A importância da proteção de dados em um mundo pós pandemia

Helmer Aguiar Pinto	Tecnólogo em Redes de Computadores. Faculdade Estácio do Ceará – (Estácio FIC) – Brasil. Email: helmerap@gmail.com

Resumo

Descoberto em Wuhan, China, em dezembro de 2019, o Coronavírus se espalhou exponencialmente pelo mundo, chegando ao Brasil em fevereiro do presente ano, com os casos notificados sendo monitorados pelas agências de saúde reguladoras. Com a evolução das ocorrências, governos de estados como São Paulo, Rio de Janeiro, Fortaleza e Manaus decretaram lockdown. A partir da ordem de bloqueio total, estabelecimentos como escolas, universidades, bancos, comércios e outros, tiveram que "fechar rapidamente as portas" para evitar o crescimento exponencial da curva de contágio, com o intuito de não colapsar o sistema de saúde, como ocorreu em países como Itália, Espanha e Estados Unidos. De maneira a não paralisar por completo as atividades, estabelecimentos de diversos setores tiveram que adaptar-se em tempo hábil para manter todos os setores e funcionários em atividade. Entretanto, muitas dessas empresas não estavam preparadas para o uso dos recursos computacionais à distância como uma solução a continuidade do trabalho, sendo de crucial importância o setor de Tecnologia da Informação - TI. Surgiu assim uma nova revolução tecnológica. Empreendeu-se implementações de acesso remoto através de VPN (*virtual private network*) para uma simulação do local de trabalho, "tunelando" através da internet em conjunto com ferramentas de segurança como criptografia e rotas de navegação, tendo como destinatário final, o firewall da empresa. Segundo dados da ACI Worldwide, com o aumento das interações digitais, as transações realizadas tiveram um salto gigantesco. Vendas online e de varejo aumentaram 209%, assim como o volume de downloads cresceu 26% em comparação com o mesmo período do ano passado. Insta frisar que com o aumento desssa transações, as tentativas de golpe também ampliaram. Um das formas mais conhecidas de ataques é através do malware ransomware, que é uma modalidade de sequestro virtual, com o intuito de arrecadar fundos das corporações mundiais. Ataques como estes, devem ser avaliados e tratados como assuntos de extrema importância, haja vista ser possível inibi-los com simples práticas e implementações de segurança em "bordas empresariais". Como uma dessas práticas de segurança está a Lei Geral de Proteção de Dados, mais conhecida como "LGPD". A finalidade principal desta lei é a responsabilidade das empresas com o armazenamento de dados dos clientes, acessos e transações de todo o seu tráfego da rede. Faz-se mister ressaltar esta lei, pois sua implementação permitirá que o órgão regulamentador, a Autoridade Nacional de Dados Pessoais, ao rastrear transações criminosas, possa assim identificar o(s) verdadeiro(s) autor(es) através de logs e registros do qual as empresas terão que obrigatoriamente manter armazenados. Em um mundo digitalmente globalizado, sabe-se que dados são tão ou até mesmo mais valiosos que dinheiro. Com a vinda da "LGPD", teremos assim uma forma de guarda e proteção dessas informações do qual são sigilosas e de extrema importância no mundo atual. Dados são futuro, e o futuro se constrói com dados.

Palavras-chave: Coronavírus, Tecnologia da Informação, Malware, Dados.

Abstract

Discovered in Wuhan, China, in December 2019, Coronavirus spread exponentially around the world, arriving in Brazil in February of this year, with reported cases being monitored by health regulatory agencies. With the evolution of the occurrences, governments of states such as São Paulo, Rio de Janeiro, Fortaleza and Manaus decreed lockdown. From the order of total lockdown, establishments such as schools, universities, banks, businesses and others had to "quickly close the doors" to avoid the exponential growth of the contagion curve, in order not to collapse the health system, as occurred in countries like Italy, Spain and the United States. In order not to paralyze completely the activities, establishments of diverse sectors had to adapt in time to maintain all the sectors and employees in activity. However, many of these companies were not prepared for the use of computer resources at a distance as a solution to the continuity of the work, being of crucial importance the sector of Information Technology - IT. Thus emerged a new technological revolution. Remote access implementations were undertaken through VPN (virtual private network) for a workplace simulation, tunneling through the Internet together with security tools such as encryption and navigation routes, with the company's firewall as the final recipient. According to data from ACI Worldwide, with the increase in digital interactions, the transactions carried out had a giant leap. Online and retail sales increased 209%, as well as the volume of downloads grew 26% compared to the same period last year. It is important to emphasize that with the increase of these transactions, the coup attempts have also expanded. One of the most known forms of attacks is through the malware ransomware, which is a modality of virtual kidnapping, in order to raise funds from the world corporations. Attacks like these must be evaluated and treated as extremely important subjects, since it is possible to inhibit them with simple practices and security implementations in "business borders". One of these security practices is the General Law of Data Protection, better known as "LGPD". The main purpose of this law

