A SOCIEDADE DA INFORMAÇÃO E SEUS DESAFIOS: A NECESSIDADE DE EFETIVAÇÃO DE UMA POLÍTICA PÚBLICA DE COMBATE AO *RANSOMWARE* NO BRASIL

THE INFORMATION SOCIETY CHALLENGE'S: THE NEED TO IMPLEMENT A PUBLIC POLICY AGAINST RANSOMWARE IN BRAZIL

Felipe Rangel da Silva;[1]

Rodrigo Giublin Teixeira.[2]

Resumo: Pelo presente estudo se busca por meio de pesquisa bibliográfica em doutrina e jornais, bem como análise crítica de diplomas normativos pertinentes, demonstrar a necessidade de implementação no Brasil de uma política pública específica de combate ao *ransomware*, prática de sequestro de dados informáticos internacionalmente popularizada a partir de janeiro de 2016, da qual inúmeras instituições foram vítimas, expondo pessoas e promovendo o pagamento de resgastes por todo o mundo. A contextualização do cenário da Sociedade da Informação será feita para elucidar quanto às novas demandas inerentes à nova organização social, para qual novos desafios surgem acompanhando cada inovação tecnológica, demonstrando que a segurança na rede significa efetivação de um direito fundamental de segurança pública, vez que por meio dela se opera, nos dias de hoje, o desenvolvimento pleno da pessoa, dada a imprescindibilidade da internet para realização das mais diversas atividades humanas. Também será feita análise quanto ao cotejo legislativo atual, desmistificando a ideia de uma possível já previsão legal da prática do *ransomware*, além de se demonstrar que muito além da simples existência da norma, é mais do que necessário a implementação de medidas eficazes para minimização dos efeitos da prática no Brasil, sendo necessário o ingresso imediato do problema na agenda política do país.

Palavras-chave: *Ransomware*. Sociedade da Informação. Política Pública. Segurança digital.

Abstract: By the present study, using a bibliography research at doctrine and jornals, as well by a chritical against applicable law, that will be show the need to implement a specific public policy against ransomware, pratice that made popularized in 2016 january and where is made the kidnapping of data, making a lot of victims around the world. It will be contextualized the Information Society specificities to show the new demands of this new society organization,

[1] Mestre em Ciências Jurídicas pelo Centro Universitário Cesumar - UNICESUMAR. Pós-graduado lato sensu em Direito do Trabalho e Previdenciário pelo Instituto Brasileiro de Direito Constitucional e Cidadania de Londrina em convênio com a Universidade Estadual Norte Pioneiro. Pós-graduado lato sensu em Direito e Processo Civil pelo Instituto Paranaense de Ensino em Maringá. Graduado em Direito pela Faculdade Maringá.

[2] Doutor em Direito das Relações Sociais - Direito Processual Civil - pela Pontifícia Universidade Católica de São Paulo (PUC/SP) (2009/2012). Mestre em Direito Negocial, com concentração em Direito Processual Civil, pela Universidade Estadual de Londrina (UEL) (2003/2004). Especialista em Direito Civil e Processual Civil pelo Instituto Paranaense de Ensino (IPE/OAB) (2002/2003). Graduado em Direito pelo Centro Universitário de Maringá (CESUMAR) (1997/2001).

Artigo recebido em 11/03/2019 e aprovado para publicação em 30/05/2019.

where new challenges comes with ever new technology advance are made, putting the internet security as a fundamental right developed by the public security, because by the using of internet is made the human action on this days. It will be made the analyzis of actual legislation, concluding that there is not exist specific law against ransomware pratice in Brazil, and even that exist, this don't mean that the problem is solved, so it have been necessary the implemantation of effect actions to neutralized the problem in Brazil with a specific public policy.

Keywords: Ransomware. Information Society. Public policy. Digital security.

1 INTRODUÇÃO

As novas tecnologias que surgem e se popularizam em uma velocidade antes inimaginável em razão da propagação imediata da informação, decorrente principalmente da internet, produzem impacto jurídico relevante para o qual o Direito ainda não provê de mecanismos suficientes a absorvê-lo e regulamentá-lo de forma a não prejudicar seu pleno funcionamento. Utilizando de pesquisa bibliográfica em doutrina correspondente e jornais que comprovam os fatos suscitados, bem como por meio de uma análise crítica à legislação já existente no país, buscar-se-á demonstrar como tais alterações influenciam o cotidiano brasileiro, bem como as medidas que devem ser adotadas pelo governo no que tange à efetivação de uma política pública de combate ao *ransomware*,[3] em específico.

O impacto tecnológico se dá nas diversas áreas do Direito, tendo a presente pesquisa, por sua vez, foco na obrigação estatal na proporcionalização de segurança aos usuários da rede mundial de computadores, haja vista o surgimento do assim designado *ransomware* (que pode ser, grosso modo, traduzido como o sequestro de dados na internet). Por tal conduta, criminosos digitais têm feito vítimas (pessoas físicas, pequenas e grandes corporações) no mundo todo, com ataques de escala mundial a partir do ano de 2016. Tradicionais empresas já foram vítimas dessa conduta, redes sociais e até mesmo estúdios da indústria cinematográfica, dentre outros.

Por estarmos diante de uma nova era, assim designada por muitos como a era digital, de novos adventos como o *ransomware* surge a necessidade de regulamentação de matérias até então inimagináveis. Não que a segurança da rede seja tão somente agora discutida, mas o surgimento desse tipo de ataque (ainda mais diante da importância das corporações e pessoas políticas atingidas) intensificou mundialmente a discussão sobre o tema. Assim, é necessário ambientar o cenário em que o problema se origina: a Sociedade da Informação. Conceituada

[3] Em tradução livre está associado a uma modalidade de sequestro.

pelos estudiosos da sociologia, ela é terra fértil para o surgimento (cada vez mais acelerado) de questões dantes inimagináveis. Isto porque nela o centro de toda geração de riqueza deixa de ser a produção industrial e passa a ser o acesso, guarda e capacidade de tráfego da informação, revelando-se esta última o verdadeiro ouro do século XXI.

No bojo destas novas realidades sociais, é possível conjecturar a segurança na internet como direito fundamental decorrente da segurança pública, de modo que se tem no uso da internet uma ferramenta de desenvolvimento humano, revelando-se a ausência de acesso ou a falta de segurança no uso, em análise última, inegável ofensa aos direitos da personalidade.

Portanto, passa a ser a inclusão da questão na pauta das políticas públicas medida que se impõe, haja vista que, por meio da apresentação das fases e de sua teoria, o combate ao *ransomware* (inerente à segurança digital) é demanda do Estado, a fim de se fazer cumprir tal obrigação por meio da instituição de uma política pública específica, a ser desenvolvida em duas vertentes: a educação digital e a repressão aos ilícitos perpetrados por meio da internet.

2 A SOCIEDADE DA INFORMAÇÃO

Já não mais vivemos as mesmas condições, tanto sociais quanto econômicas e culturais, de nossos país. Até então sem qualquer problema, eis que desde muito tempo (talvez sempre) assim o fora com a humanidade. Contudo, algo torna nossa vivência nestes dias muito especial, para se dizer o mínimo. E o grande motim dessa diferenciação para as sociedades anteriores está na velocidade da mutação social.

Os paradigmas levavam décadas a serem quebrados e assim então constituídas novas ideias e novos pensamentos, o que ocorre atualmente em tempo demasiadamente curto (até mesmo em dias).

Como todos escrevem e já é praticamente de conhecimento popular, o que caracteriza a convencionalmente denominada Sociedade da Informação é a assunção desta (informação) como obra-prima da obtenção (ou manutenção) de poder, ou seja, é ela caracterizada pelo poderio econômico, social e principalmente político que possui aquele capaz de dominá-la, criando ou fazendo circular conteúdo.

Sociedade da Informação (ou Sociedade do Conhecimento ou Nova Economia) é um termo que surgiu no fim do século XX em decorrência da globalização, determinando-a como um modelo novo de organização social no qual a informação, como principal fonte de conhecimento, acaba por determinar a produção e distribuição (acumulação) de riqueza, influindo também nas condições de bem-estar social, vez que o acesso a tais passa a ser

preponderante para o desenvolvimento da pessoa, já que todas as suas atividades (laborais, sociais e de lazer) estão inseridas no contexto do fluxo informacional e dependente de dispositivos tecnológicos (PEZZELLA; BUBLITZ, 2014, p. 22).

Por sua vez, Paulo Hamilton Siqueira Junior assim define a chamada sociedade da informação:

> A sociedade da informação é constituída em tecnologias de informação e comunicação que envolve a aquisição, o armazenamento, o processamento e a distribuição da informação por meios eletrônicos, como rádio, televisão, telefone e computadores, entre outros. Essas tecnologias não transformam a sociedade por si só, mas são utilizadas pelas pessoas em seus contextos sociais, econômicos e políticos, criando uma nova estrutura social, que tem reflexos na sociedade local e global, surgindo assim a sociedade da informação. (SIQUEIRA JUNIOR, 2012, p. 236)

Vê-se, já em sua conceituação, que as tecnologias não representam fator de alteração social por si só. Em verdade são inseridas na vida das pessoas à medida que estas assim a consideram como potencializadoras de alguma atividade humana, como estudo, atividade física, lazer etc. Em outros termos, não é a tecnologia em si que muda o comportamento social, mas sim a adoção dela pela sociedade como ferramenta de desenvolvimento humano.

O paradigma social que se vive hoje decorre da implementação de novas tecnologias de informação desenvolvidas nas últimas décadas, que estão a mudar a forma com que se dão os relacionamentos. O resultado final dessas transformações não é apenas uma consequência do surgimento da tecnologia, mas sim a interdependência destas e os modelos econômico e social. Assim "as tecnologias não são em si mesmas um elemento determinante. Mas abrem um leque de possibilidades de apropriação, tanto ao nível individual como ao nível social, que condicionam a utilização das tecnologias ao mesmo tempo que são condicionadas por elas" (MORENO, 2015, p. 4).

