Elba Vieira

Doutoranda em Ciência da Informação pela Universidade Federal da Bahia (UFBA). Profissional com sólida experiência nas áreas de Segurança da Informação, Tecnologia e Riscos. Co-Autora da obra "LGPD – Lei Geral de Proteção de Dados Pessoais – Manual de Implementação" (Editora Thomson Reuters - 2019). Palestrante e painelista do "Datacenter Dynamics" e jurada do "Datacenter Dynamics Awards".

Resumo: O isolamento social, provocado pela pandemia gerada pelo novo corona-vírus e a COVID-19 (doença associada ao vírus), transformou a rotina das empresas no mundo inteiro, forçando-as a dar respostas adequadas em um curto espaço de tempo. Uma delas é o trabalho remoto, instrumento já utilizado, mas que teve uma expansão significativa neste período. O planejamento e uso adequado desta modalidade laboral, dentro do contexto da gestão de crises, planos de continuidade de negócios, programas de segurança cibernética nem sempre fazem parte do arcabouço estratégico das empresas. Neste novo cenário mundial, as dúvidas começam a pairar na mente de líderes de negócios e profissionais em geral, sobre como utilizar mecanismos para se proteger, trabalhando fora dos limites físicos das empresas, através de recursos corporativos ou próprios. Ao mesmo tempo, criminosos aproveitam o momento de fragilidade para explorar o tema "corona-vírus" e tudo que está em seu entorno, atingindo empresas e indivíduos. Este artigo tem o objetivo de discorrer sobre estes assuntos, trazer reflexões e propor algumas recomendações de segurança para minimizar os riscos e armadilhas no mundo digital.

Palavras-Chave: Novo Corona-Vírus. COVID-19. Trabalho remoto. Segurança Cibernética.

1. CENÁRIO ATUAL

Virada de um novo ano. Era 1º de janeiro de 2020 e, naquele dia, nem a melhor de todas as previsões imaginava o que estava por vir nas mudanças abruptas de rota deste grande barco chamado "Terra". E aquela que, possivelmente, é a maior ameaça à raça humana, neste século, continua avançando de forma assustadora, subtraindo vidas, debilitando a saúde de milhares de pessoas, devastando o emocional de centenas de famílias e desafiando a mente de cientistas e pesquisadores do mundo inteiro. Estamos falando do novo "Corona-Vírus" e da doença que ele provoca ao infectar um organismo humano: a COVID-19.

Estamos iniciando o segundo trimestre do ano e, ao longo de apenas 3 meses, já percebemos mudanças radicais na vida de bilhões de pessoas em quase todos os países do globo, provocadas pelos efeitos devastadores deste vírus: talvez a maior delas seja a necessidade do isolamento social para reduzir o contato físico entre as pessoas, minimizar a disseminação do vírus para não colapsar os sistemas de saúde pelo mundo e evitar perdas humanas, conforme orientações da OMS[1], que oficializou a doença como uma pandemia, durante o mês de março.

Considerando que o isolamento social tornou-se necessário, milhões de pessoas passaram a realizar inúmeras tarefas de suas casas, como uma resposta rápida das empresas em meio à crise, o que inclui a realização de atividades laborais, através dos equipamentos e ferramentas de tecnologia à sua disposição, os quais, na maioria das vezes, são recursos próprios. Estamos falando do trabalho à distância, ou "trabalho remoto" ou "teletrabalho" que é considerado qualquer acesso feito à uma rede corporativa, através de conexões externas, fora das instalações físicas da empresa.

A CLT[2] possui um capítulo específico que trata do teletrabalho, definindo-o como "a prestação de serviços preponderantemente fora das dependências do empregador, com a utilização de tecnologias de informação e de comunicação que, por sua natureza, não se constituam como trabalho externo".