is the responsibility of companies with the storage of customer data, accesses and transactions of all their network traffic. It is important to emphasize this law, because its implementation will allow the regulating organ, the National Authority of Personal Data, when tracking criminal transactions, to identify the true author(s) through logs and registers of which the companies will have to keep mandatorily stored. In a digitally globalized world, it is known that data is as or even more valuable than money. With the coming of "LGPD", we will thus have a form of guarding and protection of this information of which it is confidential and of extreme importance in the current world. Data is future, and the future is built with data.

Keywords: Coronavirus, Information Technology, Malware, Data.

Introdução

Ao dar andamento e desenvolvimento do artigo em questão, levantou-se o cenário atual do mundo no ano de 2020. Estamos em um mundo no qual não se sabe as cenas dos próximos capítulos, visto que não se tem nenhuma exatidão do paradeiro e melhoria da doença que aflinge a esfera global.

É de grande importância comentarmos como está o cenário de todo esse ano. Começaremos a entender a origem da doença, e como ela se transformou em pandemia. Analisaremos as etapas vivenciadas por todos os países e como seus governantes agiram para combater esse mal atual.

No texto em questão, iremos abordar a importância da tecnologia em tempos de pandemia e como ela pode auxiliar o dia-a-dia de todos os trabalhadores mundiais, visto que quase todos os setores tiveram paradas e muitos deles obtiveram apoio através de acesso remoto de colaboradores das empresa.

Por fim navegaremos em uma Grande mudança na Lei brasileira e abordaremos a chegada da Lei Geral de Proteção de Dados no território brasileiro, no qual entra em foco nesse momento atual devido ao fato que tudo se resume aos dados, sejam empresariais ou pessoais. Essa traz consigo uma aplicação e abordagem inovadora no território brasileiro no que tange aos dados das pessoas em paralelo ao que pensamos e imaginamos que tempos de "privacidade" em navegações e acessos que diariamente fazemos em nossos computadores e celulares.

Desenvolvimento

A virada do ano 2019/2020 vai entrar para história, mas não por ser a virada do milênio ou algo parecido, mas como o marco do início da maior pandemia dos últimos 50 (cinquenta anos). O início desse período turbulento deu-se com a Organização Mundial da Saúde (OMS), sendo alertada sobre vários casos de pneumonia na cidade Wuhan, província de Hubei, China em dezembro de 2019. Desde então, os números de doentes aumentaram em larga escala, surgindo assim as primeiras vítimas letais.

Cientistas descobriram que essa doença infecciosa estava sendo causada por uma família grande de vírus comuns, o Coronavírus. Esse vírus previamente não tinha sido ainda identificado em seres humanos, pois além de ser oriundo de espécies animais como camelos, gatos, gados e especialmente, morcegos, raros são os casos que animais possuem potencial ofensivo contra a espécie humana. Atualmente popular e conhecido como COVID-19 ou SARS-COV-2 é a variação que infecta seres humanos e tem origem animal do morcego. Apresenta um espectro clínico que varia entre infecção assintomática ou oligossintomáticas (poucos sintomas), sendo que desses casos, 20% deles requer um atendimento hospitalar devido a dificuldade respiratória e que aproximadamente 5% podem necessitar de suporte vacilatório. É interessante ressaltar que, muitas vezes o Covid-19 pode ser confundido com um simples resfriado com sensação de febre, dor de garganta, dor de cabeça, tosse e coriza, podendo ir até uma pneumonia severa. Um diagnóstico clínico completo, pode ser realizado a partir dos seguintes critérios: diagnóstico clínico, diagnóstico clinico-epidemiológico, diagnóstico clínico-imagem, diagnóstico laboratorial e diagnóstico laboratorial em indivíduo assintomático.

