DIGITAL 5.0

O DESAFIO DA CONFIANÇA E DA SEGURANÇA NA **ECONOMIA DIGITAL**

patrocínio

ABDI Agência Brasileira de Desenvolvimento Industrial

cgee Centro de Gestão e Estudos Estratégicos *Ciência, Tecnologia e Inovação*

SEBRAE

stefanini GROUP

TecBan

TOTVS

realização

FDC

DIGITAL 5

O DESAFIO DA CONFIANÇA E DA SEGURANÇA NA **ECONOMIA DIGITAL**

patrocínio

ABDI Agência Brasileira de Desenvolvimento Industrial

cgee Centro de Gestão e Estudos Estratégicos *Ciência, Tecnologia e Inovação*

SEBRAE

stefanini GROUP

TecBan

TOTVS

realização

FDC

FICHA CATALOGRÁFICA
Elaborada pela Biblioteca Walther Moreira Salles
Fundação Dom Cabral

D574

Digital : o desafio da confiança e da segurança na economia digital/Núcleo de Inovação e Empreendedorismo. - Nova Lima: Fundação Dom Cabral, 2021.
(Economia digital ; 5)
E-book : il. color.

E-book no formato PDF.
ISBN: 978-65-994597-5-7

1. Confiança. 2. Privacidade. 3. Ética. I. Título. II. Série.

CDD: 170

Bibliotecária: Daiane Campos Procópio – CRB 6/3215

doi.org/10.52959/978-65-994597-5-7

CRÉDITOS

EDITORES-EXECUTIVOS
Carlos Arruda
Heloísa Menezes
FUNDAÇÃO DOM CABRAL

APOIO EDITORIAL
Camila Cavalini Pedroso
Daniel Galdino Netto
FUNDAÇÃO DOM CABRAL

PROJETO GRÁFICO E REVISÃO
CeD | Criação&Design FDC
Anderson Luizes | *Designer Gráfico*
Daniela Ank e Euler Rios | *Coordenadores*
Rubens Cupertino | *Revisor*
FUNDAÇÃO DOM CABRAL

A **Fundação Dom Cabral** é um centro de desenvolvimento de executivos, empresários e empresas. Há 40 anos pratica o diálogo e a escuta comprometida com as empresas, construindo com elas soluções educacionais integradas, resultado da conexão entre teoria e prática. A vocação para a parceria orientou sua articulação internacional, firmando acordos com grandes escolas de negócios. A FDC está classificada entre as dez melhores escolas de negócios do mundo, no ranking do jornal Financial Times, e é a primeira na América Latina.

FALE COM A DIGITAL
economiadigital@fdc.org.br
0800 941 9200

EBOOK INTERATIVO

CONHEÇA OS ÍCONES DE NAVEGAÇÃO PRESENTES NESSE EBOOK E SUAS FUNCIONALIDADES

- ABSTRACT
- TEXTO ORIGINAL
- AVANÇAR ARTIGO
- RETROCEDER ARTIGO
- RETORNO AO SUMÁRIO
- VÍDEO
- WEBSITE

SUMÁRIO

CLIQUE SOBRE OS NÚMEROS E TÍTULOS PARA ACESSAR OS ARTIGOS

163

COMO O ATIVISMO DIGITAL PODE SER USADO PARA ENFRENTAR DESIGUALDADES SOCIOECONÔMICAS E DIVISÕES DIGITAIS?

Clovis Freire

O ativismo social e a sua forma digital, fruto da revolução tecnológica das TICs, é crítico para romper o ciclo vicioso das desigualdades que se alimentam mutuamente: "As divisões digitais expuseram o fato de que as desigualdades digitais e socioeconômicas se tornaram interligadas", segundo o brasileiro que atua na Organização das Nações Unidas.

Palavras-chave: ativismo social, ativismo digital, gaps digitais, desigualdades.