De observar-se, neste sentido, o grande número de empresas chamadas *startups*[4] e seu destaque mundial, como o reconhecidamente polo localizado no Vale do Silício (São Francisco, Califórnia). Por elas são desenvolvidas um número inimaginável de novas tecnologias e aplicativos, porém, somente àqueles dispositivos ou programas que ajudam no

[4] Do inglês, em tradução literal *startup* significa "iniciantes". É o conceito que determina aquelas pequenas empresas que buscam desenvolver uma ideia de produto ou serviço inovadora. Destacaram-se recentemente pela indústria de aplicativos para *smartphones*, mas não se limitam a isto. Estão em destaque no campo da robótica, medicamentos, equipamentos médicos e indústria em geral. Para Andreia Cristina Dullius e Paola Rucker Schaeffer "Startups são consideradas empresas nascentes de base tecnológica, que possuem na inovação tecnológica disruptiva os fundamentos de sua estratégia competitiva. Entre as principais características de tais negócios estão o caráter de organização temporária com potencial de rápido crescimento, os quais atuam em um ambiente de extrema incerteza, em busca de um modelo de negócios que possa tornar-se repetível e escalável". (DULLIUS; SCHAEFFER, 2016, p. 36).

desenvolvimento de alguma atividade humana (laboral, de lazer, familiar) é que têm o projeto continuado, com investimento de capital e colocação no mercado consumidor.

A partir de então, ou seja, a partir do momento em que determinada tecnologia passa a ser adotada pela pessoa como potencializador de alguma atividade humana é que podemos verificar a influência existente no comportamento humano, não sendo apenas a criação da tecnologia fator de desenvolvimento ou interferência comportamental.

Desse fato, muitos apontamentos são merecedores de serem feitos, especialmente no campo da antropologia.

Manuel Castells é, sem dúvida, referência por ter analisado esta sociedade com maior profundidade, e, no que chamou de Paradigma da Tecnologia da Informação, apresenta cinco características preponderantes para o reconhecimento e emancipação de uma dita Sociedade da Informação.

Primeiramente, destaca a posição da informação como matéria-prima de modo que "são tecnologias para agir sobre a informação, não apenas informação para agir sobre a tecnologia, como foi o caso das revoluções tecnológicas anteriores" (CASTELLS, 2005, p. 78). Aqui há de se destacar que o autor enumera esta como a principal razão pela qual se justifica a nomeação de verdadeira sociedade da informação e não ser possível vê-la apenas como mais uma fase da revolução industrial.

Em segundo lugar, o que caracteriza a sociedade da informação é a penetrabilidade dos efeitos das novas tecnologias na vida individual e coletiva, de modo que há grande inferência no modo de vida a cada criação tecnológica. Em terceiro, destaca a lógica de redes, pela qual a informação pode chegar a todos, de forma distribuída. A quarta característica apontada pelo autor é a flexibilidade inerente a este sistema de redes, pela qual é possível a alteração de conteúdo e também da estrutura da tecnologia, ou seja, sua mutabilidade perene (CASTELLS, 2005, p. 78).

Por fim, outra característica da sociedade da informação influenciada pela revolução tecnológica seria a integralidade das novas tecnologias, ou seja, a possibilidade de comunicação e ligação entre os vários dispositivos, de modo que cada vez mais os dispositivos físicos são melhorados e em complemento melhorados também os programas e meios de comunicação (ibid., p. 79).

Verifica-se, portanto, características muito peculiares e determinantes para o reconhecimento de uma verdadeira sociedade tecnológica diferente da anteriormente posta, caracterizada pela produção industrial. O desenvolvimento destas características faz surgir um comportamento social que sem sombra de dúvida rompe com o panorama pretérito.

A divisão do dia em oito horas de trabalho, oito de lazer e oito de descanso implementada a partir da otimização da produção industrial – evidentemente após as lutas e conquistas sociais que assim delimitaram o tempo de trabalho, a existência de finais de semana e outros benefícios – sofre atualmente uma quebra de paradigma. Isso porque a massa mais nova de trabalho, já nascida dentro da popularização da internet, tem suas próprias características e uma delas é a mescla de atividades e interconectividade perene, de modo que ao mesmo tempo em que trabalham, também veem um vídeo ou uma foto nas redes sociais e resolvem coisas do trabalho em casa e vice-versa, também se divertindo (NASBITT; NASBITT; PHILIPS, 2006, p. 51-54).

Isto é apenas um exemplo de mutabilidade social que justifica a ruptura da sociedade atual, dita da informação, com o modelo implementado pela produção industrial.

Importante retrato do contexto em que se pode verificar a mudança de paradigma social a possibilitar a constatação desta nova sociedade da informação é traçado por Paulo Hamilton Siqueira Junior, no sentido de que:

> De uma perspectiva mais concreta, a sociedade da informação é posterior ao pós-modernismo, e passou a se desenvolver a partir da década de 80, gerando um ambiente marcado pela globalização, neoliberalismo, desregulamentação, Estado mínimo, privatizações, delegação de funções estatais a agências reguladoras e outras instituições estruturadas no modelo empresarial, poder difuso compartilhado por poderes locais, regionais e estruturas continentais em rede, dentre outros pontos importantes.
> A expressão sociedade da informação é entendida no contexto dessa sociedade pós-industrial, no que ela representa de qualitativamente relacionado à informação. Isso significa que não engloba toda a sociedade contemporânea, na medida em que muitas regiões e populações estão hoje excluídas do ambiente informacional, mas sim aquele setor dominante do mundo globalizado, o qual se caracteriza pela informação, comunicação e pelo domínio da tecnologia de ponta (SIQUEIRA JUNIOR, 2012, p. 238).

Como se viu, a internet é, portanto, peça fundamental para o desenvolvimento da dita Sociedade da Informação.

Ao que denomina de Geração da Internet (os nascidos já após a popularização da internet nos anos 1990), Don Tapscott em seu livro *A Hora da Geração Digital* aponta oito características inerentes aos pertencentes desta geração: i) liberdade (de consumo, de trabalho, de relacionamento); ii) customização de bens e serviços para adequação à realidade social inserida; iii) escrutínio (sabem diferenciar, mediante investigação particular na própria rede, notícias e fatos verídicos de inverídicos); iv) integridade (estão engajadas com problemas sociais e buscam associação, ainda que on-line, para resolução de questões humanitárias); v) colaboração (pensam em soluções que são compartilhadas a todos, em escala global); vi)

entretenimento (a produção laboral é influenciada pela criação de ambientes atrativos, com jogos e intervalos recreativos, inexistindo a divisão clássica de tempo do dia para trabalhar e tempo do dia para descansar e se divertir, ambos ocorrem simultaneamente); vii) velocidade (em razão da velocidade existente na internet, de respostas e comunicação, esta geração exige também velocidade das demais pessoas, sendo critério fundamental para manutenção da sua atenção a rapidez nos envolvimentos sociais); viii) inovação (demonstram um anseio em se manterem atualizados mediante o domínio do que há de mais novo e útil com relação à tecnologia) (TAPSCOTT, 2010, p. 91-119).

Ainda que a ela (internet) não esteja suscetível ao acesso de todos – no Brasil, por exemplo, o Instituto Brasileiro de Geografia e Estatística IBGE aponta que 116 (cento e dezesseis) milhões de brasileiros têm acesso à internet, o que denota aproximadamente 65% da população (IBGE, 2016) –, fato é que a internet influencia direta ou indiretamente na vida de todos os cidadãos do globo terrestre.

Os atos da vida civil ou migraram para o ambiente virtual ou então são diretamente determinados por este. Por exemplo, a parcela de brasileiros que não tem acesso à internet depende dela para consecução de qualquer benefício previdenciário ou outro fornecido pelo Estado, vez que este armazena e utiliza da internet para manejo e verificação de todas as informações dos cidadãos brasileiros. Para além do ambiente público, também no privado se verifica tal influência, na medida em que quase todos os produtos consumidos também por esta parcela da população são produzidos mediante o emprego de tecnologia e inerente utilização da internet para sua realização, como o veículo automotor, os alimentos industrializados, a energia elétrica etc. Enfim, é difícil encontrar, nos dias de hoje, algo que não se utilize da internet para ser feito.

Neste sentido, em comentário à obra de Castells aponta-se que de fato vivemos em uma sociedade em rede, localizada em uma chamada "Galáxia da Internet", na qual a influência do fluxo de informações na Internet não se restringe ao número de usuários, pois ainda que indiretamente, a internet afeta a vida de todos pelo fato de que todas as atividades humanas estão de certa forma refletindo a estrutura da rede. Assim, "Dentro dessa realidade, é evidente que a sociedade informacional compartilha tudo o que sabe, o que vê, o que ouve e o que sente, muito diferente de outras épocas, quando todo o conhecimento era, de certa forma, centralizado. Essas facilidades e possibilidades transformaram o mundo, consolidando o "virtual" e a "cultura digital" (TADEU NASCIMENTO; DE MACEDO, 2016, p. 11).

Possível a partir da constatação de um novo paradigma social, esta cultura digital permite a realização de ações dantes não acessíveis ao cidadão comum, não detentor de algum

poderio político. Por tal procedimento, o produto e serviço produzido deixa de ser considerado apenas em si mesmo e passa a se pulverizar a atenção dando-se voz e participação mais individualizada e ativa dos indivíduos na sociedade. Isso se verifica, principalmente, em questões eleitorais, nas quais se verifica cada vez mais a utilização de redes sociais para defesa de ideais e posições ideológicas.