Apesar de vídeos de pessoas passando mal na rua e cidades chinesas paralisadas, o mundo não se preocupou. Tudo parecia muito longíquo e extremamente desesperador, para um país que há alguns anos atrás vencera a gripe aviária sem mais alardes. A população mundial só começou a preocupar-se com a gravidade da doença quando surgiram os casos na Itália, seguidos das cenas de pessoas sendo transportadas em macas completamente fechadas e médicos vestidos como se estivessem indo para uma viagem lunar e vários caixões sendo colocados em caminhões. Após a Itália, o Covid-19 atingiu gravemente Espanha, Estados Unidos e Brasil, fazendo que os governantes desses e de países fronteiriços tomassem medidas com o intuito de frear o contágio.

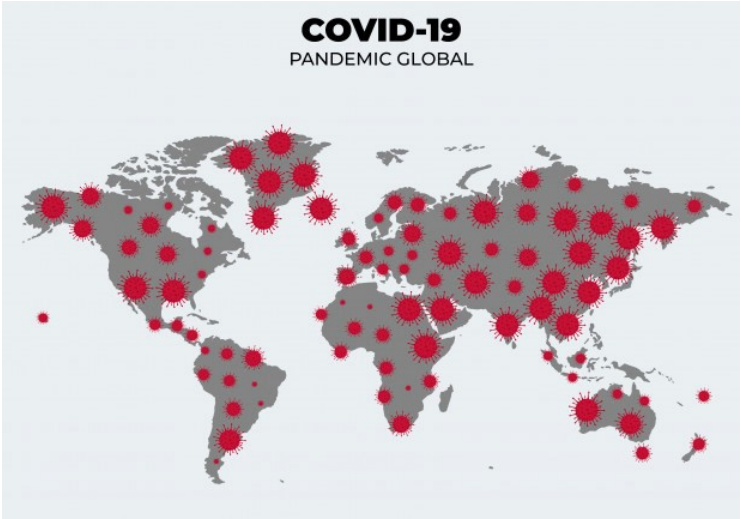

Imagem 1 Lugares atingidos pela epidemia do COVID-19

Dentre as medidas tomadas para frear o crescimento de caso da doença, adotou-se algumas medidas mais enérgicas como: quarentena, isolamento social e o lockdown. Por esses três termos serem bastante confundidos, importante mencionar aqui, de forma resumida, suas diferenças.

A quarentena é exatamente a recomendação para pessoas que tiveram o contato com pacientes contaminados pelos vírus ou que estiveram em regiões com surtos da doença, sendo o período determinado de isolamento ser de acordo com o período de incubação do vírus, o qual varia entre 1 e 14 dias. Já o isolamento social é uma recomendação médica para pessoas que podem ter tido contato com algum paciente infectado e estão aguardando o resultado do exame ou que tenham o diagnóstico confirmado. Para um efetivo controle, é recomendado que se isolem das demais pessoas a fim de evitar a propagação da doença.

Por fim, o lockdown consiste em restringir a circulação da população em lugares públicos, permitindo apenas a utilização de serviços essenciais e de forma limitada, como farmácias, supermercados ou hospitais.

Com a evolução das ocorrências, governos de estados como São Paulo, Rio de Janeiro, Fortaleza e Manaus decretaram lockdown. A partir da ordem de bloqueio total, estabelecimentos como escolas, universidades, bancos, comércios e outros, tiveram que "fechar rapidamente as portas" para evitar o crescimento exponencial da curva de contágio, com o intuito de não colapsar o sistema de saúde, como ocorreu em países como Itália, Espanha e Estados Unidos. De maneira a não paralisar por completo as atividades, estabelecimentos de diversos setores tiveram que adaptar-se em tempo hábil para manter todos os setores e funcionários em atividade. Entretanto, muitas dessas empresas não estavam

preparadas para o uso dos recursos computacionais à distância como uma solução a continuidade do trabalho, sendo de crucial importância o setor de Tecnologia da Informação - TI. Surgiu assim uma nova revolução tecnológica.

