# A FRAGILIDADE DOS TRIBUNAIS BRASILEIROS E ATAQUES DE *RANSOMWARE*

Diego Souza Barreto[1 e 2]

Fernanda Ivo Pires[3]

**Resumo:** Atualmente, percebem-se grandes investimentos dos tribunais brasileiros com intuito de garantir maior celeridade aos seus processos. Ocorre, todavia, que a mesma preocupação não é observada quanto à segurança dos dados armazenados nestas instituições. Em recentes ataques, foi possível observar ações de *ransomware* em tribunais diversos, o que demonstra a fragilidade dos seus sistemas e desacordo com o quanto determinado pelas leis nacionais que visam a proteção de dados.

**Palavras-chave:** tribunais, *ransomware*, dados, LGPD

## 1. Introdução

Segundo o *site* de notícias sobre tecnologia, Tecmundo, a companhia de segurança e informação eslovaca, ESET, constatou que o Brasil é, atualmente, o quarto país da América Latina mais afetado pelo *ransomware*[4], programa mal-intencionado capaz de criptografar arquivos, inutilizando-os para o acesso do usuário e cobrando uma determinada quantia em criptomoedas para desbloqueá-los.

Uma das principais e mais perigosas famílias de *ransomware*, conhecida pelo codinome *Crysis*, se utiliza de *e-mails* falsos de cobrança de dívidas, muitas vezes se passando por empresas contratadas pela vítima, induzindo a pessoa clicar em *links* infectados. Mas não apenas os computadores pessoais são atacados, servidores de redes privadas de empresas e instituições públicas também sofrem desse mal.

---

[1] Graduado em Bacharelado em Direito. Analista Jurídico. E-mail: disobarreto@gmail.com.

[2] O presente artigo reflete uma adaptação do Trabalho de Conclusão de Curso promovido no curso de bacharelado em Direito no Centro Universitário Jorge Amado pelo, até então, graduando Diego Souza Barreto sob a orientação da Professora Doutora Fernanda Ivo Pires. O trabalho foi defendido em 02 jul. 2020.

[3] Doutora e mestre em Direito Civil pela PUC-SP. Professora universitária. Autora de obras jurídicas. Associada fundadora do IBERC. Advogada. E-mail: fipires@uol.com.br

[4] PAYÃO, Felipe. Brasil é um dos países mais afetados por ransomware na América Latina. *Tecmundo*, S.l., 2019. Disponível em: < https://www.tecmundo.com.br/seguranca/137884-brasil-paises-afetados-ransomware-america-latina.htm>. Acesso em: 21 set 2019.

Neste sentido, começam a surgir notícias de ataques a tribunais brasileiros, os quais se encontram em uma corrida por maior celeridade na tramitação dos seus processos; entretanto, estão muito aquém do que se espera em segurança e preservação de dados.

## 2. Informatização dos tribunais brasileiros

O Poder Judiciário brasileiro finalizou o ano de 2019 com 77,1 milhões de processos em tramitação, que aguardavam alguma solução definitiva.[5] Trata-se de um número muito alto, provocado por diversos fatores como alta litigiosidade, excesso de recursos etc.

O fato é que a quantidade de novas ações é inversamente proporcional ao volume de processos encerrados, o que resulta em enorme morosidade e profundas injustiças.

Na tentativa de reverter tal situação, chama-se a atenção para a aproximação do Poder Judiciário com as novas tecnologias. Obviamente que, em meio à avalanche tecnológica apontada pela revolução 4.0, o Direito não poderia passar ao largo de tamanhas transformações.[6]

Em recente estudo publicado pelo Conselho Nacional de Justiça (CNJ), percebe-se que, embora os gastos com investimentos em tecnologia, nos últimos anos, permaneçam estáveis, trata-se de vultosa quantia:

> A série histórica de gastos com informática apresentou tendência de crescimento entre os anos de 2009 e 2014 e se manteve estável, com sutis oscilações, nos últimos 5 anos. As despesas de capital apresentaram comportamento crescente entre os anos de 2009 a 2012, quando iniciou a tendência de queda, observada até 2015. Desde então, tais despesas têm se mantido relativamente estáveis, com elevação de 0,04% no último ano (Figura 23). Essas despesas abrangem a aquisição de veículos, de equipamentos e de programas de informática, de imóveis e outros bens permanentes, além das inversões financeiras.[7]

