqueira, já estava estabelecido e permitido no mencionado código, o que denota, ainda que de forma tímida, a sua posição de vanguarda quanto à fixação de regras para as práticas processuais de forma eletrônica, ao lado da já mencionada Lei n.º 11.419/2006.

Mais recentemente, o Conselho Nacional de Justiça (CNJ) permitiu a possibilidade de os tribunais instaurarem o denominado Juízo 100% Digital, em decorrência da Resolução n.º 345, de 09 de outubro de 2020 (CONSELHO NACIONAL DE JUSTIÇA, 2020).

Esse modelo prevê que todos os atos sejam realizados pelos meios digitais, afastando-se qualquer necessidade de deslocamento das partes ou de seus representantes aos órgãos do Judiciário. Além da prática eletrônica dos atos processuais, qualquer atendimento a ser realizado por servidores em relação às demandas judiciais se dará, igualmente, de forma virtual, inclusive o contato entre juiz e advogado.

Deve-se salientar que essa iniciativa concretiza um fortalecimento considerável na automação dos tribunais, cujo objetivo é incrementar a produtividade e minimizar o tempo de duração do processo, reduzindo despesas do Estado com a atividade jurisdicional. Os próprios motivos declinados na resolução aprovada pelo CNJ denotam a existência dessa finalidade, mas deixam de mencionar, por óbvio, os inconvenientes da implementação dessa via, alguns dos quais já mencionados anteriormente, nomeadamente a restrição ao acesso dos excluídos digitais e os ataques de *hackers*.

Reforçando essa tendência, inclusive com aplicação anterior à ideia do Juízo 100% Digital, é visto o crescimento cada vez maior da inteligência artificial no exercício da jurisdição. A inteligência artificial é assim denominada porque usa a tecnologia como forma de reproduzir, na medida do possível, a aptidão do ser humano de compreender situações, identificar problemas, pensar em soluções possíveis e aplicá-las de forma mecanizada e célere (BARRETO JÚNIOR; SPAREMBERGER, 2020).

Com a utilização dos algoritmos, deixa-se o uso da tecnologia apenas como forma de (re)operacionalizar a atividade jurisdicional e a atuação das partes no processo por meio das plataformas digitais, para utilizá-la como forma de apuração e organização de dados, reestruturando informações, afetando os próprios julgamentos emitidos pelo órgão judiciário. A sistematização de dados, a predição de informações e a criação de algoritmos são importantes mecanismos utilizados nessa finalidade (NUNES, 2021).

É interessante notar que as possibilidades geradas pelo emprego da inteligência artificial são incomensuráveis e não se configuram em algo que se encontra apenas no campo das ideias. Sua efetiva aplicação já tem ocorrido, como a ferramenta denominada “Victor”, um algoritmo de classificação de dados utilizado pelo Supremo Tribunal Federal na análise de processos, buscando relacioná-los aos temas de repercussão geral declarados pela Corte. Mais recentemente foi criado o “RAFA” (Redes Artificiais Focadas), cujo objetivo é identificar, nesse mesmo tribunal, os processos que envolvem direitos humanos e os dezessete objetivos da Agenda 2030 da Organização das Nações Unidas.

A propósito, são enfáticas as cogitações de ampliação do uso dos algoritmos, para evitar ruídos ou falhas no julgamento humano (KAHNEMAN; SIBONY; SUNSTEIN, 2021), não se podendo perder de vista que a decisão algorítmica sozinha não permite explicabilidade, residindo aí o desafio da automação absoluta, uma vez que não se pode terceirizar a vida (FRAZÃO, 2021).

Outro aspecto essencial quanto à inteligência artificial envolve a transparência e a segurança jurídica em seu uso, com a adoção de regras claras e expressões inteligíveis, de fácil compreensão (MORAIS DA ROSA, 2019). E, desde logo, sua implantação e expansão deve ocorrer depois de esgotados diálogos públicos e de construção de políticas públicas sólidas para o acesso à inovação, até para que se saiba quem são seus desenvolvedores, como os algoritmos são formados, qual o destino da imensidão de dados tratados, como são descartados, como e se é

remunerado seu uso fora das finalidades precípuas, enfim, com respeito ao fundamento mais pungente do Estado Democrático de Direito.