Redes e Pandemia

No mundo pós-pandemico que encontramo-nos hoje, foi necessário empreender várias implementações de acesso remoto através de VPN (Virtual Private Network) para uma simulação do local de trabalho. Em uma pesquisa comandada por Paulo Brito, uma empresa como a CISCO, gigante mundial em conectividade e líder no mercado, enfrentou problemas para administrar acesso remoto seguro de 140 mil funcionários e parceiros, com 130 mil dispositivos, dos quais 55 mil BYOD em 498 escritórios de 94 países.

A adoção repentina de VPNs para o home office de funcionários pegou a maioria das empresas de surpresa. Poucas empresas têm VPNs e dispositivos disponíveis para todos os funcionários, aumentando assim a utilização de dispositivos pessoais, BYOD - Bring Your Own Device, e consequentemente o nível de recursos de segurança na empresa, como softwares de anti-vírus.

Vale ressaltar que mesmo tendo o máximo de cuidado, a rede utilizada pelos funcionários em home office será a doméstica, que não convém de um ambiente seguro e robusto como em uma rede corporativa, sendo este ambiente doméstico passível de ataques de softwares maliciosos e de programas do tipo malware, sendo o mais preocupante para um ambiente corporativo o ransomware, no qual deixa todos o ambiente atacado sem utilização alguma através de um sequestro virtual dos dados mediante pagamento financeiro. Demonstrando que a utilização de VPN ainda é a melhor forma de proteger os dados empresariais ao trabalhar de casa.

Pode-se falar das características de utilização de VPN em home office para funcionários que por meio da criptografia nas informações e nas comunicações entre *hosts* da rede privada é possível aumentar consideravelmente a confidenciabilidade dos dados que trafegam pela rede. Por meio do sistema de *tunelamento*, os dados podem ser enviados sem que outros usuários tenham acesso, e mesmo que os tenham, ainda os receberão criptografados. Por isso, é fundamental que a empressa possa cuidar da rede VPN e ser capaz de garantir segurança e integridade das informações e dos dados que são transmitidos, diferentemente de uma rede doméstica, visto que a doméstica não possui criptografia e nem gerenciamento de utilização do acesso à internet.

A utilização de redes públicas tende a apresentar custos muito menores que os obtidos com a implantação de redes privadas, sendo este, justamente o grande estímulo para o uso de VPNs. No entanto, para que esta abordagem se torne efetiva, a VPN deve prover um conjunto de funções que garanta “Confidencialidade, Integridade e Autenticidade”. Pelo conceito de confidencialidade, entendemos a tarefa de interceptar uma seqüência de dados, sendo imprescindível que os dados que trafeguem sejam absolutamente privados, de forma que, mesmo que sejam capturados, não possam ser entendidos. Por integridade, caso os dados sejam capturados, é necessário garantir que estes não sejam adulterados e re-encaminhados, de tal forma que quaisquer tentativas nesse sentido não tenham sucesso, permitindo que somente dados válidos sejam recebidos pelas aplicações suportadas pela VPN. Com a autenticidade, somente usuários e equipamentos que tenham sido autorizados a fazer parte de uma determinada VPN é que podem trocar dados entre si; ou seja, um elemento de uma VPN somente reconhecerá dados originados em por um segundo elemento que seguramente tenha autorização para fazer parte da VPN.