CARTA DO EDITOR

Confiança digital é um dos impulsionadores da economia no mundo fígital, em que as bases da confiança não estão alicerçadas nos contatos pessoais, mas em mecanismos capazes de garantir aos usuários e empresas operações seguras e respeito aos direitos humanos e sociais, como privacidade, ética e trabalho digno. Na medida em que o uso de dados se torna importante para tudo, ele e seu uso adquirem uma função social.

O livro V da Série Economia Digital Passada a Limpo discute os desafios que envolvem a confiança das pessoas e dos negócios na economia digital, capazes de assegurar a sua sustentabilidade e crescimento com segurança não só para os negócios digitais, mas também para o futuro da humanidade. Segurança e resiliência cibernéticas, ética no uso de tecnologias, desinformação no ambiente de abundância de informação, governança da internet que assegure liberdade com respeito aos direitos humanos, trabalhos dignos são alguns dos temas retratados no livro, fundamentais para colocar o ser humano na centralidade do debate e das atividades da economia digital.

imagem: Freepik.com

doi.org/10.52959/2021535427

INTRODUÇÃO

POR QUE É TÃO FUNDAMENTAL TER CONFIANÇA NA ECONOMIA DIGITAL?

Heloísa Menezes e Carlos Arruda

""Num mundo inundado de informações relevantes, clareza é poder". Na primeira frase da Introdução do seu *best seller* "21 Lições para o Século XXI", Yuval Harari se propõe a ajudar a humanidade a ter clareza a respeito dos grandes debates globais atuais e sobre o futuro da espécie humana. Entre esses debates estão o futuro da democracia e o poder das tecnologias, já que a fusão da revolução da tecnologia da informação com a biotecnologia "nos coloca os maiores desafios com que nossa espécie já deparou. A fusão das duas áreas pode em breve expulsar bilhões de seres humanos do mercado de trabalho e solapar a liberdade e a igualdade. Algoritmos de *big data* poderiam criar ditaduras digitais nas quais todo o poder se concentra nas mãos de uma minúscula elite, enquanto a maior parte das pessoas sofre não em virtude da exploração, mas de algo pior: irrelevância" (Harari, 2018 pp 15).

No mesmo tom do alerta do historiador israelense, que destaca as ameaças e perigos que as novas tecnologias trazem, buscamos, no quinto livro da coletânea sobre economia digital, analisar mais detidamente os riscos envolvidos com o rápido e amplo avanço das tecnologias digitais e do seu uso nos negócios e no nosso dia a dia. Riscos estes que têm ameaçado a segurança nas operações das empresas, a sua imagem e a própria democracia, arranhando a confiança nas tecnologias, nas empresas e na economia digital. Exemplo do drama é demonstrado pelos resultados da pesquisa do Pew Research Center de 2019, que identificou que 70% dos americanos acreditam que seus dados pessoais estão menos protegidos atualmente do que há cinco anos, e que 81% deles disseram que os riscos provenientes da coleta de dados por empresas superam os potenciais benefícios[1]. Enxergar riscos superiores aos benefícios das milhares de aplicações digitais na vida dos cidadãos pode constituir limitação digna de análise. Registro aqui um exemplo pessoal. Há três anos, eu, Heloisa Menezes, estando em Berlim com jovens alemãs amigas do meu filho, estranhei o fato de elas usarem aquele velho telefone celular cuja única função é telefonar. As jovens alemãs não queriam usar smartphone para preservar a sua privacidade. Atitude refletida na orientação da regulação da

privacidade da União Europeia, que privilegia o respeito às pessoas e não à facilitação da inovação, como a regulação norte-americana. Tal comportamento demonstrou uma radical visão cultural, talvez herança das guerras, que visa proteger os cidadãos. Imaginem a potencialização do holocausto em tempos em que seja possível imediata identificação dos cidadãos!