Não obstante os desafios na utilização da inteligência artificial e das novas tecnologias constata-se que a jurisdição caminha para o emprego dos meios tecnológicos, digitais e de automação cada vez maior, como consequência da atual sociedade da informação.

Esse movimento é denominado por Dierle Nunes (2021) como a virada tecnológica no Direito Processual. A densidade dessas transformações desponta de tal maneira que seus impactos não se restringirão à forma como os atos processuais são praticados. A automatização crescente, de um número cada vez maior de atribuições dentro do procedimento, com incursões profundas no exercício da jurisdição é trajetória inexorável.

Não se olvida, contudo, que todos os avanços ocorridos no exercício da função jurisdicional pela via eletrônica devem ser implementados como meios que possibilitem e simplifiquem a atuação dos sujeitos do processo, não podendo configurar-se como obstáculos a que isso aconteça, sob pena de restar visível o prejuízo a vários direitos e garantias processuais constitucionalmente previstos (NUNES; BAHIA; PEDRON, 2020).

Mais ainda, é necessário que a aplicação das novas tecnologias se dê num ambiente cibernético seguro, até mesmo para que viabilize a adequada execução de todas as potencialidades que essas ferramentas prometem.

Contudo, na prática, o que se tem visto são notícias frequentes de ataques cibernéticos sofridos pelos tribunais brasileiros, a exemplo do que ocorreu no Supremo Tribunal Federal (STF, 2021), no Superior Tribunal de Justiça e no Tribunal Superior Eleitoral (FUX, 2020).

Em geral, a prática conhecida como *ransomware* (RANSOWARE, 2021) consiste na inoculação de vírus que impede o funcionamento orgânico dos sistemas, objetivando extorquir quantias dos afetados, geralmente pagas em criptomoedas, o que praticamente impede seu rastreamento.

Nessa nova realidade de manipulação de dados sob risco de ataques cibernéticos, assim como da extrema necessidade de se oportunizar aos cidadãos o acesso a essas novas tecnologias conforme promessa constitucional[3], questiona-se

[3] A previsão constitucional do direito fundamental de acesso às novas tecnologias encontra-se no art. 218, *caput*, com a seguinte redação: “Art. 218. O Estado promoverá e incentivará o desenvolvimento

em que medida a tecnologia favorece ou aprisiona a função estatal enfocada. Esse debate, sob o prisma da segurança da informação e da garantia de acesso aos bens fundamentais à vida coletiva, é o que se pretende enfrentar no tópico que se segue.

2. A TECNOLOGIA A FAVOR DO JUDICIÁRIO OU O JUDICIÁRIO REFÉM DA TECNOLOGIA?

Como ressaltado, a tecnologia é relevante para o indivíduo, para a sociedade e para a atuação do Estado. A utilização adequada das ferramentas digitais conduz à modernização das estruturas e da atividade jurisdicional, garantindo a publicidade e a transparência dos atos praticados pelo Judiciário, por meio dessa função que lhe é inerente. De fato, tal relevância não vem desacompanhada de consequências negativas e que atingem diretamente os direitos do ser humano, como indivíduo e como coletividade.

Uma das consequências negativas decorrentes dessa circunstância é a dificuldade de se controlar a utilização indevida nas ferramentas tecnológicas, o que gera hesitação e incertezas na utilização do espaço cibernético, elevando-se à posição de destaque as questões afetas à segurança da informação.

A análise dessa temática sobreleva de importância quando se tem em mente que o Estado, no exercício da jurisdição pelos meios eletrônicos, é alçado à categoria de operador e controlador de dados sensíveis dos cidadãos, por armazenar e manipular as mais diversas informações pessoais constantes das inúmeras demandas que tramitam em seus sistemas operacionais. Inclusive, por essa razão, o Poder Público encontra-se submetido a uma série de atribuições e deveres específicos previstos na Lei nº 13.709/2018 (BRASIL, 2018), conhecida como a Lei Geral de Proteção de Dados (LGPD), o que reforça, ainda mais, a necessidade de se debruçar sobre as diretrizes relacionadas ao cuidado e à preservação das informações sob sua custódia.