Já anunciava Pierre Lévy, a seu tempo, como efeito do avanço tecnológico e a universalização do acesso à informação e às novas tecnologias, que possibilitam a criação de uma cibercultura, o que denominou de inteligência coletiva decorrente do fluxo de informações inerente ao ciberespaço, ponderando quanto a esta que:

> (...) nos casos em que processos de inteligência coletiva desenvolvem-se de forma eficaz graças ao ciberespaço, um de seus principais efeitos é o de acelerar cada vez mais o ritmo da alteração tecnossocial, o que torna ainda mais necessária a participação ativa na cibercultura, se não quisermos ficar para trás, e tende a excluir de maneira mais radical ainda aqueles que não entraram no ciclo positivo da alteração, de sua compreensão e apropriação.
> Devido a seus aspecto participativo, socializante, descompatibilizante, emancipador, a inteligência coletiva proposta pela cibercultura constitui um dos melhores remédios para o ritmo desestabilizante, por vezes excludente, da mutação técnica. Mas, neste mesmo movimento, a inteligência coletiva trabalha ativamente para a aceleração dessa mutação. Em grego arcaico, a palavra "pharmakon" (que originou "pharmacie", em francês) significa ao mesmo tempo veneno e remédio. Novo *pharmakon*, a inteligência coletiva que favorece a cibercultura é ao mesmo tempo *veneno* para aqueles que dela não participam (e ninguém pode participar completamente dela, de tão vasta e multiforme que é) e um *remédio* para aqueles que mergulham em seus turbilhões e conseguem controlar a própria deriva no meio de suas correntes (LEVY, 1999, p. 30).

A internet figura, assim, como centro de aceleração de todo o movimento em rumo à Sociedade da Informação. Sem ela, seria impossível o desenvolvimento tecnológico e a mutação social que hoje nos deixam à vontade para analisar um novo paradigma social.

Nesse sentido, corroborando esta ideia de que as tecnologias agregam valor ao desenvolvimento humano e suas potencialidades, é possível afirmar que na sociedade da informação, as diariamente lançadas novas tecnologias da informação se apresentam como ferramentas de auxílio na realização das potencialidades humanas, tanto para o bem quanto para o mal, sendo relevante, por sua vez, na emancipação do povo e consequente limitação do poder do Estado (SERRAGLIO; ZAMBAM, 2016, p. 28).

A informação é, pois, importante não apenas para segmento empresarial privado, mas em verdade para todos os outros ramos, vez que, muito embora a atividade empresarial hoje tenha por valor máximo os dados informacionais, a esfera jurídica reforça esta importância ao se ter inúmeros direitos que estão atrelados à informação (MACHADO; FILHO, p. 529).

Outra característica importante que decorre da popularização da internet é a praticamente inexistência de barreiras internacionais, ao menos no que tange ao ambiente virtual. Houve um tempo (não muito distante em termos históricos) em que a realidade social limitava-se ao que se compreendia dentro do país. Informações e notícias internacionais chegavam com atraso ao aproveitamento ou mesmo sequer se tomava conhecimento.

Com a internet e o fluxo de informações, bem como a velocidade com que as comunicações são feitas atualmente, os problemas e desídias sociais deixaram de ser um problema apenas interno de cada país e passaram a existir demandas mundiais, na busca principalmente da dignidade de todo e qualquer ser humano. Os Direitos Humanos se impõem e passam a ser exigidos por todos em âmbito internacional.

Verifica-se, em verdade, a existência de uma possível sociedade global, pela qual as barreiras territoriais não mais se sustentariam.

O assunto é muito amplo e há quem defenda tanto a manutenção quanto a extinção das divisões em territórios e outros, mais futuristas e visionários, constituição de um estado único, global. Contudo, as dificuldades e o cenário atual acabam por derrocar, a nosso ver, o encaminhamento à uma sociedade unificada em termos de soberania.

Em contraponto, muito embora se vislumbre o encaminhamento a uma sociedade única em termos comunicacionais, a constatação desta sociedade globalizada e interligada (ou seja, da informação), não significa o fim dos territórios nacionais, pois "não é de fim do território que se trata, para desarmar as soberanias e abrir as fronteiras (arrombá-las mesmo), o que pode ser ambivalente, como é óbvio. Na sociedade da informação o território e a territorialidade não somem, pelo contrário, acrescentam-se" (DA CUNHA, 2017, p. 8).

Vale dizer, pois, que o fluxo e a velocidade de troca de informações e interconectividade que caracterizam a Sociedade da Informação não significam a desestruturação dos estados. Ao contrário, a instantânea comunicação e ciência pulverizada à população de fatos globais acaba por ressaltar as fronteiras internacionais e colocam os Direitos Humanos como *minimum* a ser alcançado e passível de exigência pela comunidade internacional:

> Nas sociedades modernas as relações sociais são deslocadas de seus contextos territoriais de interação e se reestruturam por meio de relações indefinidas de tempo e espaço. Os homens se desterritorializaram, favorecendo uma organização racional de suas vidas. Uma mudança tão relevante precisa se utilizar de um sistema técnico que permite o controle do espaço e do tempo. Por isso, o paradigma da "moderna nação" não deve contemplar-se como algo oposto à mundialização, posto que está implícita na própria modernidade. Nação e mundialização não são antagônicas, senão que ambas devem ser contempladas como nos momentos de desenvolvimento

> histórico da modernidade. A nação moderna conduz logicamente à "modernidade mundo": "contrariamente ao que muitas vezes se supõe, a nação é a primeira afirmação da mundialidade. Ela leva em seu peito uma modernidade-mundo... a modernidade inclui uma vocação mundial, e não pode ser contida dentro de fronteiras nacionais." (JULIOS-CAMPUZANO, 2011, p. 129).[5]

Ressalva feita ao entusiasmo que leva à ideia de uma sociedade única, falando em termos de território, não se pode descartar a característica da dita Sociedade da Informação que é a unificação global das pessoas mediante o fluxo informacional robusto e instantâneo que hoje se executa diariamente, levando-a a determinar a informação como principal produto, bem como a utilização das tecnologias como principal ingrediente de alteração na forma de relacionar-se humanamente e de comportamento social em geral.

3 DA FUNDAMENTALIDADE DO ACESSO À INTERNET SEGURA NA SOCIEDADE DA INFORMAÇÃO

Após análise das especificidades que permeiam a Sociedade da Informação, é possível concluir que se faz necessário avançar no que tange à relação entre novos direitos fundamentais e internet. É indispensável, assim, que seja garantido não apenas acesso à internet, mas também que o mesmo se dê à uma internet segura.

O acesso à internet pode, assim, perfeitamente ser reconhecido como um direito fundamental em razão da sociedade digital que vivemos hoje.

Merece apontamento, ainda que superficial, as diferentes denominações dos direitos nesta oportunidade retratados. Isso porque ora são conclamados como direitos humanos, ora como direitos fundamentais e, por assim dizer, também os direitos da personalidade (que compõe parte dos direitos fundamentais) são retratados com nomenclaturas distintas.

Grosso modo, a diferenciação se justifica pelo plano em que o direito (por exemplo, a privacidade) está legitimado: se internamente, expressamente garantido por meio de uma Constituição, dir-se-á fundamental; se não expresso e necessária a utilização de diplomas

[5] Texto original: En las sociedades modernas las relaciones sociales son desplazadas de sus contextos territoriales de interacción y se reestructuran por medio de relaciones indefinidas de tiempo-espacio. Los hombres se desterritorializan, favoreciendo una organización racional de sus vidas. Un cambio tan relevante precisa servirse de un sistema técnico que permita el control del espacio y del tiempo. Por eso, el paradigma de la "modernidade-nación" no debe contemplarse como algo opuesto a la mundialización, puesto que ésta va implícita en la propia modernidad. Nación y mundialización no son antagónicas, sino que ambas deben ser contempladas como dos momentos del desarrollo histórico de la modernidad. La modernidad-nación conduce lógicamente a la "modernidad-mundo": "contrariamente a lo que muchas veces se supone, la nación es una primera afirmación de la mundialidad. Ella porta en su seno una modernidade-mundo... la modernidad encierra una vocación mundial, y no puede ser contenida en el interior de las fronteras nacionales." (JULIOS-CAMPUZANO, 2011, p. 129).

internacionais que tratam do assunto, poder-se-á tratá-lo e pô-lo à efetivação com base nos direitos humanos.

Fábio Konder Comparato elucida quanto à diferenciação entre direitos humanos e direitos fundamentais, aduzindo que é na vigência efetiva dos direitos do homem que se dispõe sua separação: os direitos fundamentais são aqueles reconhecidos como direitos humanos pelas autoridades estatais competentes para elaborarem as normas – tanto dentro do Estado quanto em âmbito internacional (COMPARATO, 2010, p. 70-71).

Sendo assim, as diferenças residem no grau de capacidade de concretização em âmbito da norma que está sendo conclamada, de modo que os Direitos Fundamentais podem ser considerados duplamente positivados, atuando tanto interna quanto externamente. Isso ocorre ao passo que os Direitos Humanos, apesar de positivos, concentram-se apenas em ordem internacional, com uma abrangência mais generalizada e universal que tem por objetivo e fim último proporcionar a efetiva humanização dos direitos, condicionando a validade das normas expressas de determinado Estado ao bloco rígido destes direitos ditos humanos, que condicionam o tratamento ao indivíduo em qualquer lugar do mundo, seja no Ocidente, seja no Oriente. Os Direitos Fundamentais, por sua vez, possuem substrato na dignidade da pessoa humana e na limitação do poder estatal, sempre com previsão (expressa ou mediante interpretação expansiva) na Constituição. Isto, porém, não inibe a possível existência de valores jurídicos ainda não positivados e que ensejam, em decorrência da dignidade, limitação ao Poder Público e demais indivíduos (ANDRADE, 2017, p. 78).

Pois bem. Com aplicação da teoria dos direitos fundamentais e preceitos constitucionais ao objeto do presente estudo, podemos inferir a fundamentalidade do acesso à internet segura (além, evidentemente, da dignidade da pessoa humana), como também do próprio princípio da segurança pública ou pessoal.