Nossos autores seguramente não propõem, no livro, que se deixe de usar as tecnologias e os modelos de negócios digitais, pois seria não usufruir dos inúmeros benefícios da tecnologia para a humanidade e tentar lutar contra o inevitável. Porém, eles defendem o uso seguro, consciente, transparente, ético e regulado das tecnologias, contribuindo para a constante inovação e resolução de problemas, tendo o ser humano no centro de tudo. Mas de que tipo de riscos à confiança na economia digital estamos falando? E o que isto tem a ver com a vida das empresas, em tempos de predominância de debates sobre ESG (acrônimo para Environment, Social e Governance)? Assim como se discute a necessidade de ESG estar no centro da estratégia das empresas como temas prioritários da agenda de governança dos Conselhos de Administração, dos executivos C-Levels e de todo e qualquer colaborador que acesse os sistemas da empresa, cibersegurança, ciber-resiliência e transformação digital responsável também o devem. Rogério Pires, diretor de Healthcare da TOTVS, demonstra como as tecnologias, em especial a inteligência artificial, são aliadas da saúde, dos médicos e da gestão das empresas de saúde, mas afirma que a palavra da tecnologia nunca pode ser a final, e sim a do profissional de saúde. O *compliance* e a privacidade de dados vêm cada vez mais fortes para ditar como a tecnologia será usada, empoderando cada vez mais o paciente.

Da mesma forma que as empresas precisam agir para a preservação do planeta, na era em que os dados são o "novo petróleo", representando o ativo mais relevante da economia digital, junto com as pessoas, as empresas precisam atuar diretamente para garantir a "sustentabilidade" dos dados, tratando-os com senso de preservação e de confiança. Segundo o autor Leidivino Natal, CEO da Stefanini Rafael, a segurança da informação nas empresas começa pela garantia de confiabilidade e confidencialidade dos dados, seja no ambiente físico, seja no digital. O autor alerta para a expectativa de que os gastos com cibersegurança cheguem a U$S 3 trilhões em 2021 e que, somente no 1º semestre deste ano, o número de ataques cibernéticos a empresas brasileiras cresceu 220%, em comparação ao mesmo período em 2020.

As pequenas empresas não escapam de tal desafio. Larissa Querino e Ricardo Araújo, da Agência Brasileira de Desenvolvimento Industrial – ABDI, destacam a importância da ciber-resiliência para este segmento empresarial, que muitas vezes estão inseridas na cadeia de valor de grandes empresas. Além de se defender dos ataques, é fundamental construir estratégias de resiliência e preparação das empresas aos ataques que virão. Para lidar com as ameaças contra o ativo dados, os autores da Stefanini Rafael e da ABDI oferecem uma série de recomendações às empresas e às políticas públicas, que se somam às obrigações conforme reguladas pela LGPD – Lei Geral de Proteção de Dados.

A diretora da Autoridade Nacional de Proteção de Dados – ANPD, Miriam Wimmer, em conjunto com o especialista

Lucas Borges, destacam, à luz de pesquisas junto à sociedade civil, que "o uso irrestrito e sem regras desse que é o grande ativo que mobiliza a economia do século XXI pode gerar efeitos negativos sistêmicos sobre todo o ecossistema digital, que podem ser comparados aos que decorrem da exploração desenfreada de recursos naturais ocorrida nas últimas décadas. Vale dizer, tanto num caso como no outro, há o risco de ocorrer o que os economistas chamam de 'tragédia dos comuns', situação na qual todos perdem e sofrem com os problemas gerados em razão do predomínio de decisões fundadas em considerações de curto prazo, que atingem e minam a sustentabilidade dos recursos coletivos no longo prazo, entre os quais a própria confiança." Ao citar pesquisas que demonstram que somente 15% das micro e pequenas empresas brasileiras (que representam 99% dos negócios brasileiros[2]) confirmaram estar prontas para atender às novas determinações legais e que dois terços sequer implementaram medidas básicas, como a criação de políticas de proteção de dados, os autores identificam claramente uma questão de risco à implementação da LGPD e ao uso seguro de dados pelas empresas brasileiras.