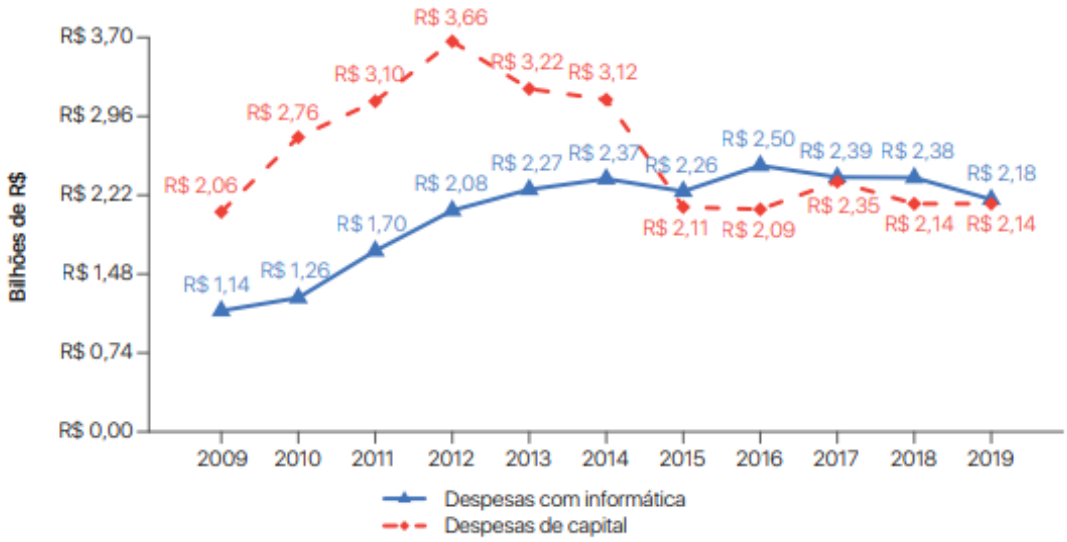
---

[5] CONSELHO NACIONAL DE JUSTIÇA. *Justiça em Números 2020*: ano-base 2019. Brasília: CNJ, 2020. Disponível em <https://www.cnj.jus.br/wp-content/uploads/2020/08/WEB-V3-Justi%C3%A7a-em-N%C3%BAmeros-2020-atualizado-em-25-08-2020.pdf>. Acesso em: 05 out. 2020.

[6] PIRES, Fernanda Ivo. Poder judiciário, inteligência artificial e efeitos vinculantes. In: Mafalda Miranda Barbosa; Felipe Braga Netto; Michel César Silva; José Luiz de Moura Faleiros Filho. (Org.). *Direito digital e inteligência artificial: diálogos entre Brasil e Europa*. 1ed. Indaiatuba: Foco, 2021, v. 1, p. 496.

[7] CONSELHO NACIONAL DE JUSTIÇA. Obra citada*Justiça em Números 2020*: ano-base 2019. Brasília: CNJ, 2020. Disponível em <https://www.cnj.jus.br/wp-content/uploads/2020/08/WEB-V3-Justi%C3%A7a-em-N%C3%BAmeros-2020-atualizado-em-25-08-2020.pdf>. Acesso em: 05 out. 2020.

Figura 23: Série histórica das despesas com informática e com capital




A aquisição tecnológica não se restringe à simples automatização de tarefas repetitivas ou à informatização do processo; traz, sobretudo, largo investimento em Inteligência Artificial.

Em pesquisas desenvolvidas pela Fundação Getúlio Vargas (FGV), por meio do Centro de Inovação, Administração e Pesquisa do Judiciário (CIAPJ), sob coordenação de Luis Felipe Salomão[8], é possível notar que se trata de números bastante significativos quanto à utilização de tecnologia pelos tribunais e, ainda mais, quando se refere a uma sofisticação maior como a Inteligência Artificial. [9]

Tais investimentos são louváveis, mas não se pode descuidar, em paralelo, de algo ainda mais sério, que é a segurança no armazenamento de dados de quase toda a população.

Infelizmente, ataques por *ransomware* vêm ocorrendo nos tribunais brasileiros, o que demonstra a enorme fragilidade nos seus sistemas e demandaria maior implemento de medidas de segurança. Ressalta-se, ainda, que, curiosamente, essas ofensivas vêm ocorrendo já sob a égide da Lei Geral de Proteção de Dados (Lei nº. 13.709/2018).