Já o termo "Home-Office" é uma modalidade do trabalho remoto, visto que sua realização é feita na residência do colaborador (vou aqui usar esse termo para generalizar o conceito de empregado, funcionário etc). Uma definição interessante que li recentemente na HSM Management[3] foi: "o termo home office já nos dá uma boa dica

[1] Organização Mundial de Saúde (World Health Organization – WHO).
Disponível em: https://www.who.int/emergencies/diseases/novel-coronavirus-2019
[2] Consolidação das Leis Trabalhistas.
Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm
[3] HSM Ebook "Liderança e Trabalho Remoto".
Disponível em: https://materiais.revistahsm.com.br/lideranca-trabalho-remoto

do que efetivamente acontece em nossas vidas ao adotar esse modelo de trabalho: a casa é o escritório e o escritório é a casa. Assim, sem separação. E manter uma rotina produtiva, apesar de ser difícil em especial para quem está iniciando, não é o nosso maior desafio. Para que o trabalho flua e as pessoas se engajem precisamos atualizar nosso modelo mental".

Hoje, o trabalho remoto saiu de lá do fim da fila de prioridades das empresas e precisou ser adotado às pressas, de forma massiva, tornando-se um dos principais pilares que as sustentam, para que possam manter o funcionamento de suas operações através de seus colaboradores, possibilitando sua sustentação no mercado. Políticas e processos foram criados ou revisados e equipamentos, ferramentas e dispositivos tecnológicos foram adaptados para suportar esta nova realidade.

O trabalho remoto é, inclusive, uma resposta das empresas ao enfrentamento de crises, não somente como agora, em plena pandemia, mas em situações outras de catástrofes de grandes dimensões, como inundações, furacões, falta de energia elétrica, epidemias, etc, devendo ser considerado como uma das medidas de segurança a ser formalizada em planos de continuidade de negócios.

Já sabemos que o isolamento social "retirou" milhões de pessoas de seus ambientes físicos de trabalho. Muitas dessas pessoas já estavam acostumadas ao trabalho remoto (eu, inclusive), algumas até declaram-se "nômades digitais" que podem estar em qualquer local do planeta para realizar suas atividades. Mas, talvez a maioria não esteja acostumada a esta nova forma de trabalho.

Costumo dizer que, pra tudo, existem ônus e bônus. Com o trabalho remoto não é diferente. Estar mais tempo com a família, dar adeus ao trânsito, reduzir despesas com os automóveis, reduzir stress com a loucura dos grandes centros urbanos e reduzir índices de carbono na atmosfera são alguns benefícios de estar em sua própria residência e dela sair para trabalhar apenas com alguns "cliques" em seus equipamentos e recursos tecnológicos. Mas a rotina caseira não possui tanto "glamour" quanto parece. É preciso disciplina para não perder o foco com tantas distrações em casa (família, casa, comida, compras, animais de estimação, etc etc).

Bem, o momento é de crise e nela precisamos nos adaptar e ressignificar muitas coisas. Somos testados a todo momento para tomada de decisões diante de novas situações e, para a maioria das pessoas, trabalho remoto é sinônimo de uma nova situação. A empresa está preparada para o trabalho remoto em maior escala? Existem políticas e normas que definem e orientam diretrizes de segurança? O que colaboradores podem ou devem fazer, ao utilizar seus computadores pessoais para trabalhar remotamente? É necessário utilizar ferramentas de segurança específicas? Estas são apenas algumas reflexões sobre os atuais desafios.

Matutando sobre todas essas questões, minha proposta aqui é discorrer sobre ameaças digitais e armadilhas que cercam o mundo do trabalho remoto, pontos importantes relacionados à segurança cibernética e algumas recomendações que podem servir para minimizar riscos e evitar incidentes que impactam, significativamente, as operações essenciais de infraestruturas críticas.

Critérios e riscos trabalhistas precisam ser igualmente considerados, mas este assunto não faz parte do escopo deste artigo. Considero importante o acionamento da área jurídica das empresas para, em tempo, ajustarem e formalizarem os instrumentos necessários ao trabalho remoto dos colaboradores, em função das bases legais que precisam ser observadas.