A regulação deve proteger os cidadãos e usuários e orientar o setor empresarial sem inibir a inovação. A previsão do uso de *sandboxes* regulatórios[3] no Marco Legal das Startups, pelo Banco Central e ANPD, é exemplo claro das possibilidades de inovar em ambiente regulado. O papel do Banco Central de garantir a segurança e solidez do sistema financeiro nacional e promover e induzir a inovação é demonstrado na entrevista com o diretor de regulação do órgão, Otávio Damaso, para quem o forte e histórico investimento em tecnologia realizado pelo sistema financeiro, aliado a uma postura aberta do órgão regulador, garantiu inovar com segurança, oferecendo cada vez mais aos clientes eficiência, conveniência, menores custos e segurança na operação. "Instituições financeiras vivem de credibilidade. Bancos tradicionais e *fintech*s têm o mesmo zelo com relação à segurança cibernética. Todos sabem que credibilidade é tudo no negócio deles". Ao lembrar do smartphone como uma das tecnologias mais disruptivas aplicadas ao setor financeiro, Damaso afirma que "olhando para frente, há tanta novidade que pode ser difícil saber quais serão as tecnologias mais disruptivas". Mas cita a moeda digital, CDBC, PIX, *open banking*, o volumoso investimento em IA, o uso de DLT (Distributed Ledger Technology[4]) e *blockchain* (uma forma de DLT que garante registros de todas as operações em uma rede) nas operações inter e intra instituições financeiras, *machine learning*, 5G e IoT. Segundo o diretor, o poder transformador do *open banking* guarda semelhança com a internet. No seu início, não se fazia ideia de como mudaria a vida da sociedade mundial. Apesar de ainda não podermos prever tudo o que as instituições financeiras criarão com o *open banking*, carrega um enorme potencial de gerar novos produtos e serviços, já que ele é uma plataforma, diferentemente do PIX.

Entre as modernas técnicas de gestão estratégica e de gestão da inovação, é estimulado o uso de ficção científica como ferramenta de antecipação do futuro. Em um cenário de ficção científica retratado nos alarmantes episódios da série do Netflix, *Black Mirror,* poderíamos pensar em futuros com riscos evitáveis?

Assim como há um grupo de riscos mais afeito a todo tipo de negócios, como os ciberataques, outro grupo adquire uma perspectiva mais ampliada, ao

envolver não somente as empresas, sejam elas as empresas em geral ou as grandes plataformas digitais (que ao mesmo tempo em que são impactadas, são atores relevantes na geração dos riscos), mas também os cidadãos, as relações de trabalho, a relevância das pessoas, a liberdade e a democracia. Estamos falando da privacidade de dados pessoais, mas também de ética algorítmica, da desinformação como estratégia, de gaps digitais causados por falta de capacidade formativa, de renda, de acesso à infraestrutura digital, mas também de trabalho digno no mundo digital. As grandes plataformas digitais são o principal alvo dos questionamentos. O livro traz uma série de artigos que descrevem e avaliam tais riscos à confiança na economia digital e, por que não dizer, ao futuro da humanidade, como alerta Yuval Harari.

A fluidez e a rapidez das informações, aliadas à pouca profundidade das análises, colaboram para as "bolhas" de opinião que se formam a partir das estratégias tecnológicas da desinformação. Até onde vai a liberdade da rede, base da criação da internet e a liberdade de expressão? Quais são as responsabilizações dos cidadãos, empresas, plataformas de redes sociais e seus representantes pela produção e circulação de informações falsas e desinformação deliberada? E a regulação? Qual a sua dimensão e forma? A autorregulação é suficiente?