Quanto a esta, nos dizeres de Rodrigo Ghiringhelli e Maura Basso pode-se concluir que se trata de direito fundamental, pois:

> A Constituição Federal do Brasil dispõe acerca de segurança pública no Título V – DA DEFESA DO ESTADO E DAS INSTITUIÇÕES DEMOCRÁTICAS. Dispõe o caput do artigo 144 da CF: Art. 144. A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio.
> A abordagem proposta sobre direitos fundamentais acaba por remeter ao estudo acerca da cláusula de abertura propiciada pelo §2º do art. 5º da CF, que permite afirmar que, mesmo sem estar expressamente prevista, a segurança pública ou pessoal pode ser considerada direito fundamental (GHIRINGHELLI; BASSO, 2009, p. 280).

Sob esse viés, não é difícil conceber a segurança digital também como direito fundamental e, portanto, exigível perante o Estado. As garantias expressamente previstas na Constituição não excluem outros direitos decorrentes dos princípios por si mesmo admitidos como norteadores da ordem jurídica, ou ainda de tratados internacionais ratificados pelo Estado.

Assim, pois, trata-se de uma cláusula de abertura, pela qual não se é permitida elaboração de rol taxativo, havendo direitos e garantias constitucionais que surgem no decorrer do tempo e, por decorrência de outro princípio (substrato maior na dignidade da pessoa humana) gozam de mesmo prestígio constitucional e demandam imperativa efetivação, podendo-se vislumbrar uma concepção materialmente aberta dos direitos fundamentais.

Como trazem os autores, o art. 5º da Constituição não pode, assim, ser considerado com viés taxativo, categorizando-os, portanto, como direitos fundamentais formais e materiais. Os primeiros denotam àqueles direitos e garantias fundamentais que por opção legislativa ficaram alocados no texto constitucional de forma expressa. Já os materiais, em que pese não estarem no catálogo apresentado pela Constituição, devem assim ser equiparados àqueles em razão de sua relevância (GHIRINGHELLI; BASSO, 2009, p. 281).

Superada, neste sentido, a ideia de que podem ser tidos como fundamentais apenas aqueles direitos expressamente previstos na Constituição – ainda que realmente árdua seja a tarefa de identificação de quais direitos não catalogados são consubstanciados por matéria constitucional – não prospera, vez que também há de se considerar a já consolidada dogmática da nova interpretação constitucional (denominado Neoconstitucionalismo), pela qual o procedimento não mais sub-roga-se em mera análise subsuntiva do binômio norma versus caso concreto.

O desenvolvimento técnico-jurídico para consagração da fundamentalidade de algum direito fora do rol expresso na Constituição perpassa por análise e justificação válida – vale dizer, fundamentada – das razões que levam ao reconhecimento desta.

Direitos fundamentais existem, assim, em outras partes do texto constitucional ou mesmo em outros textos legais nacionais (leis ordinárias, complementares, resoluções, normativas, dentre outros) ou então de ordem internacional, não restando dúvida quanto à abertura material dos direitos individuais e coletivos fundamentais.

Nesse sentido, a segurança pessoal e a segurança pública não estão expressamente garantidas como direitos fundamentais na Constituição Federal, mas facilmente se pode a elas atribuir tal status, conforme raciocínio desenvolvido.

Por sua vez, o acesso à internet deve propiciar, além da universalização do conhecimento e inserção social, segurança para aqueles que a utilizam para realização das tarefas mais importantes de sua vida. O diagnóstico é fácil quando em exercício simples de raciocínio se vislumbra a atividade empresarial, por exemplo, toda dependente da utilização da internet. Os meios de produção da imensa maioria dos bens e serviços estão estruturados com a utilização da internet, de modo que a questão aqui abordada não trata somente de usuários individuais, mas, em verdade, o panorama é global, universal, ou seja, a demanda por uma internet segura é tanto de usuários quanto de fornecedores de produtos e serviços.

Aliás, como já mencionado anteriormente, não se conceberá a possibilidade de viver sem acesso à internet em um futuro muito próximo, pois, o panorama atual já evidencia a necessidade de utilização da internet para realização das mais diversas atividades civis e particulares, quanto mais para as demandas e inovações que se aproximam. Filmes de ficção científica são cada vez mais reais, mas não nos baseamos nestes para poder afirmar que muito em breve a comunicação demandará a utilização da internet, ao menos nas relações entre Estado e cidadão, e também entre fornecedores e consumidores.

Pode-se afirmar, portanto, já hoje que "O acesso à internet tornou-se um direito básico, de que também depende desenvolvimento humano e, em última instância, a realização de Direitos Humanos e liberdades fundamentais" (BACCIOTTI, 2014, p. 111). A não garantia de acesso à internet acaba por gerar uma casta de excluídos sociais, sendo ele – o acesso à internet – já passível de reconhecimento como direito fundamental ao desenvolvimento pleno da pessoa pertencente à Sociedade da Informação.

Esta fundamentalidade do acesso à internet está evidenciada pela exclusão social gerada pelo não fornecimento de internet à parcela da sociedade, o que é denominado por Karina Joelma Bacciotti como "brecha digital" e se dá em cinco níveis, quais sejam: i) a diferença de condições de acesso entre países desenvolvidos e países subdesenvolvidos; ii) dentro do país, entre os indivíduos que moram nas cidades e àqueles que residem na zona rural; iii) o terceiro tipo de exclusão digital se refere à diferença entre gêneros e gerações, carregando cunho social mais aguçado, evidenciando mundialmente uma qualificação e acesso à educação menor às mulheres; iv) quanto aos deficientes, especialmente os visuais, que não têm acesso à máquinas e terminais adaptados, ficando sem acesso ou com acesso comprometido à internet; e v) limitações de conteúdos por parte do governo (ibid., p. 113).

Outras limitações podem ser imaginadas, servindo os exemplos apenas para elucidação e atentando-se com maior veemência à questão da educação digital, que será analisada adiante.

Basta, por ora, a constatação de que nos dias de hoje a pessoa necessita da internet para viver e desenvolver plenamente suas atribuições como pessoa, evitando-se assim a violação dos direitos da personalidade (especialmente no que tange às liberdades), sendo este um dos objetivos expressamente previstos pelo Marco Civil da Internet.[6]

Todavia, o simples fornecimento de acesso à internet já se revela insuficiente para tal consagração. Isso porque a qualidade e segurança da internet oferecida também são elementos preponderantes à consecução do objetivo que se propõe com a ela (especificamente de interconectividade).

Caso contrário, o acesso à internet pode se revelar, em verdade, um meio de ofensa aos direitos da personalidade, como já se vê constantemente nos noticiários com a prática de crimes em ambiente virtual.

Destaca-se, neste sentido, evidentemente, a prática do *ransomware*, o qual será mais adiante abordado de forma pormenorizada. Contudo, há de se salientar que fraudes bancárias, estelionatos de diversas formas, furtos e violações à imagem, honra e privacidade têm sido diariamente perpetradas por meio da internet.

A obrigação estatal, assim, está para além do simples fornecimento de acesso universal à internet. É necessário àquele que se propõe ser o garantidor da paz social garantir também que a internet seja um ambiente minimamente seguro ao usuário. Isso perpassa pelo desenvolvimento, claro, de ferramentas que garantam identificação de infratores e mecanismos de reparação, bem como de prevenção de ilícitos, mas também da promoção de uma educação digital, capaz de proporcionar ao usuário noções mínimas de desenvolvimento de tecnologias e programação, a fim de incutir também na pessoa do usuário uma habilidade para discernimento e utilização segura da internet e suas inúmeras ferramentas e aplicativos.

A Rede deve ser considerada não apenas um meio de comunicação ou de transmissão de dados, vez que vivemos já na dita Sociedade da Informação, na qual tais objetos (dados e informação) consubstanciam-se em valores principais e merecedores de especial atenção e proteção. Mediante adequada análise e consideração do que é a internet nos dias de hoje, não concebível mais a ideia de que o acesso a esta se dá simplesmente pela conexão, mas sim no acesso à infraestrutura adequada que seja capaz de permiti-la, a disponibilidade (inexistência de restrições) do conteúdo e a educação digital, revelando-se, qualquer privação destes, violação ao direito de acesso à internet, o qual se revela fundamental.

[6] Art. 4º. LEI 12.965/2014. A disciplina do uso da internet no Brasil tem por objetivo a promoção: I - do direito de acesso à internet a todos […].

4 DA NECESSÁRIA IMPLEMENTAÇÃO DE UMA POLÍTICA PÚBLICA DE COMBATE AO *RANSOMWARE* NO BRASIL

Ransomware pode ser determinado como "um termo abrangente usado para descrever uma classe de *malwares* que serve para extorquir digitalmente as vítimas, fazendo-as pagar um preço específico" (LISKA; GALLO, 2017, p. 16). Por *malware*, entenda-se programa de computador malicioso.

Para Lawrence Miller *ransomware* é um software malicioso (*malware*) usado em ataques cibernéticos para criptografar dados da vítima utilizando chaves de encriptação conhecidas unicamente pelo invasor, que tornam as informações inacessíveis até o pagamento de um resgate (normalmente por meio de uma criptomoeda, como a *Bitcoin*) a ser feito pela vítima. Destaca que só nos EUA foram registrados 4 (quatro) mil ataques diários no mês de janeiro de 2016, quando podemos dizer que a prática tomou conhecimento global (MILLER, 2017, p. 3).

Analisando o cotejo legal brasileiro poder-se-ia, em análise rasa, suscitar que a prática estaria tipificada e, portanto, desnecessária uma política pública neste sentido, em razão da existência da Lei 12.737/2012, batizada de Lei Carolina Dieckamann. Contudo, além de simplesmente possuir uma lei específica não significar necessariamente que há uma política pública relativa a qualquer assunto estatal, no Brasil há ainda que se afirmar inexistir referida disposição, vez que o referido diploma não trata do *ransomware* em si, mas tão somente da invasão de dispositivo eletrônico, que é apenas um crime-meio para a consecução do objetivo do criminoso, que é a extorsão. Nem ela (Lei de Proteção a Dispositivos Informáticos) nem o Código Penal (parte especial) guardam satisfatória adequação com a novel prática delituosa internacional que horrorizou o mundo a partir de janeiro de 2016.