2. RISCOS E ARMADILHAS

Para além da geladeira recheada de guloseimas, há muitos desafios a serem superados num dia de trabalho em casa, principalmente quando se trata de um ambiente tecnológico não corporativo (e, portanto, mais exposto às ameaças digitais). A segurança no acesso a dados corporativos, dados pessoais (e sensíveis), não pode ser comprometida. As empresas precisam identificar, formalizar e comunicar diretrizes e recomendações que devem ser seguidas pelos seus colaboradores.

Infelizmente, o crime cbernético (*Cyber Crime*) costuma ter aumento expressivo em períodos de fragilidade e comoção mundial, como agora. Criminosos disseminam códigos maliciosos (*malwares*) pela Internet, vasculham redes vulneráveis a ataques, espalham informações falsas com os temas em destaque e *links* para sites programados em obter dados pessoais, anexam arquivos com vírus e outras pragas digitais e enviam e-mails para um grande número de contas, usam engenharia social para persuadir pessoas, espalhando caos e terror.

A The Shift[4] publicou uma matéria muito interessante sob o tema dos riscos de uma "ciberpandemia" (fazendo referência a um importante estudo elaborado pelo *Cambridge Centre for Risk Studies* e pela seguradora *Lloyd's*), dizendo que "Em 24 horas, um só e-mail infectado, aberto e passado adiante, poderia infectar 30 milhões de dispositivos digitais travando, com um *ransomware*, os sistemas de mais de 600 mil empresas no mundo todo. O custo dessa ciberpandemia seria de US$ 193 bilhões, dos quais apenas 14% teriam algum tipo de seguro contra ciberataques, deixando portanto um rastro de prejuízo de US$ 166 bilhões". Para um momento já tão difícil, os impactos

[4] Plataforma de jornalismo de dados, com foco em inovação disruptiva. É comandada pelas jornalistas Cristina De Luca e Silvia Bassi. Disponível em: https://mailchi.mp/theshift/newsletter-theshift-o-contexto-da-ruptura-12410612?e=0cf9ad014f

causados por uma ciberpandemia poderia colapsar a Internet e isso causaria consequências assustadoras.

Penso que o momento é de cooperação, para que seja possível sobrevivermos a este cenário. Como diz o incrível Harari[5], em seu recente ensaio "Na batalha contra o coronavírus, faltam líderes à humanidade": "O verdadeiro antídoto para epidemias não é a segregação, mas a cooperação". E segue, logo depois, dizendo que "Sem confiança e solidariedade globais não seremos capazes de parar a epidemia do coronavírus, e é provável que enfrentemos mais epidemias desse tipo no futuro. Mas toda crise é também uma oportunidade".

O crime cibernético existe há bastante tempo, mas, lembrando que "a oportunidade faz o ladrão", é importante refletir sobre o grande volume de pessoas envoltas no tema da pandemia, conectadas na rede mundial, acessando e compartilhando conteúdos em aplicativos, redes sociais, e-mails e tantas outras ferramentas. Riscos e armadilhas sempre vão existir. O importante é identificá-los e tratá-los de forma planejada e segura, dentro das possibilidades de cada empresa.

3. ESTRATÉGIAS PARA LÍDERES

O momento é crítico, complexo, vulnerável e muda a todo instante. Líderes devem ser capazes de observar o cenário, observar as demandas e necessidades de sua empresa, seus colaboradores e, com base nas condições e ferramentas que tem em mãos, devem atuar da forma mais adequada e possível.

Líderes devem deixar claro, aos seus colaboradores, como riscos de segurança devem ser gerenciados durante o período de uso do trabalho remoto, quais medidas de segurança estão definidas para minimizar os riscos, quais políticas, normas e procedimentos de segurança devem ser executados, o que fazer em caso de incidentes e, ao longo de todo o processo, orientar e comunicar novas diretrizes ou diretrizes alteradas.