O professor Demi Getschko, um dos precursores da internet no mundo e no Brasil, atualmente Diretor Presidente do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), continua a defender o princípio original da rede mundial: a sua liberdade, uma rede aberta e sem um centro de controle ou administração. "A vantagem de existir a internet e de poder usá-la livremente superam de longe os riscos que ela carrega. Entretanto, parece vital, não só para a sobrevivência da rede, mas também, e especialmente, para a preservação da civilidade nas relações humanas coletivas, e da morigeração no trato pessoal, que sempre observemos o princípio de Postel citado acima: 'sejamos conservadores no que enviamos, e tolerantes no que recebemos'". A forma de usufruir os grandes benefícios que a internet traz varia entre os usuários. Há os novos entrantes – que podem ser potenciais e ingênuas vítimas das armadilhas e golpes que campeiam na internet, os comedidos – que se arriscam menos e "preservam não apenas sua privacidade, mas seu poder de julgamento". Há os que, maravilhados pelas possibilidades e exuberância da rede, juntam-se às hordas que seguem 'formadores de opinião' do momento e, eventualmente, participam na formação de 'bolhas' de opinião, estimulando acaloradas e na maioria das vezes inconsistentes discussões, onde os argumentos *ad hominem* são os que predominam.

As medidas de moderação da circulação da informação nas plataformas têm tido certo efeito onde são adotadas, mas ainda limitado em vista da dimensão que o fenômeno toma global e localmente, com profundos impactos no futuro da humanidade. Assim, Sascha D Meinrath, Steven Mansou e Humza Jilani, especialistas em políticas públicas digitais, descrevem os riscos e sugerem cinco níveis crescentes de ações regulatórias para conter a informação falsa nas plataformas digitais e reforçar a democracia, baseadas em divulgação e transparência, auditorias algorítmicas, multas por não cumprimento intencional , diminuição da proteção de responsabilização e processo criminal.

Alguns de tais riscos são combatidos por iniciativas de regulação pelas autoridades e de autorregulação pelas empresas, mas também atualmente assistimos à criação, pela sociedade civil, de iniciativas de controle social de práticas antiéticas ou ameaçadoras da inclusão, do bem-estar social e da democracia. É o ativismo social e digital descrito pelo pesquisador Clóvis Freire da UNCTAD, órgão da ONU, "necessário para que as pessoas percebam que existe o descompasso entre sistemas tecno-econômicos e sistemas societário-institucionais, para quebrar a inércia e promover as mudanças sociais necessárias, além de ajudar na conscientização sobre temas já existentes", como o do gap digital, ou que ainda não estão "no radar" da sociedade e das empresas, como as questões éticas relacionadas ao uso de mídias sociais, por exemplo.

Exemplo de ativismo digital relevante é uma iniciativa do respeitado Berkman Klein Centre for Internet & Society (BKCIS), pertencente à Universidade de Harvard, que criou o Institute for Rebooting Social Media[5]. O BKCIS propõe para os próximos três anos uma reforma completa das plataformas de redes sociais, que se desviaram do propósito para o qual foram criadas. De motores da democracia e da disseminação da verdade, agora são vistas como facilitadoras da disseminação de mentiras, de divisão entre as pessoas, causadoras de danos físicos e psicológicos. Segundo Jonathan Zittrain, cofundador da BKCIS, "embora a identificação dos problemas possa variar, é difícil encontrar alguém defendendo o ambiente atual das redes sociais"[6].

Encontra-se em debate, atualmente, uma visão complementar ao requerimento de controle social. Se por um lado assistimos ao surgimento do ativismo social e digital para minimizar os riscos do digital, há outros pesquisadores, como Miguel Lago, que analisam a possível redução na participação social nas políticas públicas com o aumento do uso de IA, *big data* e automatização dos diagnósticos dos problemas das cidades, substituindo a função social do cidadão de reclamar dos governantes quando há, por exemplo, buracos nas ruas. Haveria o risco de parecer que as mídias sociais representam a voz do povo, reduzindo a política pela polarização. A desinformação destitui a legitimidade das autoridades ou a referência a elas, podendo levar à perda de confiança nas instituições, uma ameaça ao futuro democrático.