## 3. *Ransomware*

A sociedade brasileira vem se informatizando cada dia mais, movimento que se percebe nos tribunais, como visto supra. Por isso a necessidade de esclarecimento sobre as ferramentas

[8] Ministro do Superior Tribunal de Justiça.
[9] FUNDAÇÃO GETÚLIO VARGAS. Webinar - I Fórum sobre Direito e Tecnologia - 2020 (parte 1). Disponível em: <https://www.youtube.com/watch?v=LbVnv7a1wkU> Acesso em: 01 out 2020.

que estão a seu alcance. Não se espera que todos se especializem e aprofundem no tema, mas ao menos que se apercebam sobre riscos em potencial a que estão sujeitos e que a *internet* não pode mais ser compreendida como "terra de ninguém".

O uso de aparelhos eletrônicos como computadores, *smartphones*, *tablets*, *smartwatches*, dentre outros, em grande escala, tem sido uma realidade incontestável em todas as classes sociais, nas mais variadas culturas mundiais. Apesar de ser um assunto ainda considerado "novo", o uso da informática pelo grande público começou a surgir em 1977 com o notável sucesso da *Apple II*[10] e seu sucessor, o *Macintosh* (1984), computadores domésticos da Apple, que levariam a, até então, tecnologia utilizada por empresas e por militares, para dentro dos lares familiares.

Computador doméstico, computador pessoal ou, simplesmente, *PC* (*personal computer*), tornou-se cada vez mais um item comum nas residências familiares, chegando no Brasil na década de 1970, mas, ganhando maior popularidade nos anos 90. O computador, popularmente chamado, constitui uma interação entre dois elementos: a parte física, chamada de *hardware*, e a parte virtual, denominada *software*.

A importância conceitual tanto do *hardware*, quanto do *software*, serve para identificar onde o programa malfeitor irá atacar e a maneira como age. O programa infectado encontrar-se-á armazenado tanto no HD, quanto na memória RAM, enquanto a máquina estiver em atividade. É importante, neste momento, dizer que, o dano causado pelo *Ransonware* não interfere fisicamente na máquina. Ou seja, o HD e a memória RAM não serão diretamente afetados, mas estarão virtualmente infectados, impossibilitando seus usos até que o sistema operacional (SO) venha a ser formatado. Todos os dados ali contidos, entretanto, não poderão ser recuperados.

## 3.1. Conceito

O que muito se chama de vírus, na verdade, trata-se apenas de uma das espécies de programas mal-intencionados, conhecidos por *malwares*, que se utilizam de diversos métodos e finalidades para prejudicar, de alguma forma, o usuário da rede mundial de computadores.

[10] ZAMBARDA, Pedro. Apple faz 37 anos; conheça a história da empresa criada por Steve Jobs. TechTudo, 2016. Disponível em: <https://www.techtudo.com.br/artigos/noticia/2013/04/apple-faz-37-anos-conheca-historia-da-empresa-criada-por-steve-jobs.html>. Acesso em: 07 mar. 2020.

O *ransomware* é um *software*[11] e, portanto, é um conjunto de códigos, de programações, que forma um aplicativo que será executado em tela, utilizando-se dos recursos de *hardware* do computador (CPU, memória RAM, HD / SSD) para seu funcionamento. É um *software* de fim, ou seja, necessitará de um sistema operacional instalado na máquina para executá-lo em tela. Ademais, o *ransomware* é uma espécie de *malware*; portanto, é um *software* malicioso / mal-intencionado, utilizado para atacar um computador, seja ele um computador pessoal, um servidor ou até uma rede compartilhada, atacando diversos computadores ao mesmo tempo.

O *ransomware* age como um "sequestrador" de dados. Ao ser executado no computador, criptografa todos os arquivos contidos na máquina, deixando-os inutilizáveis e, após, apresentará uma tela informando o que está acontecendo com a máquina e que o usuário somente poderá ter seus documentos de volta caso pague uma certa quantia (geralmente em criptomoedas) e informar sobre o pagamento através de um *e-mail* (supostamente impossível de rastrear) fornecido pelo(s) malfeitor(es).[12]

Apesar de ser um *malware* conhecido publicamente há poucos anos, o *ransomware* já existia há um considerável tempo, porém, somente criptografando arquivos. Com a popularidade das moedas digitais, entre elas, a *bitcoin*, passou-se a pedir um resgate para que a máquina voltasse ao seu *status quo*. Surgiu, então, a mais conhecida espécie de *ransomware*, que é a *Ransomware Petya*.