O risco de exposição desses dados e a fragilidade do sistema de informática e de armazenamento de informações dos tribunais brasileiros tomou corpo recentemente com as invasões de *hackers* nos sítios eletrônicos de alguns dos seus principais órgãos. Não obstante a ausência de transparência do Poder Público na

científico, a pesquisa, a capacitação científica e tecnológica e a inovação" (BRASIL, 1988). Trata-se de uma prerrogativa essencial para que os indivíduos se capacitem para o exercício do direito fundamental de acesso ao processo-garantia.

prestação de informações acerca de tais ingerências, na eventual existência ou e extensão de dados manipulados e se, de fato, tais problemas foram contornados, não se olvida que, no mínimo, tem-se uma afronta à ideia de segurança que deve permear a atuação dessas instituições.

O exemplo mais emblemático foi o ataque cibernético sofrido pelo Superior Tribunal de Justiça em 03 de novembro de 2020, que impediu o acesso à plataforma e a realização de inúmeros atos processuais por seis dias, com a suspensão dos prazos durante esse período. Dadas as suas proporções, essa situação foi tida como a mais significante investida em desfavor da rede de um ente público no Brasil. O tribunal que primeiro vivenciou a implantação da tecnologia na prestação dos seus serviços dentro do Judiciário, iniciada em 2009, viu-se na premência de ter que lidar com uma ocupação *hacker* de seu sistema, e todas as consequências daí advindas.

É importante salientar que, após o ataque em questão, o Tribunal Superior Eleitoral foi alvo de acesso indevido ao seu banco de dados na data do 1º turno das eleições de 2020, com exposição de questões administrativas a respeito de servidores e Ministros que ali já atuaram.

No início de 2021, o Supremo Tribunal Federal igualmente teve seu sistema invadido, de modo que, por medidas de segurança, o sítio eletrônico foi retirado do ar, para impedir a atuação dos *hackers* e evitar maiores danos ao armazenamento dos dados e à prestação do serviço público.

Tais situações formam um rol exemplificativo de ocorrências desse tipo e denotam como tais invasões têm ocorrido com relativa periodicidade nos tribunais superiores. Contudo, com muito mais frequência também se notam ocorrências dessa espécie em tribunais federais e estaduais de segunda instância, como se deu no Tribunal Regional Federal da 1ª Região (HACKERS, 2020) e no Tribunal de Justiça do Rio Grande do Sul, apenas para nominar alguns deles (TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL, 2020).

A primeira consequência importante de situações como esta é a interrupção forçada das atividades dos órgãos jurisdicionais. A invasão dos sistemas, de pronto, ocasiona a paralisação de milhares de processos, prejudicando direitos fundamentais dos jurisdicionados, por via direta e também indiretamente, a partir do momento em que a descontinuação da atividade jurisdicional também afeta a estrutura administrativa do Estado, que igualmente depende, em muitos aspectos, do órgão judiciário.

Outro ponto importante, certamente a principal questão a ser analisada nesse contexto, refere-se à proteção dos dados existentes nas plataformas dos tribunais. A invasão de qualquer sistema faz com que os dados nele contidos fiquem à mercê de serem destruídos, manipulados, vendidos, alterados ou divulgados, comprometendo toda a sua estrutura e conteúdo, delineando um cenário, no mínimo preocupante, para os usuários[4]. Quando tal situação ocorre com plataformas geridas pelo poder público, a preocupação toma proporções maiores, inclusive por envolver a possibilidade de modificação ou supressão de dados que podem atingir e desvirtuar a própria sorte da demanda judicial, sem falar na hipótese de divulgação de informações sigilosas, com graves e profundos prejuízos às partes envolvidas. Não apenas a segurança jurídica é atingida, mas também os direitos e garantias fundamentais dos envolvidos nas ações judiciais correm sérios riscos de violação.

A exposição e a debilidade da proteção dos sistemas dos tribunais brasileiros, para além dessas questões, desbordam em impactos negativos à própria soberania do Estado. Sob essa perspectiva, o que se verifica é que as funções estatais ficam subjugadas ao poder tecnológico daqueles que dominam o ciberespaço, que se utilizam da tecnologia e dos meios digitais como forma de subverter o seu uso tradicional, voltado para a concretização da agilidade e da eficiência na prática de atos em geral.

Na esteira desse pensamento, quando o Estado fica tolhido de fazer cumprir, em sua plenitude, atribuições constitucionalmente previstas, como se dá com o exercício da jurisdição, tal circunstância ganha maior relevo, haja vista ultrapassar a violação de direitos de um indivíduo, ou de uma coletividade específica. Nesse caso, dependendo da incursão sofrida, alcança-se o Estado como instituição.