O jornalista Nilson Santos agrega um nível ao debate, ao tratar do aprisionamento causado pela Mentira, que cria um vínculo de confiança com o emissor da mensagem que deliberadamente utiliza argumentos falaciosos e ficcionais para o exercício do poder. Citando pesquisa de professores do MIT (Massachusetts Institute of Technology), que constatou que informações falsas têm 70% mais probabilidade de serem retuitadas e levam seis vezes menos tempo para alcançar o mesmo número de pessoas do que histórias verdadeiras, conclui-se que estamos cada vez mais desinformados na sociedade da informação. Porém, o avanço tecnológico permite que se identifique como a Mentira se traveste de Verdade. O autor, por fim, defende que o "impacto corrosivo das ondas sequentes de informações falsas nos alicerces das sociedades democráticas coloca na ordem do dia que se estabeleçam políticas públicas que acelerem a curva de aprendizado da sociedade para lidar com desinformações forjadas e/ou postas em circulação por negligência ou má-fé".

A pesquisadora da Université Paris II, Nina Santos, complementa esse argumento analisando como a desinformação estrategicamente orientada pode se esconder nos caminhos tecnológicos, passando despercebida e naturalizada como parte constituinte do mundo digital. Seu artigo demonstra como a tecnologia está por trás das cortinas e os três processos pouco visíveis ou invisíveis que levam à desinformação, quais sejam as lógicas opacas das plataformas, a volatilidade dos conteúdos e a monetização nas plataformas digitais.

Agregando ao debate os desafios éticos do avanço das tecnologias digitais, alguns autores, como a pesquisadora e professora da UNICAMP Sandra Ávila, especialista em *machine learning,* defende que é hora de deixarmos de usar as tecnologias que trazem riscos para a sociedade, como as que automatizam o racismo. É o caso do reconhecimento facial, banido em vários países do mundo, pois ainda não se reconhece adequadamente a pele negra, acirrando o racismo que já existe e que não pode ser alimentado por dados que são influenciados também por vieses históricos.

Enquanto no tema gestão empresarial está sendo muito difundido o conceito do "desaprender", há quem defenda o "desaprendizado de máquinas" como forma de proteger a privacidade de dados pessoais. Mas a professora Sandra Ávila afirma que estamos em um momento em que precisamos menos de técnica e mais de ética. "Não estamos discutindo sobre ética, enquanto somos responsáveis pelos modelos que estamos gerando". Com ética para organizar melhores usos e processos de uso de IA funciona a confiança na tecnologia. Deve ser evitado o uso desordenado de IA para tarefas subjetivas, onde não se consegue gerar uma função ou um modelo automático. "Os modelos deveriam ter bulas, dizendo que serve para isso, mas não serve para aquilo". E a análise de sua aplicação deve se dar através de muitos testes, realizados por uma equipe diversa, para evitar os vieses algorítmicos. Afirma que as pessoas precisam saber da importância dos dados e como eles estão sendo usados para tomar diversas tomadas de decisão na sua vida, acarretando riscos. Assim, a professora traz outra perspectiva para a discussão: dados como direitos humanos.

Prosseguindo nas análises, o secretário de estado e professor da UFRGS, Luis Lamb, trata do desafio econômico de mensurar o PIB gerado pelos intangíveis na economia digital. Afirma que o componente tecnológico dos negócios ocupa, na contemporaneidade, papel central nas relações entre os atores econômicos e que o impacto ético dos negócios digitais se torna, em realidade, inseparável e indistinguível de qualquer relação econômica, tendo em vista a ubiquidade das tecnologias digitais. E introduz outro tema relevante para a confiança nas relações econômicas baseadas no digital: as incertezas quanto à natureza do trabalho e relações entre empregadores e empregados, impactadas pela transformação digital dos negócios e pelas novas exigências quanto à formação, habilidades e competências do capital humano.