O mesmo raciocínio pode ser aplicado à questão da recém aprovada Lei Geral de Proteção de Dados. Ora, nesta também não se verifica por si só uma consagração de política pública específica no combate ao *ransomware*, haja vista que trata da responsabilidade pelo tratamento de dados por empresas legítimas prestadoras de serviços e não do aspecto criminal da conduta em si, mas sim de questões periféricas como a responsabilidade civil de prestadores de serviços.

Tem-se, assim, a necessidade de implementação de uma política pública de combate ao *ransomware*, verificando-se na sua hipótese todos os elementos estruturantes de uma intenção e objetivo a ser alcançado pelo Estado, obedecendo à criação de uma política pública várias exigências e possuindo fases de estruturação, as quais serão delineadas.

Analisando principalmente os conceitos trazidos por Dye e Jenkins, Michael Howlett conceitua política pública como um "fenômeno complexo que consiste em inúmeras decisões tomadas por muitos indivíduos e organizações no interior do próprio governo e que essas decisões são influenciadas por outros atores que operam interna e externamente no Estado" (HOWLETT, 2013, p. 12).

Importa destacar que o desenvolvimento de uma política pública para atendimento à necessidade exposta no título do presente trabalho, qual seja a propiciação de meios para se combater a conduta de sequestro de dados, não significa que deve ser um plano elaborado por este ou aquele governo, este ou aquele candidato.

É necessário, pois, primeiramente distinguir política propriamente dita de política pública. Os ideais de um governo estarão presentes no processo de criação da política pública, sem sombra de dúvida. O que dá legitimidade para tanto, por sua vez, é a expressão da vontade popular, a qual elege um em detrimento de outro para assim então se buscar solução dos problemas sociais específicos.

Todavia, após iniciada a implementação de uma política de governo, há uma transmutação, dada em razão da atribuição de juridicidade à política, quando então se pode falar em política pública. Esta última, então, dotada de juridicidade, passa a não mais se apresentar como mera vontade de governo, mas sim como objetivo juridicamente obrigatório de consecução à nação.

Apresentando o plano macroinstitucional, Maria Paula Dallari Bucci ensina que:

> O governo é o nicho da política no Estado: as decisões políticas são essencialmente manifestações de poder. Mas a política de maior alcance, compatível com a complexificação das possibilidades e dos meios obtidos com o desenvolvimento do capitalismo, depende da conformação do poder em estruturas despersonalizadas, organizadas segundo regras e procedimentos jurídicos. E com isso, progressivamente, a política vai deixando de ser exclusivamente política, para ser, ao mesmo tempo e cada vez mais, também direito, organizado em instituições (BUCCI, 2013, p. 45).

Denota-se, assim, que há solidez ao que se entenda como política pública, não sendo alterada a cada alteração de governo. Possibilita, assim, caracterizá-la como macroinstitucional, ou seja, além das instituições. É uma vontade comum exprimida pela maioria para qual todos, Estado e jurisdicionados, devem caminhar.

Com relação ao tema objeto da pesquisa, a questão é ainda mais abrangente, pois importa em questões de direitos humanos, os quais internacionalmente são, há muito tempo,

protegidos com tratados e convenções para as quais, como dito anteriormente, o Brasil é reiteradamente acusado de descumprimento.

Quanto a esta obrigação estatal, Alain Supiot revela que:

> Hoje, a abertura das fronteiras, que atende a uma série de fatores bem conhecidos (econômicos, políticos e técnicos), abala esses âmbitos nacionais da vida em sociedade. As solidariedades nacionais são por sua vez questionadas, de um lado, pelo que se chama a globalização e, do outro, pela relocalização, pela reterritorialização. Globalização e localização são as duas faces inseparáveis de estratégias econômicas mundiais que se fundamentam na valorização de vantagens competitivas locais. O Estado encontra-se, assim, numa situação perigosa. No plano internacional a "globalização" conduz a uma ordem jurídica em que o Direito Internacional da concorrência, que supostamente encarna o interesse comum das diferentes nações, impõe-se aos Estados (SUPIOT, 2007, p. 192).

Não se trata, pois, de um problema que se quer resolver, mas sim de uma obrigação, pois já superada, e muito, este primeiro plano da criação de uma política pública, havendo juridicidade inquestionável na questão da prática do *ransomware*, por se constituir em violação aos direitos da personalidade, conforme visto anteriormente.

Delineada a ideia de desenvolvimento da política propriamente dita à política pública, com a ressalva quanto à juridicidade desta última assim já considerada, pode-se caminhar para seu segundo momento: o plano microinstitucional. Este, por sua vez, caracteriza-se pelo processamento com que o objetivo será implementado. Nos dizeres de Maria Paula Dallari Bucci:

> Políticas públicas definem-se como programas de ação governamental, em cuja formação há um elemento processual estruturante: "política pública é o programa de ação governamental *que resulta de um processo ou conjunto de processos juridicamente regulados* [...]".
> A expressão *processo* empregada nessa proposição está mais ligada ao viés da ciência política que ao direito. Refere-se ela à sucessão de etapas da "vida institucional" de uma política pública, desde a inserção do problema na agenda política até a implementação da decisão, passando pela formulação de alternativas e a tomada da decisão em si". O processo é o fator de unidade, "fio condutor" a orientar a identificação e compreensão de determinada política pública (...) (BUCCI, 2013, p. 109-110).

Trata-se, portanto, da incorporação ao sistema administrativo daquilo que se pretende instituir como política pública, com apresentação das prioridades, dos recursos a serem utilizados, quem serão os beneficiados e qual o tempo será necessário para a efetivação e durabilidade da política pública.

Na lição trazida por Maria Paula Dallari Bucci, a classificação dos planos de criação de uma política pública conta ainda com o que ela denomina de plano mesoinstitucional, que

se situa entre os dois primeiros mencionados (macro e microinstitucional). Nele, entre o governo (macro) e a ação governamental (micro) estão os "arranjos institucionais, políticas públicas na sua forma exterior, conjunto de elementos, iniciativas e normas que compõem o programa de ação governamental devidamente estruturado" (BUCCI, 2013, p. 205).

Em suma, neste plano se caracteriza a implementação da política pública com sua inclusão no ordenamento jurídico, fazendo-se devida ressalva quanto à abrangência do instituto, que não significa dizer apenas leis e resoluções. Como se sabe, princípios constitucionais são dotados de normatividade, servindo, portanto, por exemplo, como fundamento jurídico válido à efetivação de direitos fundamentais.

Quanto à política pública, ainda, há que se considerar todo e qualquer diploma normativo, como resoluções, normativas, ordens internas, e não apenas leis ou dispositivos constitucionais, todo regramento pode ser inserido neste plano mesoinstitucional e revela, na prática, a ação (vontade) governamental, a qual pode, inclusive, ser colegiada (vários Estados) como se verifica em regramentos formulados por órgãos coletivos como a ONU e o Conselho Europeu, elaboradores do já estudado GDPR, por exemplo.

Na prática, pois, o desenvolvimento de uma política pública se dá em cinco fases, as quais serão agora tratadas, em definições trazidas pela obra de Michael Howlett. Em um primeiro momento, a criação da política pública necessita de uma montagem de agenda. Por meio dela, é reconhecido o problema para o qual se buscará implementação de medidas à sua solução. Saber qual problema ou necessidade da população merece a dispensa de tal nível de atenção é fundamental e se revela a mais importante das fases de criação da política pública. Como muito bem assevera o autor:

> Em sua essência, a montagem da agenda diz respeito ao reconhecimento de que algum assunto é um problema que requer mais atenção por parte do governo (...). Isso não garante, de modo algum, que o problema será eventualmente abordado, ou resolvido, por alguma atividade adicional do governo, mas apenas que ele foi isoladamente destacado para que o governo o leve em consideração entre a massa de problemas que existem numa sociedade em determinado momento. Isto é, ele foi elevado de seu *status* como objeto de preocupação para o status de um problema privado ou social e, finalmente, ao *status* de uma questão pública (*publicissue*) potencialmente sujeita à ação governamental. Se, por um lado, as ameaças e desafios constituem as forças que com mais frequência motivam a definição de tópicos na formação da agenda política, por outro, em outras ocasiões as agendas políticas podem ser estabelecidas pela atratividade de uma oportunidade, como a corrida do programa espacial dos Estados Unidos para levar um homem à Lua na década de 1960. (HOWLETT, 2013, p. 104)

Quanto a esta questão de oportunidade tratada pelo autor, há que se ponderar que, quanto ao tema aqui discutido, a migração da prática de *ransomware* para alvos como

pequenas empresas e pessoas físicas, que eclodiram em janeiro de 2016 (muito embora a prática não seja tão recente), enseja uma disposição governamental mais ávida em resolver problemas pretéritos de precariedade da segurança na internet.

Evidente que a questão deve estar presente na agenda governamental brasileira. Todavia, dada a expansão de problemas sociais relevantes e de uma alegada falta de orçamento público, muitas questões deixam de ser encaradas como deveriam, muito embora a segurança na internet envolva praticamente todos os setores produtivos de nossa Sociedade da Informação e deva ser, assim, tratada com máxima prioridade.

Em um segundo momento, a política pública assim reconhecida e integrante da agenda governamental precisa de um plano, um curso de ação pelo qual as medidas a si inerente serão tomadas no objetivo de resolver ou diminuir as consequências do problema eleito.