A vulnerabilidade de sistema que gerencia atividades de um ente público denota que outros órgãos públicos também estão sujeitos a esse tipo de investida[5], o que coloca em risco questões fundamentais para o Brasil, seja no que se refere ao acesso a dados de relevância nacional, seja no que tange ao exercício das próprias

[4] Foi o que ocorreu em invasão realizada nos sistemas do Tribunal Regional Federal da 3ª Região, na qual houve alteração de documentos inclusos na plataforma do processo judicial eletrônico (PJE) (JUSTIÇA, 2021). Esse caso denota que os ataques cibernéticos têm sido cada vez mais audaciosos e com consequências cada vez mais graves.

[5] As instituições públicas, de forma geral, têm sido recorrentemente vítimas de ataques cibernéticos. Um dos mais recentes ocorreu no Ministério da Saúde, em 10 de dezembro de 2021, ocasionando a interrupção do funcionamento do sítio eletrônico e de outros diversos sistemas do mencionado órgão (PF, 2021).

funções estatais, que, em última análise, visam atender a necessidades de interesse público.

Essa questão deve ser ainda mais destacada pelo fato de que a aplicação da tecnologia para a realização de serviços públicos tem sido uma realidade cada vez mais contundente, havendo automação progressiva de tarefas no campo jurídico, com potencial utilização de métodos de *learning machines*. Tal contexto demonstra a necessidade de se levantar e aduzir não apenas o lado positivo dessa constatação, mas também o lado negativo que ela pode ensejar.

Toda essa discussão igualmente cogita a necessidade de se analisar o uso da tecnologia de forma ética e lícita, um dos principais desafios da sociedade da informação. Os avanços tecnológicos trouxeram importantes ferramentas para a atuação dos usuários, porém também permitem que elas sejam utilizadas para atingir negativamente um número indeterminado de pessoas e, mesmo, de instituições (BARRETO JÚNIOR; SPAREMBERGER, 2020), como acontece nos ataques cibernéticos aos tribunais brasileiros, de que se ocupa este trabalho.

A utilização de plataformas digitais e da *internet*, tendo em vista a rapidez na transmissão de dados e informações, a ausência de barreiras físicas para que tal ocorra e, principalmente, a dificuldade de identificação dos vestígios eventualmente deixados por uma atuação indevida nessa seara, é um meio atrativo para a prática delituosa.

Por óbvio, a utilização indevida das novas tecnologias não pode ser motivo para abandoná-las. Nem isso seria possível, uma vez que os ganhos havidos com sua aplicação são inumeráveis, inclusive como forma de se fazer concretizar a democracia e a cidadania (LÔBO; BOLZAN DE MORAIS; NEMER, 2020).

Em função disso, constata-se a necessidade premente e contínua de pesquisas, análises e aplicação de ferramentas voltadas para a segurança digital. Premente e contínua, porque, ao passo que se tem avanços nessa seara, também há progressos na criação e implementação de instrumentos voltados para o mau uso das tecnologias, que, aliás, têm se mostrado extremamente diversificados e com elevada sofisticação.

O governo federal tem buscado regulamentar as questões afetas à segurança necessária e exigida pela sistemática trazida pela aplicação das novas tecnologias, inclusive e principalmente no âmbito dos órgãos públicos.

A preocupação com essa temática mostrou-se mais determinante em 2015, quando então foi publicada a Portaria CDN nº 14, de 11 de maio daquele ano (CONSELHO DE DEFESA NACIONAL, 2015), por meio da qual foi homologada a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal, válida para os anos de 2015 a 2018. Tais setores foram considerados estratégicos, exigindo um planejamento contundente para aprimorar a segurança dentro da organização administrativa federal, inclusive em decorrência dos impactos gerados por tais questões na sociedade global.

O plano teve como objetivo principal evitar ingerências impróprias nos sistemas dos órgãos públicos, cuja utilização da tecnologia era crescente, como meio de facilitar o exercício das atribuições da Administração Pública. Justamente em decorrência do incremento no uso dos meios digitais, foi destacada a necessidade de proteção das plataformas públicas, inclusive em relação aos ataques cibernéticos, que, ao lado das fraudes e dos sequestros de dados, já vinham em curva ascendente de crescimento, não apenas no Brasil, mas em nível mundial.