Clóvis Freire, da UNCTAD, e o professor Wilson Engelmann, da UNISINOS, chamam a atenção para tais consequências e incertezas. Segundo Clóvis Freire, as "divisões digitais expuseram o fato de que as desigualdades digitais e socioeconômicas se tornaram interligadas. Com o mundo digital e o mundo físico se tornando mais integrados, para fechar a

brecha digital temos que também enfrentar as desigualdades socioeconômicas. Não é possível enfrentar um sem atacar o outro". Na mesma linha, Janaína Costa e Celina Carvalho, do Instituto Tecnologia e Sociedade, o ITS, analisam outro aspecto da economia digital que poderia reduzir o gap de acesso a vários serviços ao cidadão e a pequenas empresas, a identidade digital. Relatório da Mckinsey Global Institute aponta que a economia do Brasil pode crescer 13% se ajustar seu déficit de identidade digital, mas as autoras apontam que as dificuldades de acesso à identidade digital "adentram uma arena em que velhos problemas permanecem: barreiras de acesso à documentação pessoal básica, práticas frágeis de proteção de privacidade e dados pessoais, sistemas de identificação mal arquitetados e que não se prestam a melhorar o acesso a serviços. As disfunções descritas impactam mais severamente as pequenas empresas e aqueles em situação de vulnerabilidade e podem contribuir para aprofundar o fosso de desigualdade socioeconômica e engessar a economia digital".

O professor Engelmann, ao avaliar como lidar com os impactos e riscos das novas tecnologias no mundo do trabalho e na chamada *gig econom,* apresenta as dificuldades do Direito de regular a economia de plataformas e garantir a proteção legal aos trabalhadores. A "Nova Economia" ou a "Economia Digital" poderá ser estruturada por mecanismos de "autorregulação regulada", mas deverá respeitar um equilíbrio entre todas as partes envolvidas. O autor defende a necessidade urgente de um debate político sobre a melhor forma de preparar os trabalhadores para essa nova realidade: novos tipos de seguridade social e reforma dos sistemas de saúde e previdência para acomodar os empregados sob demanda.

Em um interessante contraponto, trazendo a visão de uma empresa líder de mercado, Diego Barreto, vice-presidente do iFood, aponta o lado positivo da *gig economy,* que com suas características de flexibilidade e liberdade do trabalhador escolher quando, onde e como pretende trabalhar, tem garantido a sustentação da renda familiar de um enorme contingente de trabalhadores. Ainda no cenário pré-pandemia de COVID-19, a economia compartilhada reunia um exército de quase 4 milhões de autônomos. "Sendo um segmento em crescimento, traz claros benefícios econômicos de produtividade e a geração de renda". Diego Barreto defende que "a sociedade conectada e em rede demanda uma transformação de toda a lógica do trabalho. Saem os processos engessados e hierarquias rígidas, entram a agilidade e a colaboração, que permitem montar equipes com todos os tipos de potencialidade. Mesmo a terceirização, hoje regulamentada, é um expediente importante. Nessa outra dimensão, flexibilização é um valor não só positivo, mas fundamental". Apesar de o autor destacar os pontos positivos das plataformas digitais para o trabalho, em especial se comparado aos seus equivalentes analógicos, chama a atenção para a necessidade de equacionar várias questões, que devem ser consideradas no seu contexto institucional e nas especificidades locais. "Este é mais um ponto importante: o desafio de aprimorar o modelo, garantindo uma renda mínima por hora aos trabalhadores, além de mais segurança social e amparo, não é meramente gerencial. É sobretudo uma demanda por políticas públicas."

Em conclusão, neste quinto volume da série Economia Digital Passada a Limpo, convidamos autores com visões distintas, mas complementares, reconhecendo que a confiança e a ética digital são impulsionadores da economia no mundo *fígital,* em que as bases da confiança não se dão predominantemente pelos contatos pessoais, mas são ancoradas em mecanismos que devem garantir a cada um dos usuários, às empresas e agências governamentais, operações seguras e respeito aos direitos humanos, como privacidade, proteção contra as informações falsas e trabalho digno. Na medida em que o uso de dados se torna importante para tudo, ele e seu uso adquirem uma função social.

Acreditamos que a soma de conscientização e capacitação dos cidadãos e empresas, regulações e atuação segura e responsável por parte das empresas e da sociedade seja a receita para uma economia digital mais responsável, includente, ética e centrada no ser humano. Assim, tendo as pessoas no centro das preocupações das empresas, trabalhar para garantir a sua relevância na nova economia torna-se fundamental.