Considerando que ameaça é a "causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização", segundo a norma de segurança ABNT ISO/IEC 27002:2013[6] e que, pela mesma norma, vulnerabilidade é a "fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças", os

[5] Yuval Noah Harari. Israelense, Ph.D. em história pela Universidade de Oxford e professor universitário. Disponível em: https://www.amazon.com.br/batalha-coronav%C3%ADrus-l%C3%ADderes-humanidade-Companhia-ebook/dp/B086H52P1N/ref=sr_1_1?qid=1586793820&refinements=p_27%3AYuval+Noah+Harari&s=books&sr=1-1

[6] Código de prática para controles de segurança da informação. Associação Brasileira de Normas Técnicas (ABNT). Disponível em: www.abnt.org.br

líderes precisam estar atentos às ameaças que podem se transformar em vetores de ataques para suas empresas, precisam identificar e estar atentos às vulnerabilidades existentes em seus ativos (tecnológicos, pessoas, processos e ambientes).

Medidas de segurança são importantes para minimizar riscos, visto que eles são a "possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos causando, dessa maneira, impactos e prejudicando a Organização", de acordo com a norma de segurança ABNT ISO/IEC 27005:2019[7].

Essa mesma norma define que gestão de riscos é um processo sistemático que identifica e trata os riscos de forma contínua e periódica. Num momento de graves crises é importante que, ao menos, seja possível identificar os ativos mais críticos, os dados pessoais sensíveis, os sistemas e aplicações essenciais para os negócios, identificando os riscos com maior probabilidade de ocorrência e de maior impacto e criar e aplicar medidas para reduzir estes riscos, já que ele pode ser um indicador de certezas e incertezas às quais as empresas estão sujeitas.

A ausência de políticas e normas de segurança que estabelecem critérios e práticas positivas a serem disseminadas entre os colaboradores de uma empresa, pode também ampliar a superfície de riscos associados ao trabalho remoto, estando eles conectados à rede corporativa através de equipamentos fornecidos pela empresa ou através de sua rede doméstica (onde o risco é maior).

Um outro ponto que deve ser observado é a comunicação. Ela precisa ser clara, objetiva e transversal, sendo possível que todos entendam as diretrizes no uso do trabalho remoto, seja em formato "home-office" (em casa) ou em qualquer outro local. Todos devem conhecer as políticas relacionadas a este formato de trabalho, estar atentos aos riscos e tomar os cuidados necessários quando estiverem trabalhando.

Enfim, a cultura de segurança da informação deve ser vista como diferencial na empresa e que dará suporte à sua reputação e confiança digital perante clientes, acionistas, fornecedores e à sociedade. O velho e bom trinômio Pessoas – Processos – Tecnologias deve ser considerado em todas as estratégias de segurança nos negócios.

4. AÇÕES EM SEGURANÇA CIBERNÉTICA

A segurança de qualquer ambiente (físico ou digital) é tão forte quanto seu elo mais fraco. Este famoso ditado tem um significado diferenciado no momento atual. Identificar os ativos mais expostos e vulneráveis e aplicar medidas de segurança para

[7] Gestão de riscos de segurança da informação. Associação Brasileira de Normas Técnicas (ABNT). Disponível em: www.abnt.org.br

deixá-los impermeáveis ao risco cibernético, é uma atitude mais que essencial, ela deve ser considerada como uma das primeiras ações a serem adotadas.

A seguir, apresento algumas recomendações (não é uma lista definitiva).