Lei Geral de Proteção de Dados

Com alterações necessárias e mudanças à nível mundial, faz se necessário mencionarmos a Lei geral de Proteção de Dados (LGPD) brasileira que veio regular o tratamento de dados pessoais, conforme lei 13.709/2018 sancionada em 14 de agosto de 2018. A finalidade principal desta lei, conforme disposto em seu artigo 1º é o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Conforme o nome da lei, o artigo 2º dá ênfase em quais fundamentos e o que será assegurado com a aplicação da mesma. Vejamos:

> 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;
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Com todo o exposto nos artigos retromencionados, vale ainda mencionar o artigo 5º da referida Lei:

Art. 5º Para os fins desta Lei, considera-se:
I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019)
IX - agentes de tratamento: o controlador e o operador;
X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Redação dada pela Lei nº 13.853, de 2019)
XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (Redação dada pela Lei nº 13.853, de 2019)

O início de sua vigência estava previsto para agosto deste ano, o que conferiu ao mercado um prazo de 2 anos para adaptação. Em razão da pandemia, a vigência da lei foi adiada para o dia 3 de maio de 2021 e posteriormente a Lei 14.010 também afetou a vigência da LGPD, ao postergar para 1 de agosto de 2021 a aplicação das suas sanções.

Os malefícios com o adiamento da LGPD tendem a deixar os benefícios em segundo plano diante das implicações que a pretendida prorrogação têm com diferimento dos direitos e deveres estabelecidos pela lei. A perpetuação da lacuna atual de um marco regulatório específico à proteção de dados deixa milhões de pessoas à mercê de abusos e violações à privacidade. Também corrobora para este cenário de insegurança a omissão governamental à instalação da Autoridade Nacional de Proteção de Dados Pessoais, pois, sem parâmetros ou regras de utilização dos dados pessoais estabelecidos pela ANPD, o cenário de incertezas só aumenta. Por outro lado, os benefícios com a proposta de dilação da *vacatio legis* da LGPD, permite tanto que o Poder Público como os particulares (pessoas e empresas), tenham mais tempo para se adaptar aos termos da LGPD, especialmente em razão da emergência de saúde pública causada pelo coronavírus. Não se pode ignorar, por fim, a possibilidade de retardamento da imposição de sanções previstas na LGPD para agosto de 2021, prevista pelo projeto de lei 1.179/20. Claro que tal adiamento, como dito, depende da aprovação da Câmara dos Deputados e, posteriormente, da sanção presidencial, todavia, referido diferimento não é coerente à própria pretensão de adiamento de vigência da lei. A LGPD desprovida de sanções é nada mais nada menos que "letra morta" e pode colidir com os interesses estatais de aumento de receita com aplicação de sanções.

Assim, a adaptação das empresas à LGPD é uma medida relevante que permite às empresas aperfeiçoarem suas práticas, procedimentos internos e estruturas, criando uma relação transparente não só com os cidadãos titulares dos dados, mas também com os parceiros. Vale frisar ainda que, embora vista apenas como custo por alguns, estudos recentes demonstram que a proteção de dados gera valor para as Companhias Com o adiamento da vigência da LGPD sendo até justificavél, no mundo atual, devido a atual conjuntura, a nova legislação amplia a eficácia dos direitos e deveres da proteção e sigilo dos dados em um cenário pós pandemia. Ao contrário de tudo o que estamos vivenciando, sigilo e privacidade não são mais "direitos" na prática e sim "luxo" atualmente. Tiro isso devido ao fato que em meio a crise pandêmica, o governo Russo passou a rastrear os cidadãos através de QR CODE ao transitar pelas cidades, noticia essa veiculada na rede CNN Brasil. Na mesma linha de raciocínio foi Brasil ao debater o uso de dados das operadores de celular a fim de controlar aglomerações.

Privacidade na Internet

Em 1969, foi criada a Arpanet pela ARPA (*Advanced Research Projects Agency*), com a função de conectar laboratórios de pesquisa, pertencendo ao DOD (Departamento de Defesa dos Estados Unidos). Desta maneira, a Arpanet pode ser considerada um ancestral da atual famosa Internet.

No apogeu da Guerra Fria, a Arpanet era a garantia das comunicações e o armazenamento de informações sigilosas, pois permitia a troca e o compartilhamento de informações através de um chaveamento de pacotes, isto é, sistema de transmissão de dados em rede de computadores, no qual as informações eram divididas em pequenos pacotes que, por sua vez, continham trecho dos dados, o endereço do destinatário e informações que permitiam a remontagem da mensagem original. Após isto, no ano de 1989, no Laboratório Europeu de Física, situado em Genebra, foi criado o *world wide web*. No Brasil, a Rede só foi instalada em 1989 pelo governo federal, através do Projeto da Rede Nacional de Pesquisa – RNP.