Nesse contexto, a estratégia discriminou metas a serem alcançadas no período de sua vigência, no intuito de se garantir mecanismos de fortalecimento da segurança tecnológica e computacional, evitando e coibindo a utilização indevida dos meios digitais. Os intentos foram variados, sustentando-se em quatro pilares principais: orçamento; aprendizagem e capacitação dos agentes públicos; organização governamental para sua implementação, incluindo as bases legais necessárias para tanto; e, por fim, concretização das metas voltadas para atender as necessidades da sociedade. Tratou-se, portanto, de um planejamento global, para ser aplicado de forma específica em todas as esferas do governo federal.

Em 2018, foi instituída a Política Nacional de Segurança da Informação (PNSI) pelo Decreto nº 9.637, de 26 de dezembro daquele ano (BRASIL, 2018), por intermédio do qual restaram estabelecidas as diretrizes gerais e principiológicas a serem seguidas nessa seara.

Tal legislação estabeleceu um rol de dezesseis princípios que deveriam ser observados na estruturação dessa política, merecendo evidência a soberania nacional, a proteção aos direitos e garantias fundamentais, a troca de informações científicas e tecnológicas entre os órgãos públicos, a promoção da educação em segurança da informação, a necessidade de se pensar em medidas preventivas e

saneadoras dos problemas nessa área, bem como a integração entre o setor público e o setor privado, destacando-se neste último as instituições acadêmicas.

A rigor, a necessidade de se pensar em segurança na aplicação das novas tecnologias pelo Estado tem uma vinculação estrita com a proteção da soberania nacional, o que, aliás, se destacou linhas atrás quando se falava nos ataques cibernéticos contra o Judiciário. Os órgãos públicos são responsáveis pelo cumprimento de atribuições que posicionam o Brasil como um Estado soberano, com informações e dados de relevo nessa seara. Violações aos seus sistemas ou acesso indevido nessas bases configuram, por certo, negação a esse princípio, que tem previsão constitucional.

Por outro lado, quando se fala em segurança de informação, também é preciso que sejam resguardados direitos e garantias fundamentais, especialmente aqueles relacionados à privacidade dos indivíduos. Aqui se encontra um dos pontos mais conflitantes a respeito dessa temática, haja vista a necessidade de ponderação de princípios de elevada importância para a sociedade: a segurança, de um lado, e a privacidade, de outro.

Ademais, não se pode olvidar que as questões afetas à proteção de dados e sistemas demandam uma abordagem multidisciplinar e interorganizacional. O diálogo entre as instituições (entre si e com a sociedade, principalmente com as instituições acadêmicas) mostra-se fundamental para uma construção cada vez mais sólida dessa rede de segurança.

Igualmente, não se pode desconsiderar que a educação é bem essencial. O acesso e apropriação indevida de dados, como ocorreu com os tribunais brasileiros, podem ser mitigados com o conhecimento dos usuários do sistema acerca das ferramentas de proteção que podem ser utilizadas ou as condutas que não devem ser tomadas para que o sistema seja resguardado, como, por exemplo, evitar abrir arquivos enviados via *e-mail* dentro do sistema computacional.

Acrescente-se a necessidade de se pensar em medidas que não apenas possam enfrentar as intercorrências cibernéticas, mas, principalmente, estabelecer diretrizes que busquem evitar que elas ocorram, especialmente diante da devastação que podem gerar nas redes públicas, com prejuízos diretos aos vários setores da sociedade.

Nesse sentido, o Decreto nº 9.637/2018 delineia os objetivos da política nacional por ele instituída, todos com foco na segurança da informação, devendo

existir, como instrumentos para sua consolidação, a Estratégia Nacional de Segurança da Informação e os planos nacionais. A primeira deve abordar a forma de planejamento das ações a serem tomadas para a proteção dos sistemas e dos dados dos órgãos públicos; os segundos constituem um documento que contém a efetiva concretização dessas metas, como elas serão executadas e os recursos destinados para tanto.

Considerando os termos do mencionado decreto, em 05 de fevereiro de 2020 foi editado o Decreto n.º 10.222 (BRASIL, 2020), que estabeleceu a Estratégia Nacional de Segurança Cibernética (*E-ciber*), como um dos pontos da Estratégia Nacional de Segurança da Informação, considerado o ponto mais crítico. Nessa normativa foram estabelecidos os objetivos e as ações a serem concretizadas nesta área, com a demonstração da necessidade de alinhamento unificado sobre o assunto e a cooperação dos órgãos públicos e das instituições privadas em sua aplicação.