Segundo Jônatas Siqueira de Araujo, a *Petya* passou a surgir em meados de 2017 na Europa, tendo o seu primeiro ataque na Ucrânia, com mais de 12.500 máquinas infectadas, espalhando-se por mais de 64 países. O *malware* chegou ao Brasil no mesmo ano, sendo o ataque mais famoso ocorrido no Hospital do Câncer de Barretos, interior de São Paulo, interrompendo alguns processos assistenciais por quase uma semana, provocando dificuldades nos atendimentos aos pacientes após ter sofrido um ataque de *ransomware* e ter perdido importantes dados que promoviam sua operação.[13]

---

[11] *Software* pode ser entendido como "tudo aquilo que se vê em tela". Seria como um conjunto de direcionamentos que servem para dizer o que o computador deve fazer ou, ainda, um conjunto de linguagens ou códigos que formam a programação de uma determinada tarefa, seja de meio ou de fim, através de puro raciocínio lógico, de verdadeiro ou falso, de sim ou não, de 0 ou 1. (GOMES FILHO, Antônio Costa; FERREIRA, Marcus Vinícios; MACEDO, Michael Kramer Borges de; IGARASHI, Wagner; TODESCO, José Leomar. Importância do Hardware e Software em Organizações Ligadas ao Governo Eletrônico. *Revista Capital Científico*. Guarapuava – PR, v.6, n.1, 2008, p. 127-144. Disponível em: https://revistas.unicentro.br/index.php/capitalcientifico/article/view/807. Acesso em: 01 mar. 2020)

[12] ARAÚJO, Jônatas Siqueira de. *Malware*. 1ª ed. São Caetano do Sul: Perícia Digital. 2018. Ebook. ISBN: 978-85-921322-1-7. Disponibilizado pela Amazon Kindle Unlimited.

[13] COSSETTI, Melissa Cruz. Petya já chegou ao Brasil, novo ramsonware lembra caos do WannaCry. *TechTudo*. 2017. Disponível em: https://www.techtudo.com.br/noticias/2017/06/petya-ja-chegou-ao-brasil-novo-ramsonware-lembra-caos-do-wannacry.ghtml. Acesso em: 05.04.2020.

Além desse, existem diversos outros tipos de *ransomware*: *Locky*, *WannaCry*, *Bad Rabbit*, *Ryuk*, *Troldesh*, *Jigsaw*, *CryptoLocker*, *GoldenEye*, *GrandCrab*, dentre outros.

Algumas precauções no sentido de evitar o ataque podem ser tomadas, como manter o sistema operacional sempre atualizado, ter um bom *software antimalware* instalado no computador e fazer a limpeza virtual da máquina regularmente, mas, o mais importante, é o usuário estar sempre atento ao que acessa na *web*, bem como os dados que baixa através dela. No caso dos tribunais e órgãos públicos em geral, políticas sérias precisam ser implementadas, desde treinamento de pessoal a investimento em equipamentos e em mão de obra especializada.

Às vezes, uma simples imagem baixada, poderá conter um *ransomware* escondido em seus metadados e, se a máquina for conectada a outras, em rede, ou, em se tratando de um servidor de um tribunal, por exemplo, poderá infectar todas as outras máquinas em cadeia.

## 3.2 Ataques a tribunais brasileiros

Em novembro do ano de 2020, o Superior Tribunal de Justiça foi invadido por um *ransomware*, possivelmente um *RansomExx*, outra variante, o que ocasionou grande preocupação com os dados pessoais dos cidadãos, segurança dos processos e certamente danos reflexos que ainda podem ocorrer:

> Como medida de precaução, o acesso do tribunal à internet foi derrubado, "o que implicou no cancelamento das sessões de julgamento e impossibilitou o funcionamento dos sistemas de informática e de telefonia da Corte". Desde então, a equipe de tecnologia do STJ vem trabalhando para recuperar os arquivos criptografados, incluindo a ajuda do Centro de Defesa Cibernética do Exército Brasileiro, da Microsoft e de outras empresas que prestam serviços de tecnologia para a corte.[14]

Situação semelhante se observou no Tribunal de Justiça do Rio Grande do Sul, no qual, em 28 de abril de 2021, foi constatada a invasão:

> De acordo com o BleepingComputer, que recebeu capturas de tela de conversas entre funcionários do tribunal, o TJ-RS foi infectado com um ransomware REvil que criptografou dados do servidor e dos funcionários, interrompendo sistemas eletrônicos

[14] CARVALHO, Lucas. RansomExx: vírus que atingiu STJ também atacou TJ-PE e outros países. Disponível em https://www.uol.com.br/tilt/noticias/redacao/2020/11/07/ransomexx-virus-que-atingiu-stj-tambem-atacou-tj-pe-e-outros-paises.htm. Acesso em: 10 jun 2021.