Michael Howlett divide a formulação da política pública (*policy-making*), segunda fase da criação da política pública, em mais duas fases, apreciação e diálogo, sendo que:

> Na fase da apreciação, se identificam e se consideram os dados e a evidência. Esses podem tomar a forma de relatórios de pesquisa, depoimento de *experts*, informações das partes interessadas, ou consulta pública sobre o problema político que se tenha sido identificado. Aqui o governo tanto gera quanto recebe informações sobre os problemas políticos e suas resoluções.
> A fase do diálogo procura facilitar a comunicação entre os atores políticos com diferentes perspectivas sobre a questão e as soluções potenciais. Às vezes, são realizadas reuniões abertas em que os apresentadores podem discutir e debater as opções políticas propostas. Em outros casos, o diálogo é mais estruturado, com *experts* e representantes societários de organizações de negócio e trabalhadores convidados a falar contra e a favor das soluções potenciais. Hajer (2005) observa que a estrutura que propicia informações sobre as opções políticas pode fazer diferença considerável nos efeitos dessa participação, tanto no processo político quanto nos próprios participantes. As consultas formais e audiências públicas tendem a privilegiar a informação especializada e frustrar os novos participantes, ao passo que novas técnicas envolvendo os participantes de organizações e os pontos de vistas menos estabelecidos podem trazer mais energia e entusiasmo ao diálogo sobre as opções políticas. (HOWLETT, 2013, p. 124)

É, portanto, o momento de estudo e coleta de informações e dados estatísticos para, além de justificar-se a adoção da política pública na agenda governamental, também se traçar qual o caminho mais eficaz na consecução do objetivo almejado (solução do problema social eleito).

A terceira fase, por sua vez, trata da tomada de decisão política e se perfaz pela adoção de uma ou mais hipóteses de solução estudados e discutidos como aplicáveis ao problema, de modo que assim eleitos pelos agentes políticos responsáveis.

Esta escolha se dá por meio da utilização de critérios inerentes ao contexto social-econômico que se encontram os agentes. Historicamente, em um primeiro momento se teve

como padrão a utilização de um critério mais utilitarista, no sentido de potencializar-se o resultado com o menor emprego de esforços possível. Posteriormente, consolidou-se um critério (incremental) pelo qual uma verdadeira barganha de benefícios e responsabilidades era feita entre os agentes interessados, de modo a convencer-se o outro mediante uma contraprestação, em um procedimento dotado de essência política bem ávida.

A quarta fase de criação da política pública é sua implementação. Trata-se da parte mais prática do processo, pela qual são adotadas as medidas que levam aos resultados. Destaque-se que, a este ponto, o problema já logrou êxito em um longo e complexo caminho, sendo agora devida a prática de ações para que resultados sejam alcançados, como diminuição ou aumento de números estatísticos.

Tendo em vista o quadro histórico da implementação das políticas públicas demandar aprofundamento para elucidação quanto às formas experimentadas e acertos e erros, o que não é objeto do presente estudo, importa por ora apenas mencionar que a preocupação neste ponto é com o *design* que será dado aos programas de efetivação das políticas, de modo a se ter maior ou menor grau de concentração das ações em um agente político mais evidenciado (no nosso cenário será uma política pública de âmbito federal, estadual ou municipal ou mesmo se pulverizada entre estes três, ou ainda se implementar-se-á por meio de convênios público-privados, e, principalmente, com viés internacional).

Por fim, e com maior inerência ao Direito, está a fase de avaliação da política pública. Com mais atenção da ciência jurídica em razão de ser neste momento que as medidas adequadoras serão tomadas, e isso se dá mormente com interferência do Poder Judiciário.

Todavia, não é só isso. Não se trata apenas de judicialização. A avaliação é feita mediante procedimentos de análise pelos agentes políticos envolvidos, aplicadores finalmente da política pública, bem como pela população, com renovação das consultas populares e especializadas da segunda fase, agora com substrato mais concreto do complexo ideal-real. As avaliações podem ser classificadas como avaliação administrativa, avaliação judicial e avaliação política.

Para o elaborador da teoria aqui pincelada, Michael Howlett, como resultado desta última fase, após a avaliação de uma política pública, o problema e as hipóteses de solução podem ser totalmente revistos, o que importaria, neste caso, no recomeço de todo o processo cognitivo de implementação da política, retornando à montagem da agenda ou qualquer outro estado anterior do processo de implementação, ou ainda, sendo satisfatórios os resultados, possa-se manter o padrão de medidas adotado. A reconceituação pode significar tão somente

alteração em aspectos tangentes ao plano geral, ou mesmo o fim da própria política pública (HOWLETT, 2013, p. 199).

Interessante perceber que, até mesmo para constatação da efetividade ou não de uma política pública, critérios devem ser estabelecidos, e o são, basicamente, assim feitos com a contraposição do objetivo inicialmente estamentado e os resultados produzidos após a sua implementação.

Analisando a questão de política pública para segurança na internet, em artigo publicado para o Instituto da Defesa Nacional de Portugal, Paulo Fernando Viegas Nunes faz importantes reflexões e ponderações sobre o assunto, especialmente quanto à órbita internacional. Primeiramente, o especialista em transmissões elucida quanto à divisão de tratamento que deve ser dada em âmbito nacional e internacional, de modo que a ambos deve ser dada a atenção, mas especifica quanto aos procedimentos internos que podem ser adotados, indicando quais têm sido as medidas e objetivos a serem alcançados neste ínterim. Defende, neste sentido, a criação de um conselho nacional cuja atribuição seja a implementação de medidas e de uma política pública de proteção ao ambiente virtual, especialmente em âmbito nacional, com colaboração no que tange ao aspecto internacional (NUNES, 2012, p. 115).

Para tanto, enumera muitas medidas que devem compor o que denomina de Estratégia Nacional de Segurança Digital, dentre as quais estão: a) a garantia de proteção das infraestruturas de informação, com implementação de mecanismos de segurança e prevenção de invasões; b) melhoria da referida infraestrutura, com constante investimento em inovação e atualização das tecnologias implementadas; c) reforço da segurança da rede utilizada pelo poder público; d) reforma legislativa capaz de combater o cibercrime, com elaboração de novas leis e aplicação adaptada das normas vigentes às especificidades do âmbito virtual; e) implementar órgãos de controle (Conselho Nacional de Cibersegurança e Ciberdefesa) para os quais é atribuída função regulatória e de orientação político-estratégica e gestão de crises do ciberespaço, com garantia de autoridade ao combate aos crimes cibernéticos, garantindo segurança no espaço nacional da internet; f) garantir segurança do próprio governo quanto a ataques cibernéticos, e não somente de seus circunscritos; g) promover aculturamento de uso consciente da internet, com vistas à promoção de uma educação digital; h) investir no desenvolvimento de novas tecnologias para melhoria e maior rigidez da segurança dos dispositivos, em âmbito nacional e internacional; e i) reforçar os compromissos de cooperação internacional (NUNES, 2012, p. 124).

Conclui o analista no sentido de que "O desenvolvimento de uma Estratégia Nacional para o Ciberespaço permitirá potencializar o impacto das iniciativas governamentais já em curso, fornecendo-lhes uma visão e um enquadramento integrador, que facilita a implementação e reforça o seu impacto, num contexto onde o desenvolvimento de sinergias nacionais e de parcerias internacionais desempenha um papel central" (ibid., p. 125).

Por vezes, a própria inclusão do problema na agenda governamental decorre de uma internalização de problemas internacionais, como nos parece ser o caso da segurança na internet (SANTOS, 2014, p. 23). Isto se verifica tradicionalmente com relação ao Brasil, onde há uma tendência natural de incorporar legislações estrangeiras com adaptações (nem sempre bem-sucedidas) à realidade nacional. Por exemplo, podemos citar os aqui analisados GDPR que após entrado em vigor destrancaram projetos de lei que, como visto, vieram a consagrar a LGPD brasileira, que contém adaptações, mas sem sombra de dúvida se inspirou no regramento europeu.

Inclusive no que tange a estes diplomas normativos, podemos destacar que uma das suas características mais especiais é a adoção de medidas de governança distribuída, pela qual a fim de se conseguir ter mais segurança na internet, é distribuída responsabilidade mormente e anteriormente exclusiva do Estado com particulares e usuários, sendo este um dos pilares de uma política pública de sucesso no trato de questões de segurança da internet. Ou seja, a ideia de centralização e confiança plena no Estado como garantidor único de benefício e bem-estar social não mais subsiste, ainda mais em se tratando de matéria de tecnologia em uma Sociedade da Informação tal qual a que vivemos.

A governança operacionaliza-se por meio de mecanismos como subsídios, contratos e acordos de cooperação, tendo vantagens desde a capitalização do recurso à concretização das medidas elaboradas, como também o acesso a um vasto leque de profissionais especializados e a um mercado interessado na consecução do objetivo estatal, que permite, em outros termos, ter-se um melhor produto pelo melhor preço, sendo por isso assumido que os padrões desejados de atuação da boa gestão pública passam pela prestação de bens e serviços públicos de qualidade, de forma eficiente, transparente e sustentável. Em resumo, "é possível afirmar que a essência desta corrente teórica, governança, encontra-se na administração e na implementação de políticas públicas através de redes e parcerias entre governo, empresas e associações da sociedade civil" (CORREIA, SANTOS; BILHIM, 2016, p. 97).

A solução, todavia, não está em simplesmente pulverizar a responsabilidade historicamente recaída sobre o Estado, de modo que este deve, primeiro, dar condições de conhecimento técnico aos demais autores da Sociedade da Informação, o que perpassa

inevitavelmente pelo investimento em educação, e em específico para nós em educação digital. Assim "Mais do que nunca se impõe neste tempo complexo um 'novo Estado' capaz de projetar no país, uma dinâmica de procura permanente da criação de valor e aposta na criatividade" de modo a se ter, de fato, uma "Sociedade da Inteligência Competitiva" (QUESADO, 2012, p. 109).

E nesta oportunidade, qual seja, o incremento de uma educação digital, além de se verificar a prevenção no que tange à uma grande parcela dos ataques *ransomware*, também está presente a utilização de medidas técnicas que permitam a utilização de novas tecnologias pelo Estado para melhoria de sua segurança digital.

Evidentemente que a luta não é, sequer, leal. Sempre se estará a melhorar e reinventar mecanismos de combate aos diversos ilícitos que são e ainda serão perpetrados por meio da internet, como no caso do *ransomware*. De modo que "Os defensores simplesmente têm muito terreno técnico para cobrir, no qual o *hacker* já está em vantagem. Exige-se do defensor criatividade defensiva, boa *intelligence* e algum nível de automação na detenção de ataques e resposta. Aqui o Estado é necessário para dar a sua orientação e contributo" (CALDAS; FREIRE, 2013, p. 4).