Há, ainda, na *E-ciber*, um diagnóstico do Brasil no que se refere à segurança cibernética. Nele se verifica que, não obstante encontrar-se o país em posição de destaque quanto ao mercado de telecomunicações e de possuir todas as instituições públicas em nível federal e estadual com acesso à *internet*, não há uma rede segura de utilização do espaço cibernético, estando o Estado brasileiro posicionado como um dos países que tiveram maiores danos decorrentes de investidas indevidas nessa área.

Essas estatísticas foram comprovadas na prática, por meio dos ataques cibernéticos sofridos por tribunais de envergadura constitucional, eis que, apesar da intensidade no uso das novas tecnologias por esses órgãos, não houve proteção suficiente para evitar o acesso não autorizado em seus sistemas.

O que se pode dizer, nesse contexto e a partir dessa e de outras experiências vividas por outros órgãos públicos no Brasil, é que, mesmo existindo iniciativas do Estado no sentido de se buscar consolidar uma estrutura de proteção em segurança da informação, ou as metas ficaram apenas em previsões normativas e documentadas, ou não foram elas suficientes para elidir a situação em análise, o que, de qualquer maneira, exige que sejam repensadas as condutas a serem adotadas daqui para frente.

Essa reflexão deve considerar que os riscos e problemas advindos do desenvolvimento científico são de proporções que, muitas vezes, superam limites territoriais e temporais, como decorrência da própria essência da sociedade da

informação. A evolução da tecnologia não vem desacompanhada dos perigos cada vez mais intensos e diversificados decorrentes de sua utilização indevida (DE JULIOS CAMPUZANO, 2018).

Nesse sentido, constata-se que a complexidade e a instantaneidade de mudanças dos meios tecnológicos e digitais, acrescidas da existência de múltiplos sistemas, todos interligados e em rede, denotam que as questões afetas à segurança cibernética estão longe de ser esgotadas. Na esfera pública, a exigência de um zelo maior é ainda mais premente, tendo em vista os reflexos gerados pela disrupção das plataformas dos órgãos estatais e, pior, da manipulação dos dados armazenados, haja vista os impactos nos serviços públicos de relevo, como o é a jurisdição, e, via de consequência, na sociedade como um todo. Os ataques cibernéticos a tribunais como o Supremo Tribunal Federal e o Superior Tribunal de Justiça servem de alerta.

CONSIDERAÇÕES FINAIS

A sociedade sempre esteve em constante evolução, disso não se olvida. Contudo, a partir dos avanços tecnológicos, o salto evolutivo dos vários setores sociais acontecem numa velocidade e intensidade até então não ocorridas, tornando-se exponencial.

No entanto, como verificado, a utilização da informática, da *internet* e dos meios digitais, ao mesmo tempo em que conferem agilidade nas relações interpessoais, com reflexos positivos na eficiência e rapidez na prática de atos em geral, possuem um lado negativo, consubstanciado na vulnerabilidade do funcionamento do sistema e do acesso a dados e informações de caráter particular e público.

Essa dualidade, própria da utilização das novas tecnologias, tem sido constatada no exercício da atividade jurisdicional. De um lado, o Judiciário encontra-se inserido, cada vez mais, no espaço cibernético, valendo-se das ferramentas tecnológicas para aumentar a produtividade nessa área, em um espaço curto de tempo. Contudo, ao utilizar-se de sistemas tecnológicos para o armazenamento e tratamento de dados sensíveis, o Estado avoca para si a responsabilidade de zelar por sua higidez e, mais, lhe é imposta a atribuição de evitar sua manipulação por práticas criminosas. Na realidade, não obstante as exigências que a própria legislação brasileira impõe para a concretização da segurança da informação, o que se tem visto é uma série de ataques cibernéticos aos principais tribunais do país.

Tais invasões mostraram o viés nocivo do uso das novas tecnologias. Processos paralisados, sessões de julgamento interrompidas e, o que é pior, a possibilidade de interferência nos dados armazenados e, ainda, o sequestro das informações existentes nas plataformas geridas por esses órgãos, são algumas das consequências decorrentes desses acessos cibernéticos indevidos.