A. Se os recursos e ferramentas para trabalho remoto forem fornecidos pela empresa, para manter um nível adequado de segurança, é importante:

1) ATUALIZAR sistemas operacionais, anti-vírus (e qualquer anti-malware) instalados nos dispositivos corporativos (computadores, notebooks, tablets, celulares etc);
2) PROVER a conexão remota dos colaboradores, através de ferramentas com segurança adequada (a exemplo de VPN – *virtual private network*), estabelecendo conexões confiáveis e seguras com uso de criptografia (o mesmo critério deve valer para aplicações e dados que estiverem armazenados em nuvem);
3) CRIAR autenticação da ferramenta de acesso remoto com duplo fator, se assim for possível;
4) DEIXAR claro, aos colaboradores, que o acesso remoto deve ser utilizado para fins exclusivos da empresa;
5) CRIAR credenciais de acesso individualizadas, identificando e responsabilizando seu titular, através do uso de usuário e senha de acesso;
6) CRIAR regras de formação da senha (tamanho, troca no primeiro acesso, uso de senhas fortes, etc), coerentes com política e normas já existentes na empresa;
7) DEFINIR quem deverá indicar os colaboradores que vão trabalhar em regime de acesso remoto com os recursos corporativos;
8) DEFINIR os privilégios de acesso (quem vai acessar o quê) e por quanto tempo;
9) UTILIZAR ferramentas que usem criptografia para promover níveis de segurança adequados ao tráfego;
10) DEIXAR claro que dados pessoais (e sensíveis), além de sistemas e aplicativos críticos devem ser utilizados de forma responsável pelos colaboradores, respeitando a privacidade dos indivíduos;
11) PROVIDENCIAR o registro e a guarda das trilhas dos acessos (logs) nas ferramentas de acesso remoto, armazenando, pelo menos, código do usuário, nome, área, data e hora do acesso e os sistemas, aplicações e produtos utilizados. Isso poderá servir para uso em futuras auditorias, caso seja necessário;
12) CRIAR um "Termo de Responsabilidade" para uso dos recursos corporativos que pertencem à empresa e que serão utilizados pelos colaboradores, devendo ser assinado pelos titulares de cada credencial de acesso disponibilizada para trabalho remoto;

13) REVISAR, periodicamente, as credenciais de acesso remoto fornecidas e excluir (ou suspender temporariamente) aquelas que não mais precisem do seu uso (ex.: desligados, licenciados por longos períodos, etc);
14) CRIAR política ou norma específica para uso do trabalho remoto, em conformidade com políticas, códigos de ética e normas já existentes, formalizando todas as diretrizes que a empresa deve definir no uso do acesso remoto;
15) ENVOLVER a área jurídica e a área de recursos humanos da empresa, alinhando as diretrizes e critérios definidos para acesso remoto.

B. Se os recursos e ferramentas para trabalho remoto forem próprios do colaborador, é importante:

1) SEGUIR as diretrizes de segurança (políticas, normas e procedimentos) já existentes na empresa que trabalha;
2) CRIAR senhas fortes no uso da ferramenta para acesso remoto (por exemplo, senhas com tamanho mínimo de 8 dígitos e que misturem letras, números, símbolos, maiúsculas e minúsculas);
3) MANTER sistemas operacionais (do computador, notebook, tablet, celular, etc) atualizados e, pelo menos, uma ferramenta de anti-vírus instalada e manter atualizada;
4) PROTEGER sua rede sem fio doméstica, alterando as configurações padrão (de fábrica), alterando a senha para evitar possíveis acessos indevidos (o formato da senha pode seguir a mesma recomendação do item 2);
5) EVITAR utilizar redes sem fio públicas, abertas, sem senhas (a exemplo de redes disponíveis em locais públicos ou até mesmo disponível nas ruas). Adote esse procedimento pelo menos enquanto estiver trabalhando remotamente;
6) EVITAR armazenar dados pessoais (e dados pessoais sensíveis) próprios ou de qualquer outra pessoa, em seu equipamento pessoal (os conceitos constam na LGPD[8], definindo dado pessoal como "informação relacionada a pessoa natural identificada ou identificável", a exemplo de RG, CPF, Endereço, Email, Telefone Celular etc e dado pessoal sensível que é o "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").
7) DESCONFIAR de mensagens vindas de origem desconhecida (através de email ou qualquer rede social), principalmente neste período de pandemia. *Fake News*

[8] Lei Geral de Proteção de Dados Pessoais. Lei 13.709 de 14/8/2018.
Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

sobre COVID-19, Novo Corona-Vírus e temas similares estão sendo muito disseminadas na Internet. Busque informações de fontes confiáveis.