Neste sentido, medidas de aplicação de novas tecnologias devem ser tomadas por governos para melhoria da segurança – seja em relação a sistemas do próprio Estado, ou mesmo disponibilização destas tecnologias, com investimento e uma política de desenvolvimento, para o setor privado.

Uma possibilidade atual é a utilização do protocolo *blockchain* na administração pública como mecanismo de proteção aos dados públicos (GOVERNMENT..., 2017).

Ambientado o cenário atual, cujo armazenamento e fluxo de informações se dá preponderantemente por meio da internet, em contraponto à vulnerabilidade da rede, faz-se necessário o desenvolvimento de aplicações que de certa maneira combatam possíveis ataques e, assim, tragam segurança aos usuários da rede, que como se propôs no presente podem ser todos os indivíduos do planeta, já que direta ou indiretamente somos atingidos por ataques cibernéticos como os exemplos mencionados anteriormente. Mais ainda quando nos deparamos com a tendência irreversível de digitalização também das atividades do Poder Público, especialmente quanto ao processamento de dados.

Desta causa e efeito, o uso do protocolo *blockchain*[7] se apresenta como possível ferramenta a proporcionar maior segurança à Administração Pública e aos dados pessoais dos

[7] Livro digital público que registra todas as operações de forma imediata (on-line), utilizando sistema de segurança avançado de criptografia que garante higidez ao sistema que aplicá-lo.

jurisdicionados, uma vez que ao Estado é devido buscar a prestação do serviço de forma eficiente, considerando-se eficiência como "modo de organizar, estruturar, disciplinar a Administração Pública, (...) com o mesmo objetivo de alcançar os melhores resultados na prestação do serviço público" (DI PIETRO, 2007, p. 74), ao passo que o serviço público assim o será somente se for capaz de garantir segurança aos usuários.

Vislumbra-se, assim, que referida tecnologia pode ter aproveitamento pela Administração Pública no que tange ao armazenamento de dados públicos, bem como na gestão e, principalmente, segurança dos dados referentes aos circunscritos nas mais diversas áreas como registro civil, cadastro de pessoas físicas e jurídicas, passaporte, título de eleitor, habilitação para dirigir, imposto de renda, propriedade imobiliária e de outros bens móveis, enfim, de toda a vida pública do cidadão.

Cumpre salientar que já se encontra legislado no Brasil a criação de um cadastro único de identidade (BRASIL, 2017), pelo qual já houve o agrupamento de diversos documentos anteriormente distintos (Registro de Identidade – RG, Cadastro de Pessoas Físicas – CPF, Carteira Nacional de Habilitação – CNH e Título de Eleitor). Vale dizer também que tal medida não é exclusividade do país, uma vez que a documentação única já é, há certo tempo, realidade em outros países. Contudo, o que importa destacar é que já haverá um cadastro único de dados do cidadão (nada obstante pudessem ter sido abrangidos outros tipos de dados como propriedade e declarações de renda, por exemplo), e que tais dados serão armazenados em servidores tradicionais, mais sujeitos a invasões, as quais, como visto anteriormente, não raramente ocorrem, com exemplos já citados e com custos de manutenção muito maiores do que o protocolo *blockchain* pode oferecer.

Da análise do objetivo da administração pública – cujo Brasil foi dado como exemplo nesta oportunidade, mas no qual se verifica uma tendência mundial de armazenamento de dados on-line –, em contraponto com a capacidade de armazenamento e segurança do protocolo *blockchain*, denota-se que a hipótese de implementação deste último é deveras factível.

Essa ideia de digitalização pode gerar receio em culturas mais tradicionalistas e cautelosas quanto à confiabilidade de sistemas eletrônicos. Para o Brasil, contudo, onde o processo eleitoral é todo digitalizado, não se vislumbra tanta resistência à implantação de um sistema totalmente digital.

Quanto à possibilidade de utilização da tecnologia em comento por governos, e o posicionamento mais restritivo adotado por uns, enquanto outros vislumbram a possibilidade de avanço em sua utilização, Don Tapscott e Alex Tapscott escrevem:

> Regulators have also snapped attention, establishing task forces to explore what kind of legislation, if any, makes sense. Authoritarian governments like Russia's have banned or severely limited the use of bitcoin, as have democratic states that should know better, like Argentina, given its history on currency crises. More thoughtful governments in the West are investing considerably in understanding how the new technology could transform not only central banking and the nature of money, but also government operations and the nature of democracy. Carolyn Wilkins, the senior deputy governor of the Bank of Canada, believes it's time for central banks everywhere to seriously study the implications of moving entire national currency systems to digital money. The Bank of England's top economist, Andrew Haldane, has proposed a national digital currency for the United Kingdom. (TAPSCOTT; TAPSCOTT, 2016, p. 109)

A propósito, já há sugestões de adaptação da tecnologia *blockchain* para criação de sistemas que protejam dados pessoais, como no trabalho de Guy Zyskind, Oz Nathan e Alex "Sandy" Pentland, que desenvolveram tecnicamente um caminho para garantir segurança a dados pessoais mediante a distribuição do armazenamento de informações (ZYSKIND, NATHAN; PENTLAND, 2015, p. 10).

Evidente que o setor público possui especificidades que demandam adaptação na implementação de ações como a que se sugere nesta oportunidade, dentre elas, por exemplo, as limitações no tocante à contratação direta de fornecedores de bens e serviços. Porém, dada a magnitude da chance de resolução, ou, ao menos, grande melhora da segurança dos dados públicos, tais questões devem se sub-rogar à ordem maior de benefício geral, não devendo prevalecer qualquer limitação de natureza ordinária.

Há também que se mencionar certa objeção que pode haver entre os governantes para adoção da tecnologia em comento, já que uma maior publicidade dos atos administrativos é inerente à utilização do *blockchain*. Como sugerem alguns, os governantes talvez sejam o maior empecilho na implementação do *blockchain* pela Administração Pública, já que ela pode significar mais facilidade para fiscalização da atividade estatal. Tal resistência pode ser oriunda das previsões futuras feitas, como por exemplo, por Melanie Swan, pelas quais o armazenamento de informações civis em *blockchain* pode, ao longo do tempo e mediante implantação global, causar uma relativização da própria essência do Estado, de modo que mediante a unificação de registros se teria apenas cidadãos do mundo, sendo o país de origem apenas e tão somente um local de origem, não determinando e caracterizando o indivíduo como é hoje, baseando-se na unificação de bancos de dados espalhados pelo mundo em que toda informação de toda pessoa seria de disponível acesso a todos, bem como transferência de bens e moedas se daria de forma irrestrita (SWAN, 2015, p. 87).

Na ideia, imagina-se, evidentemente, uma sociedade futurista, para qual pode se rumar ou não. Em curto período, contudo, a implementação do protocolo *blockchain* para armazenamento e processamento de dados públicos, ainda que individualmente entre os Estados, pode significar proteção e segurança dos mesmos.

Os benefícios vão da maior inviolabilidade do sistema à veracidade e não duplicidade das informações registradas mediante o protocolo *blockchain*, possibilitando, de imediato, maior segurança e consequentemente mais eficiência do serviço público.

Temos duas necessidades dentro de uma política pública que se busca implementar: um aspecto educacional, capaz de qualificar os usuários e inserir uma cultura de uso consciente com capacidade de prevenção de ataques (dificultando a ação dos criminosos), seja individualmente ou com relação a empresas (a partir de quando poder-se-á, então, instaurar mecanismos de governança mais permissivos); e um aspecto prático de investimento em técnicas de proteção (também de âmbito público ou de proveito dos particulares) pelo qual o Estado invista e propicie o desenvolvimento de medidas que previnam ou diminuam os efeitos de ataques característicos de *ransomware*. Como mero exemplo deste último, mas não vinculativo à opção única, está a possibilidade de uso da tecnologia inerente ao protocolo *blockchain* no armazenamento de dados públicos, sendo, todavia, infindáveis as hipóteses de implementação de novas tecnologias para a garantia de uma maior segurança na internet, sendo preponderante, em verdade, a quebra de paradigma quanto ao receio de acompanhamento da inovação tecnológica pelo Estado, sendo necessário a este imiscuir-se neste cenário, sob pena de não cumprimento de suas funções públicas.

4 CONCLUSÃO

Conclui-se, pois, após análise da doutrina levantada e dos fatos sociais evidenciados pelas notícias encartadas, no sentido de que dentro do contexto desta Sociedade da Informação, o sequestro de dados eletrônicos é efeito colateral do desenvolvimento tecnológico, potencializado principalmente pela popularização da internet, que, como visto, ocupa papel principal no panorama social atual.

Os crimes, infelizmente, passaram a ser cometidos em ambiente virtual, sendo este terreno ainda mais fértil para a prática de condutas como o *ransomware*. De tal forma, por meio deles há inegável violação a direitos fundamentais, vez que a segurança digital decorre da própria segurança pública, conforme visto.

No que concerne ao Brasil, há que se apontar o fato de que muito embora existam avanços legislativos – os quais foram analisados de maneira crítica, ou seja, contrapostos com os fatos sociais levantados em matérias jornalísticas –, como, por exemplo, a Lei nº 12.737/2012, batizada de Lei Carolina Dieckmann, não é possível concluir que já exista norma específica de combate ao *ransomware*. Isso porque do contexto em que foi promulgada, bem como por análise do dispositivo que inseriu ao Código Penal Brasileiro, não subsomem-se todas as ações tomadas pelo infrator na prática do *ransomware*, verificando a violação de dispositivo informático, prevista na lei mencionada, apenas uma etapa da prática objeto do estudo, que é mais complexa, não havendo também correspondência da pena ao seu potencial ofensivo, razão pela qual não se pode admitir como prevista a prática do *ransomware* no Brasil.