> além de ter forçado o tribunal desligar sua rede, por precaução. Os cibercriminosos estão pedindo U$ 5 milhões (R$ 27 milhões) pelo resgate dos dados criptografados.
> O grupo REvil, responsável pelo ransomware que atingiu o tribunal, oferece o malware no formato de Ransomware as a Service (RaaS). Ou seja, o malware pode ser "alugado" para outras pessoas, interessadas em comprometer determinada empresa. Após um ataque bem-sucedido, os desenvolvedores do REvil e a pessoa que alugou seus serviços dividem o valor do resgate.[15]

Pode-se perceber, infelizmente, que a velocidade com que os *malwares* vêm se desenvolvendo e sofisticando ultrapassam sobremaneira um possível contra-ataque ou quiçá estudos que viabilizem a blindagem dos sistemas pelos tribunais brasileiros.

## 4. Influxos do Marco Civil da *Internet* e da Lei Geral de Proteção de Dados

Diante de toda esta perspectiva de fragilidade dos sistemas de armazenamento de dados pelos tribunais, cabe o questionamento de como operacionalizar os tão caros direitos resguardados pelo Marco Civil da *Internet* (Lei n. 12.965/2014), pela Lei Geral de Proteção de Dados (Lei n. 13.709/2018) e, obviamente, pela Constituição Federal.

O *ransomware*, dentre outros preceitos, fere a inviolabilidade do sigilo de dados; a neutralidade; a preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas [16, 17 e 18].

---

[15] PETRY, Guilherme. TJ-RS é vítima do ransomware REvil. Gangue pede U$ 5 milhões pelo resgate. Disponível em https://thehack.com.br/tj-rs-e-vitima-do-ransomware-revil-gangue-pede-u-5-milhoes-pelo-resgate/ Acesso em: 10 jun 2021.

[16] CF: art. 5. "XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;".

[17] Marco Civil da Internet: "Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei; IV - preservação e garantia da neutralidade de rede; V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei; VII - preservação da natureza participativa da rede; VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei. Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte."

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

De antemão, é possível afirmar que algumas indagações, por ora, permanecerão sem reposta e demandarão uma solução internacional, ultrapassando a simples eficácia das mencionadas leis, haja vista que os ataques, em sua maioria, são oriundos de outros países.

No emblemático caso do STJ, o tribunal garantiu que havia *backup* de todos os dados e, dessa forma, a integridade dos processos em trâmite estariam assegurados. No entanto, os problemas advindos por invasões desta natureza vão muito além do que o simples trâmite processual, são dados pessoais vazados e que, muitas vezes, referem-se a dados sensíveis[19], o que é ainda mais grave. Por outro lado, eventual pagamento de resgate, não afasta a possibilidade de vazamento dos dados.

Em importante consideração:

> O que mais impressiona no ataque ao STJ é que justamente uma das instituições mais importantes para o funcionamento do Judiciário brasileiro e mais experientes no campo da digitalização se revelou despreparada para lidar com um problema que já tem vários anos de vida. Já em 2017, quando o ransomware WannaCry causou danos milionários em todo o globo, tribunais brasileiros e outros órgãos públicos foram atingidos, ainda que em menor escala. Hoje, o Brasil é líder global em número de empresas atacadas por ransomware durante a pandemia. Ciberataques desse tipo não são novos no país e as estratégias de prevenção já deveriam estar difundidas. [20]

Socialmente, o que mais se espera é que as normas em comento sejam, em primeiro lugar, aplicadas e operacionalizadas pelos próprios órgãos julgadores de demandas relacionadas à proteção de dados.

## 5. Considerações finais

Novas tecnologias são sempre muito bem-vindas, desde que usadas em prol do bem comum, urgindo um esforço conjunto no sentido de combater pessoas mal-intencionadas.

Ataques de *ransomware* têm se mostrado uma prática constante e que põem em risco os mais sagrados direitos do ser humano. Neste sentido, infelizmente, os tribunais brasileiros vêm demonstrando uma enorme fragilidade em seus sistemas, o que proporciona inúmeras investidas maléficas.

---

[19] LGPD, Art. 5°: "II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;".