Essa situação expõe a necessidade de se repensar questões afetas à segurança e, principalmente, o cuidado que se deve ter para que os direitos e garantias do indivíduo em particular, e da sociedade em geral, sejam sempre resguardados, de modo a não serem afetados pelo uso indevido dos instrumentos tecnológicos.

Essa preocupação deve ganhar destaque quando se aborda os impactos que essa situação pode gerar no exercício da atividade jurisdicional, que, concretizada dentro do processo, como espaço dialógico que é, tem como finalidade justamente assegurar que todas essas prerrogativas constitucionalmente previstas sejam, de fato, asseguradas, de modo a consolidar as próprias diretrizes do Estado Democrático de Direito.

Há que se perquirir, a par da constatação do domínio e uso do instrumental tecnológico a serviço da atividade jurisdicional, em que medida a implementação de direitos fundamentais se faz presente nessa ambiência, diante da constatação de uma imensa gama de pessoas que se encontra excluída do acesso a bens ainda mais básicos que a *internet*.

Por fim, resta em foco, cada vez mais intenso esse novo modelo de justiça algorítmica que deve ser inclusiva, plural e destinada à efetivação dos direitos fundamentais, para que a promessa constitucional de promoção do bem de todos não seja uma quimera.

REFERÊNCIAS

BARRETO JÚNIOR, Irineu Francisco; SPAREMBERGER, Raquel Fabiana Lopes. Ética e democracia na sociedade da informação. *In*: SARLET, Ingo Wolfgang; WALDMAN, Ricardo Libel. (Org.). **Direitos humanos e fundamentais na era da informação.** Porto Alegre: Fundação Fênix, 2020, p. 175-190.

BRASIL. **Lei n.º 11.419, de 19 de dezembro de 2006.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm. Acesso em: 12 mai. 2022.

BRASIL. **Lei n.º 13.105, de 16 de março de 2015**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 12 mai. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 mai. 2022.

BRASIL. **Decreto 9.637, de 26 de dezembro de 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm. Acesso em: 21 mai. 2022.

BRASIL. **Decreto 10.222, de 05 de fevereiro de 2020**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em: 21 mai. 2022.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/ConstituicaoCompilado.htm. Acesso em: 15 mai. 2022.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução n.º 345, de 09 de outubro de 2020.** Disponível em: https://atos.cnj.jus.br/atos/detalhar/3512. Acesso em: 19 mai. 2022.

CONSELHO DE DEFESA NACIONAL. **Portaria 14, de 11 de maio de 2015.** Disponível em: https://www.gov.br/gsi/pt-br/assuntos/noticias/2015/estrategia-de-seguranca-da-informacao-e-comunicacoes-sic-e-de-seguranca-cibernetica-da-administracao-publica-federal-apf. Acesso em: 14 mai. 2022.

DE JULIOS CAMPUZANO, Alfonso. Nuevos horizontes de los derechos humanos: la crisis de la modernidad jurídica en la sociedad tecnológica. **Revista de Direitos e Garantias Fundamentais.** v. 19, n. 3, set./dez. 2018, p. 11-46.

FRAZÃO, Ana. Decisões algorítmicas e direito à explicação. **Online**: 2021. Disponível em: http://www.professoraanafrazao.com.br/files/publicacoes/2021-11-24-Decisoes_algoritmicas_e_direito_a_explicacao_Em_que_medida_e_possivel_encontrar_explicacoes_em_decisoes_algoritmicas.pdf. Acesso em: 14 abr. 2022.

FUX diz que é preciso aprimorar segurança após ataques ao STJ e TSE. **Agência Brasil**, Brasília, 18 nov. 2020. Disponível em https://agenciabrasil.ebc.com.br/justica/noticia/2020-11/apos-ataques-ao-stj-e-tse-fux-diz-que-e-preciso-aprimorar-seguranca. Acesso em: 20 abr. 2022.

HACKERS atacam TRF-1, pegam dados e comemoram nas redes. **Estadão**, 27 nov. 2020. Disponível em: https://noticias.r7.com/brasil/hackers-atacam-trf-1-pegam-dados-e-comemoram-nas-redes-23082021. Acesso em: 20 abr. 2022.