Ainda que assim não fosse, o simples existir normativo não confere efetivação e garantia de direitos. Neste sentido, a problemática está, em verdade, em como proceder para que a segurança na rede seja, de fato, assegurada. Outro caminho não há, assim, senão o combate à prática do *ransomware*. Inerente ao sucesso da investida contra esta modalidade está a utilização de ferramentas que tragam resultado prático eficaz, para além do simples legislar a matéria. Assim, pois, mais do que o que está positivado, a instrumentalização de medidas práticas pressupõe o combate eficaz ao *ransomware*.

Portanto, é preciso que a demanda integre a agenda governamental, urgentemente, de modo a proporcionar o desenvolvimento de uma política pública de combate ao *ransomware*. Como demonstrado, tal ação exige etapas e requisitos inerentes à própria teoria para implementação de uma política pública, sendo imperioso concluir que todas as exigências são atendidas para o caso estudado, de modo que, principalmente a ineficácia dos mecanismos atuais de identificação e repressão consubstanciam uma impunidade, a qual por si só já denota a problemática social e justifica a adoção de uma política pública específica. Nada obstante, ainda há que salientar que é necessária a implementação de uma educação digital, de modo a capacitar os usuários da internet para o uso adequado e com noções mínimas de segurança digital, vislumbrando a diminuição de ocorrências, vez que as invasões são em grande parte promovidas mediante abuso da ingenuidade dos usuários que abrem arquivos maliciosos e assim permitem o acesso pelos criminosos, podendo se afirmar que existe uma inércia do governo brasileiro no trato da questão, a qual demanda, como visto, a implementação de uma política pública eficaz de combate ao *ransomware* no Brasil.

REFERÊNCIAS

ANDRADE, Régis Willyan da Silva. O Diálogo entre os Direitos Fundamentais e os Direitos Humanos para criação de um Sistema Jurídico Multinível. *Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito da Unisinos*, [S.l.], v. 9, n. 1, p. 75-89, jan./abr. 2017. DOI: 10.4013/rechtd.2017.91.08.

BACCIOTTI, Karina Joelma. *Direitos humanos e novas tecnologias da informação e comunicação: o acesso à internet como direito humano.* 2014. 186 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2014. Disponível em: https://sapientia.pucsp.br/bitstream/handle/6578/1/Karina%20Joelma%20Bacciotti.pdf. Acesso em: 01 fev. 2019.

BRASIL. *Lei Federal nº 13.444, de 11 de maio de 2017.* Dispõe sobre a Identificação Civil Nacional (ICN). Brasília: Congresso Nacional, [2017]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13444.htm. Acesso em: 25 out. 2018.

BUCCI, Maria Paula Dallari. *Fundamentos para uma teoria jurídica das políticas públicas.* São Paulo: Editora Saraiva, 2013.

CALDAS, Alexandre; FREIRE, Vicente. *Cibersegurança: das preocupações à Ação.* [S.l.]: Instituto da Defesa Nacional, 2013. Disponível em: https://www.idn.gov.pt/conteudos/documentos/Working_Paper_2_Ciberseguranca_Versao_final.pdf. Acesso em: 22 out. 18.

CASTELLS, Manuel. *A sociedade em rede.* 5. ed. Rio de Janeiro: Editora Paz e Terra, 2005.

COMPARATO, Fábio Konder. *A afirmação histórica dos Direitos Humanos.* 7. ed. São Paulo: Editora Saraiva, 2010.

CORREIA, Pedro Miguel Alves Ribeiro; SANTOS, Susana Isabel da Silva; BILHIM, João Abreu de Faria. Proposta de modelo explicativo das percepções sobre gestão e políticas públicas em matéria de cibersegurança e cibercrime. *Revista da Faculdade de Letras da Universidade do Porto*, [S.l.], v. 33, p. 95-113, [s.a.]. DOI: 10.21747/08723419/soc33a5.

DA CUNHA, Paulo Ferreira. Território e Direito na sociedade da informação. *Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito da Unisinos*, [S.l.], v. 9, n. 1, p. 2-10, 2017. DOI: 10.4013/rechtd.2017.91.01.

DULLIUS, Andreia Cristina; SCHAEFFER, Paola Rucker. As capacidades de inovação em startups: contribuições para uma trajetória de crescimento. *Revista Alcance*, [S.l.], v. 23, n. 1, p. 34-50, jan./mar. 2016. DOI: 10.alcance.v.23n.1.p34-50.

DI PIETRO, Maria Sylvia Zanella. *Direito Administrativo.* 20a ed. São Paulo: Editora Atlas, 2007.

GHIRINGHELLI, Rodrigo; BASSO, Maura. Segurança Pública e Direitos Fundamentais. In: DE OLIVEIRA, Cristiane Catarina Fagundes. (Coord.). *Leituras do Direito Constitucional.* Porto Alegre: Editora EDIPUCRS, 2009.

GOVERNMENTS may be big backers of the blockchain: an anti-establishment technology faces an ironic turn of fortune. *The* Economist, 01 jun. 2017. Disponível em: https://www.economist.com/business/2017/06/01/governments-may-be-big-backers-of-the-blockchain?fsrc=scn/fb/te/bl/ed/landgrabgovernmentsmaybebigbackersoftheblockchain. Acesso em: 22 out. 2018.

HOWLETT, Michael. *Política Pública:* Seus ciclos e subsistemas. Uma abordagem integral. Rio de Janeiro: Editora Elsevier, 2013.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). *Acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal:* análise dos resultados. Disponível em ftp://ftp.ibge.gov.br/Trabalho_e_Rendimento/Pesquisa_Nacional_por_Amostra_de_Domicilios_continua/Anual/Acesso_Internet_Televisao_e_Posse_Telefone_Movel_2016/Analise_dos_Resultados.pdf. Acesso em: 21 jun. 2018.

JULIOS-CAMPUZANO, Alfonso de. La ética global de los derechos humanos: una aproximación prospectiva al impacto de las nuevas tecnologias. *Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito da Unisinos*, [S.l.], v. 3, n. 2, p. 126-139, jul./dez. 2011. DOI: 10.4013/rechtd.2011.32.02.

LÉVY, Pierre. *Cibercultura.* São Paulo: Editora 34, 1999.

LISKA, Allan; GALLO, Timothy. *Ransomware:* defendendo-se da extorsão digital. São Paulo: Editora Novatec, 2017.

MACHADO, Ronny Max; FILHO, Adalberto Simão. A nova empresarialidade e o desenvolvimento social no ambiente informacional. *Revista Jurídica Cesumar*, [S.l.], v. 18, n. 2, p. 525-548, [s.a.]. DOI: http://dx.doi.org/10.17765/2176-9184.2018v18n2p525-548.

MILLER, Lawrence. *Ransomware defense form dummies a while brand.* Nova Jersey: John Wiley & Sons, Inc., 2017.

MORENO, José. O valor econômico da informação na sociedade em rede. *Observatório OBS Journal*, [S.l.], v.9, n. 2, p. 1-28, 2015.

NASBITT, John; NASBIT, Nana; PHILIPS, Douglas. *High touch:* a tecnologia e a busca por um significado. 3. ed. São Paulo: Editora Cultrix, 2006.

NUNES, Paulo Fernando Viegas. A Definição de uma Estratégia Nacional de Cibersegurança. Disponível em: https://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD133.pdf#page=114. Acesso em: 28 set. 18.

PEZZELLA, Maria Cristina Cereser; BUBLITZ, Michelle Dias. Pessoa como Sujeito de Direitos na Sociedade da Informação: um olhar sob a perspectiva do trabalho e do empreendedorismo. *Revista Sequência*, [S.l.], v. 35, n. 68, p. 239-260, jun. 2014.

QUESADO, Francisco Jaime. A Chave da Inteligência Competitiva. *Revista Nação e Defesa*, [S.l.], v. 133, 2012. Disponível em: https://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD133.pdf#page=105. Acesso em: 22 out. 18.

SANTOS, Daniela Gonçalves Guerreiro. *A Cibersegurança em Portugal:* A ação política nacional em matéria de cibersegurança. 2016. Dissertação (Mestrado em Políticas Públicas) – Instituto Universitário de Lisboa, Lisboa, 2014. Disponível em: https://repositorio.iscte.pt/bitstream/10071/8844/3/A%20Ciberseguran%C3%A7a%20em%20Portugal.pdf. Acesso em: 20 out. 18.

SERRAGLIO, Priscila Zilli; ZAMBAM, Neuro José. Democracia e Internet: Pensando a Limitação do Poder na Sociedade da Informação. *Revista Direito, Estado e* Sociedade, [S.l.], n. 49, p. 114-141, jul./dez. 2016.

SIQUEIRA JUNIOR, Paulo Hamilton. *Teoria do Direito.* 3. ed. São Paulo: Editora Saraiva, 2012.

SUPIOT, Alain. *Homo Juridicus:* ensaio sobre a função antropológica do Direito. São Paulo: Editora Martins Fontes, 2007.

SWAN, Melanie. *Blockchain:* Blueprint for a New Economy. Sebastpol (EUA): Editora O'Reilly Media, Inc., 2015.

TADEU NASCIMENTO, Marcelo; DE MACEDO, Caio Sperandeo. O direito na sociedade da informação: a proteção aos direitos autorais e direitos conexos frente às novas tecnologias. *Universitas jus*, [S.l.], v. 27, n. 2, p. 127-137, 2016. DOI: 10.5102/unijus.v27i2.4230.

TAPSCOTT, Don. *A hora da geração digital:* como jovens que cresceram usando a internet estão mudando tudo, das empresas aos governos. Rio de Janeiro: Editora Agir Negócios, 2010.

TAPSCOTT, Don; TAPSCOTT, Alex. *Blockchain Revolution:* How the Technology Behind Bitcoin Is Changing Money, Business, and the World. [S.l.]: Penguin Random House, 2016.

ZYSKIND, Guy; NATHAN, Oz; PENTLAND, Alex "Sandy". Decentralizing Privacy: Using Blockchain to Protect Personal Data. *IEEE*, [S.l.], 2015. DOI: <10.1109/SPW.2015.27>.