Hoje, a Internet é um dos principais meios de comunicação; sendo todo e qualquer tipo de informação compartilhada pela rede acessível em todo o mundo em segundos.

A quantidade de conteúdos e informações disponíveis na rede é vasta com a utilização de serviços e recursos acessíveis, como *e-mail, Google, Facebook* etc, estando apenas a um clique. Mas toda essa facilidade é também prejudicial, porque pode ser utilizada para a prática de condutas delituosas, configurando crime, o qual pode ser cometido com o computador ou contra o computador.

Existem inúmeras formas de se invadir a privacidade dos usuários na internet. A utilização de programas maliciosos para ter acesso às informações é bastante conhecida no mundo virtual. *Spyware, Malware, Keyloggers, Spam* e *Phishing* são apenas alguns dos programas. A finalidade destes é praticamente a mesma, ou seja, recolhem informações do usuário a respeito de seus costumes e transmitem estas informações para outros, podendo ser pessoas físicas, entidades e, até mesmo, governos. Há ainda a *Deep Web* ou *Web* Invisível, caracterizando a rede que não faz parte da *Surface Web* e de tamanho maior em comparação a esta. Alguns estipulam que a *Deep Web* compreenda 96% da Web e aquela que nós utilizamos e conhecemos *Surface*, apenas 4%.

Conclusão

Portanto, com o exposto durante o desenvolvimento, podemos concluir que nesse cenário pós pandemia visualizamos a importância do trabalho remoto na vida de todos os trabalhadores. Trabalho esse que possa assegurar uma segurança das informações e proteção dos dados empresariais e pessoais através de ferramentas que proporcionem criptografia com confiabilidade.

Pode-se falar ainda que conseguimos entender um pouco melhor como o governo está tratando e como pretende impor limites para quem não "respeitar" o ambiente remoto em que estamos vivendo, sendo isso tratado em uma Lei já aprovada e que encontra-se proximo de vigorar.

Referências

BRASIL. Lei nº 13.709, de 10 de agosto de 2018. Institui a Lei Geral de Proteção de Dados (LGPD). Diário Oficial da União: 15/08/2018, pág. nº 59.

BRITO, Paulo: Adoção repentina de VPNs pegou até a Cisco de surpresa. 05 de abril de 2020. Disponível em **<**https://www.cisoadvisor.com.br/adocao-repentina-de-vpns-pegou-ate-a-cisco-de-surpresa/**>.** Acesso em 09 de setembro de 2020

CIPOLI, Pedro: O que é VPN? Disponível em <https://canaltech.com.br/internet/o-que-e-vpn-23748/#:~:text=VPN%20ou%20Virtual%20Private%20Network,rede%20p%C3%BAblica%2C%20como%20a%20Internet.>. Acesso em 10 de outubro de 2020

ILYUSHINA, Mary: Moscou passa a rastrear população e levanta preocupações com privacidade. 14 de abril de 2020. Disponível em <https://www.cnnbrasil.com.br/tecnologia/2020/04/14/moscou-passa-a-rastrear-populacao-e-levanta-preocupacoes-com-privacidade>. Acesso em 10 de outubro de 2020.

MAGENTA, Matheus: Coronavírus: governo brasileiro vai monitorar celulares para conter pandemia. 03 de abril de 2020. Disponível em <https://www.bbc.com/portuguese/brasil-52154128>. Acesso em 01 de outubro de 2020.

SOARES, Paulo Vinícius de Carvalho Soares; **TENORIO,** Caio Miachon: Benefícios e malefícios da prorrogação de vigência da LGPD. 30 de abril de 2020.
Disponível em <https://migalhas.uol.com.br/depeso/325787/beneficios-e-maleficios-da-prorrogacao-de-vigencia-da-lgpd>. Acesso em 01 de outubro de 2020.

Bibliografia Consultada

BAUMAN, Zygmunt; **LYON,** David. Vigilância líquida. Rio de Janeiro: Zahar, 2014.

MORAIS, Alexandre de. Direito Constitucional. 16ª.ed. São Paulo: Atlas, 2004.