IDEC; INSTITUTO LOCOMOTIVA. **Relatório de Pesquisa:** Acesso à Internet Móvel pelas Classes CDE. Instituto Brasileiro de Defesa do Consumidor e Instituto

Locomotiva. Nov. 2021. Disponível em: https://idec.org.br/sites/default/files/pesquisa_locomotiva_relatorio.pdf. Acesso em: 19 abr. 2022.

JUSTIÇA Federal condena hackers por falsificação de documento público em sistema processual. **Notícias Seção Judiciária do Mato Grosso do Sul**, 17 dez. 2021. Disponível em: https://web.trf3.jus.br/noticias-sjms/Noticiar/ExibirNoticia/48-justica-federal-condena-hackers-por-falsificacao-de. Acesso em: 25 mai.2022.

KAHNEMAN, Daniel; SIBONY, Olivier; SUNSTEIN, Cass R. **Ruído:** Uma falha no julgamento humano. Rio de Janeiro: Objetiva, 2021.

LÔBO, Edilene; BOLZAN DE MORAIS, José Luís; NEMER, David. Democracia algorítmica: o futuro da democracia e o combate às milícias digitais no Brasil. **Revista Culturas Jurídicas.** v.7, n. 17, mai./ago. 2020, p. 256-276.

MORAIS DA ROSA, Alexandre. A questão digital: o impacto da inteligência artificial no Direito. **Revista de Direito da Faculdade de Guanambi**, v. 06, n. 02, jul./dez. 2019, p. 1-18.

NUNES, Dierle. Virada tecnológica no Direito Processual e etapas do emprego da tecnologia no Direito Processual: seria possível adaptar o procedimento pela tecnologia? *In*: NUNES, Dierle; LUCON, Paulo Henrique dos Santos; WOLKART, Erik Navarro (Org.). **Inteligência artificial e direito processual.** Os impactos da virada tecnológica no direito processual. 2. ed. atual. e ampl. Salvador, Juspodivm, 2021, p. 17-54.

NUNES, Dierle; PEDRON, Flávio Quinaud; BAHIA, Alexandre. **Teoria geral do processo***.* Salvador: Juspodivm, 2020.

PÉREZ LUÑO, Antônio-Enrique. Los derechos humanos hoy: perspectivas y retos XXII Conferencias Aranguren Human Rights Today: Prospects and Challenges XXII Aranguren Lectures. **Isegoría. Revista de Filosofía Moral y Política.** n. 51, jul./dez. 2014, p. 465-544.

PF aponta que ataque hacker atingiu ministérios e mais de 20 órgãos do governo. **CNN**, 11 dez. 2021. Disponível em: https://www.cnnbrasil.com.br/nacional/pf-aponta-que-ataque-hacker-atingiu-ministerios-e-mais-de-20-de-orgaos-do-governo/. Acesso em: 19 abr. 2022.

RANSOWARE: entenda como o vírus é usado em extorsões e saiba como se proteger. **G1**, 23 jun. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/06/23/ransomware-entenda-como-o-virus-e-usado-em-extorsoes-e-saiba-como-se-proteger.ghtml. Acesso em: 14 abr. 2022.

REICHELT, Luís Alberto. Reflexões sobre o modelo do “Juízo 100% Digital” à luz do direito fundamental ao acesso à justiça. *In:* SARLET, Ingo Wolfgang; WALDMAN, Ricardo Libel. (Org.). **Direitos humanos e fundamentais na era da informação.** Porto Alegre: Fundação Fênix, 2020, p. 233-245.

SALMERÓN-MANZANO, Esther. Legaltech and Lawtech: Global Perspectives, Challenges, and Opportunities. **Laws**, v.10, n. 24, abr./2021, p. 01-09.

STF apura suspeita de ataque hacker e tira site oficial do ar. **Agência Brasil**, Brasília, 07 mai. 2021. Disponível em: https://agenciabrasil.ebc.com.br/justica/noticia/2021-05/STF-apura-suspeita-de-ataque-hacker-e-tira-site-oficial-do-ar. Acesso em: 19 abr. 2022.

TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. **Nota de Esclarecimento**, Porto Alegre, 11 nov. 2020. Disponível em: https://www.tjrs.jus.br/novo/noticia/nota-de-esclarecimento-3/. Acesso em: 20 abr. 2022.

WERTHEIN, Jorge. A sociedade da informação e seus desafios. **Ciência da Informação.** v. 29, n. 2, 2000, p. 71-77.