[20] SALVADOR, João Pedro Favaretto; GUIMARÃES, Tatiane. O ataque ao STJ é mais um grito de socorro da segurança cibernética no Brasil. Disponível em https://portal.fgv.br/artigos/ataque-ao-stj-e-mais-grito-socorro-seguranca-cibernetica-brasil. Acesso em: 10 jun. 2021.

Na busca por eficácia das normas de proteção de dados, é preciso repensar a que custo de busca uma corrida por informatização, não podendo se descuidar da essencial segurança jurídica.

**Referências bibliográficas**

ARAÚJO, Jônatas Siqueira de. ***Malware***. 1ª ed. São Caetano do Sul: Perícia Digital. 2018. Ebook. ISBN: 978-85-921322-1-7. Disponibilizado pela Amazon Kindle Unlimited.

CARVALHO, Lucas. **RansomExx: vírus que atingiu STJ também atacou TJ-PE e outros países**. Disponível em https://www.uol.com.br/tilt/noticias/redacao/2020/11/07/ransomexx-virus-que-atingiu-stj-tambem-atacou-tj-pe-e-outros-paises.htm. Acesso em: 10 jun 2021.

**CONSELHO NACIONAL DE JUSTIÇA**. Justiça em Números 2020: ano-base 2019. Brasília: CNJ, 2020. Disponível em https://www.cnj.jus.br/wp-content/uploads/2020/08/WEB-V3-Justi%C3%A7a-em-N%C3%BAmeros-2020-atualizado-em-25-08-2020.pdf. Acesso em: 05 out. 2020.

COSSETTI, Melissa Cruz. **Petya já chegou ao Brasil, novo ramsonware lembra caos do WannaCry.** ***TechTudo***. 2017. Disponível em: https://www.techtudo.com.br/noticias/2017/06/petya-ja-chegou-ao-brasil-novo-ramsonware-lembra-caos-do-wannacry.ghtml. Acesso em: 05.04.2020.

FUNDAÇÃO GETÚLIO VARGAS. **Webinar - I Fórum sobre Direito e Tecnologia** - 2020 (parte 1). Disponível em: <https://www.youtube.com/watch?v=LbVnv7a1wkU> Acesso em: 01 out 2020.

GOMES FILHO, Antônio Costa; FERREIRA, Marcus Vinícios; MACEDO, Michael Kramer Borges de; IGARASHI, Wagner; TODESCO, José Leomar. **Importância do Hardware e Software em Organizações Ligadas ao Governo Eletrônico.** ***Revista Capital Científico***. Guarapuava – PR, v.6, n.1, 2008, p. 127-144. Disponível em: https://revistas.unicentro.br/index.php/capitalcientifico/article/view/807 Acesso em: 01 mar. 2020.

PAYÃO, Felipe. **Brasil é um dos países mais afetados por ransomware na América Latina**. Tecmundo, S.l., 2019. Disponível em: https://www.tecmundo.com.br/seguranca/137884-brasil-paises-afetados-ransomware-america-latina.htm. Acesso em: 21 set 2019.

PETRY, Guilherme. **TJ-RS é vítima do ransomware REvil. Gangue pede U$ 5 milhões pelo resgate**. Disponível em https://thehack.com.br/tj-rs-e-vitima-do-ransomware-revil-gangue-pede-u-5-milhoes-pelo-resgate/. Acesso em: 10 jun 2021.

PIRES, Fernanda Ivo. **Poder judiciário, inteligência artificial e efeitos vinculantes**. In: Mafalda Miranda Barbosa; Felipe Braga Netto; Michel César Silva; José Luiz de Moura Faleiros Filho. (Org.). *Direito digital e inteligência artificial*: diálogos entre Brasil e Europa. 1ed. Indaiatuba: Foco, 2021, v. 1.

SALVADOR, João Pedro Favaretto; GUIMARÃES, Tatiane. **O ataque ao STJ é mais um grito de socorro da segurança cibernética no Brasil**. Disponível em https://portal.fgv.br/artigos/ataque-ao-stj-e-mais-grito-socorro-seguranca-cibernetica-brasil. Acesso em: 10 jun 2021.

ZAMBARDA, Pedro. **Apple faz 37 anos; conheça a história da empresa criada por Steve Jobs**. TechTudo, 2016. Disponível em: https://www.techtudo.com.br/artigos/noticia/2013/04/apple-faz-37-anos-conheca-historia-da-empresa-criada-por-steve-jobs.html. Acesso em: 07 mar 2020.