Algumas destas recomendações foram extraídas de conteúdos como o Fórum Econômico Mundial[9], que podem minimizar riscos de segurança comuns, em especial, neste momento de fragilidade em que todos nós estamos vivendo. Infelizmente, o crime organizado não alivia...não faltam evidências de casos de aplicativos falsos para dispositivos móveis, disseminação de *Fake News* com *links* e anexos para aplicação de golpes, ataques às infraestruturas críticas que fornecem serviços essenciais, em busca de dados pessoais sensíveis e tantos outros exemplos que a mídia tem exposto ao longo das últimas semanas, desde que a pandemia foi anunciada.

A distribuição periódica de orientações para os colaboradores é de grande importância neste momento. Segundo Vieira[10] "Um Programa de Treinamento de Pessoas, numa Organização, deve criar condições para sensibilizar todos aqueles que, de alguma forma, lidam com dados pessoais. É importante pensar na redução de riscos e incidentes de segurança, e uma das formas de alcançar isso é através da disseminação de práticas positivas de segurança, de forma periódica, para a adoção de comportamento proativo e preventivo, diante das ameaças. Quanto mais os usuários praticarem a segurança, mais a Organização poderá estar protegida contra ameaças diversas".

O site do Internet Segura[11], dá dicas de segurança bem interessantes, utilizando linguagem clara e objetiva. Uma delas é "Boatos ajudam a espalhar desinformação pela Internet e podem conter códigos maliciosos e tentativas de golpes. Ao receber notícias sobre o tema Coronavírus seja cuidadoso ao compartilhar, verifique a fonte da informação e em caso de dúvidas, não compartilhe e ajude a tornar a Internet um ambiente mais saudável, seguro e confiável".

Os colaboradores de qualquer empresa, de qualquer ramo de negócio, precisam ter um mínimo de informação sobre o tema, para que possam praticar a segurança em seu dia-a-dia, seja no mundo físico ou digital, o que irá, certamente, minimizar riscos e evitar incidentes. As empresas precisam promover ações neste sentido.

[9] Organização sem fins lucrativos, fundada em 1971, atua com pesquisas e temas importantes para a humanidade. "*How to protect yourself from cyberattacks when working from home during COVID-19*".
Disponível em: https://www.weforum.org/agenda/2020/03/covid-19-cyberattacks-working-from-home/

[10] Elba Vieira. Capítulo 6 – A proteção de dados desde a concepção (by design) e por padrão (by default). In: LGPD – Lei Geral de Proteção de Dados Pessoais. Manual de Implementação. Coord. Viviane Maldonado. São Paulo: Thomson Reuters Brasil, 2019.

[11] Portal idealizado pelo CGI.br (Comitê Gestor da Internet no Brasil) que reúne iniciativas de conscientização sobre segurança e uso responsável da Internet.
Disponível em: https://internetsegura.br/coronavirus/

5. DESAFIOS

A todo instante, surgem novas informações sobre o tema relativo ao acesso remoto ou home-office ou teletrabalho. Como bem citado por Pinto[12], a respeito dos pontos contidos na MP 927/2020[13], sobre o tema que estamos abordando aqui, "A presente medida provisória descortinou o que não era novidade: o teletrabalho é uma das ferramentas mais potentes na tentativa de preservação de empregos. Aqui também estou falando para os tempos de 'normalidade cidadã'".

Passado esse difícil momento, quiçá o trabalho remoto torne-se o "novo normal" nas empresas, que já experimentam e observam vantagens e desvantagens deste modal, mesmo com a diversidade de profissões, tipos de trabalho, áreas de atuação e as responsabilidades das empresas enquanto controladoras de dados pessoais (e sensíveis) sob sua responsabilidade.

Pinto, ainda sobre a MP 927/2020, afirma que "não me parece esforço desproporcional aproveitar o momento e regulamentar o teletrabalho em acordo individual escrito, até porque é considerável a probabilidade de o teletrabalho virar realidade perene na vida das empresas, após esta inconveniente pandemia". Mais adiante, ele diz que "o Teletrabalho desponta como lenitivo importante em tempos de tantas patologias".

Inúmeros são os desafios para quem trabalha no formato à distância ou para quem está começando agora (imagino que milhões de pessoas), em função do isolamento social imposto e necessário.

Manter-se atualizado é imprescindível, acompanhar as notícias de tecnologia e segurança, através de sites e ambientes conhecidos ou recomendados, é outra medida que deve fazer parte do cotidiano de quem precisa trabalhar no meio digital. As ameaças evoluem a todo momento, os criminosos estão utilizando ferramentas cada vez mais poderosas e sofisticadas para atacar, invadir, acessar indevidamente e obter dados e informações que se transformem em lucro e poder.

Como citado na música de Caetano Veloso[14], "é preciso estar atento e forte". Que estejamos sempre atentos, tanto como profissionais de segurança e tecnologia, como cidadãos de um mundo em constante transformação.

---

[12] Luis Otávio Camargo Pinto. Presidente da SOBRATT – Sociedade Brasileira de Teletrabalho e Teleatividades. "O Teletrabalho e a Medida Provisória No. 927/2020". Disponível em: http://www.sobratt.org.br/index.php/30032020-o-teletrabalho-e-a-medida-provisoria-no-9272020/

[13] "Dispõe sobre as medidas trabalhistas para enfrentamento do estado de calamidade pública reconhecido pelo Decreto Legislativo nº 6, de 20 de março de 2020, e da emergência de saúde pública de importância internacional decorrente do coronavírus (**covid-19**), e dá outras providências". Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Mpv/mpv927.htm

[14] Cantor e compositor brasileiro. Música: Divino Maravilhoso. Disponível em: https://www.letras.mus.br/caetano-veloso/44718/

6. CONSIDERAÇÕES FINAIS

Ainda citando Luiz Otávio Camargo Pinto, proponho uma reflexão a ser digerida bem lentamente: “o isolamento social não dá qualquer alternativa para a sociedade. Ou nos adaptamos rapidamente, naquilo que for possível, ou estaremos fadados ao completo imobilismo diante dos efeitos desastrosos no campo da economia decorrentes desse indigesto estado de calamidade pública”.

Que saibamos viver e conviver, nestes tempos difíceis, com as alternativas, possibilidades, tecnologias que estão aí para serem utilizadas em benefício da humanidade, fazendo o trabalho girar, minimizando os efeitos da crise e evitando a paralisia das empresas públicas e privadas.

Que tenhamos, igualmente, a capacidade de perceber novas oportunidades para viver em um mundo em constante e rápidas mudança; a capacidade de inovar, mesmo com dificuldades e limitações; e capacidade de criar novas formas de convivência e comunicação, seja para trabalhar, como para aprender, nos comunicarmos e nos divertimos.

Que esta crise sirva de laço, unindo povos e sociedades em cooperação global, visando um bem maior para a humanidade, preparando os indivíduos de hoje para um novo mundo amanhã!

Fica aqui uma reflexão final do magnífico Harari[15]: “Será o *Homo Sapiens* capaz de dar sentido ao mundo que ele criou?”

[15] Yuval Noah Harari. Israelense, Ph.D. em história pela Universidade de Oxford e professor universitário. Livro “21 licões para o século 21” (p. 16). Companhia das Letras. 2018.