NOTAS

1 PEW RESEARCH CENTER. Americans and Privacy: concerned, confused and feeling lack of control over their personal information, 24 nov. 2019. Disponível em: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/. Acesso: 24 set. 2021.

2 https://www.sebrae.com.br/sites/PortalSebrae/ufs/sp/sebraeaz/pequenos-negocios-em-numeros,12e87943634475 10VgnVCM1000004c00210aRCRD. Acesso em 24 set. 2021

3 https://www.gov.br/startuppoint/pt-br/programas/sandbox-regulatorio. Acesso em 24 set. 2021

4 Para uma simples descrição sobre DLT e blockchain, acesse https://exame.com/future-of-money/blockchain-e-dlts/as-diferencas-entre-blockchain-e-dlts/ Acesso em 24 set. 2021

5 https://cyber.harvard.edu/programs/institute-rebooting-social-media. Acesso 24 set 2021.

6 Ver matéria É possível reiniciar as redes sociais para deixá-las menos tóxicas? - TecMundo. Acesso 24 set 2021

Heloisa Menezes

Professora convidada da Fundação Dom Cabral

Heloisa Menezes é professora convidada da Fundação Dom Cabral, empreendedora e consultora. Foi secretária de Desenvolvimento da Produção do Ministério do Desenvolvimento, Indústria e Comércio Exterior, diretora técnica do Sebrae Nacional, diretora da Confederação Nacional da Indústria, superintendente do IEL/FIEMG e membro de diversos conselhos. Heloisa é economista, mestre em Ciências em Desenvolvimento Agrícola pela UFRRJ.

Carlos Arruda

Professor da Fundação Dom Cabral

Carlos Arruda é professor na área de Inovação e Competitividade e Gerente Executivo do Núcleo de Inovação e Empreendedorismo da Fundação Dom Cabral – FDC. Foi diretor adjunto de parcerias, pesquisa e relações internacionais da FDC e presidente do conselho do UNICON. É membro dos conselhos da Biominas e do conselho assessor da Salesforce do Brasil. Mestre em administração pela UFMG e PhD em negócios internacionais pela Universidade of Bradford (Reino Unido).

PARTE I

AS CONDIÇÕES PARA O AUMENTO DA CONFIANÇA E DA SEGURANÇA

doi.org/10.52959/2021535427

COMO ASSEGURAR CONFIANÇA NA NOSSA ECONOMIA DIGITAL COMPARTILHADA?

Daniel Dobrygowski

Nossa economia global e interligada é cada vez mais indistinguível do que antes era chamada de economia digital. A imensa escala, escopo e complexidade da Quarta Revolução Industrial tocou todos os aspectos da economia e da sociedade[1]. Nas últimas décadas, todo setor econômico tem enfrentado pressões para digitalizar e enfrentar os desafios significativos que tal digitalização traz consigo – incluindo os riscos à segurança. Essas pressões só aumentaram à medida que a digitalização se tornou a solução para a continuidade dos negócios e para a conectividade social durante a pandemia do coronavírus.

Ao mesmo tempo, nossa economia digital está envolvida em outro conjunto de riscos, os da insegurança cibernética e da desconfiança digital. Falhas de segurança cibernética, *hacks* e violações de informações sensíveis representam atualmente o maior risco causado pelo homem, enfrentado por líderes empresariais e econômicos[2]. Em parte devido a essa insegurança, bem como à falta de uma governança adequada e de responsabilidade pelas novas tecnologias, a confiança pública na inovação tecnológica está em seu nível mais baixo[3].

A fim de garantir a sustentabilidade de nossa economia digital, devemos voltar deste precipício cooperando, entre setores e indústrias, em apoio à nossa segurança compartilhada e tomar medidas para garantir que nossas tecnologias sejam confiáveis. Esses aspectos são questões fundamentais para os líderes de toda a economia.

Portanto, os líderes devem aproveitar todas as oportunidades para construir tanto segurança quanto confiança em suas estratégias e cooperar para garantir uma base tecnológica segura e confiável para nosso crescimento compartilhado.

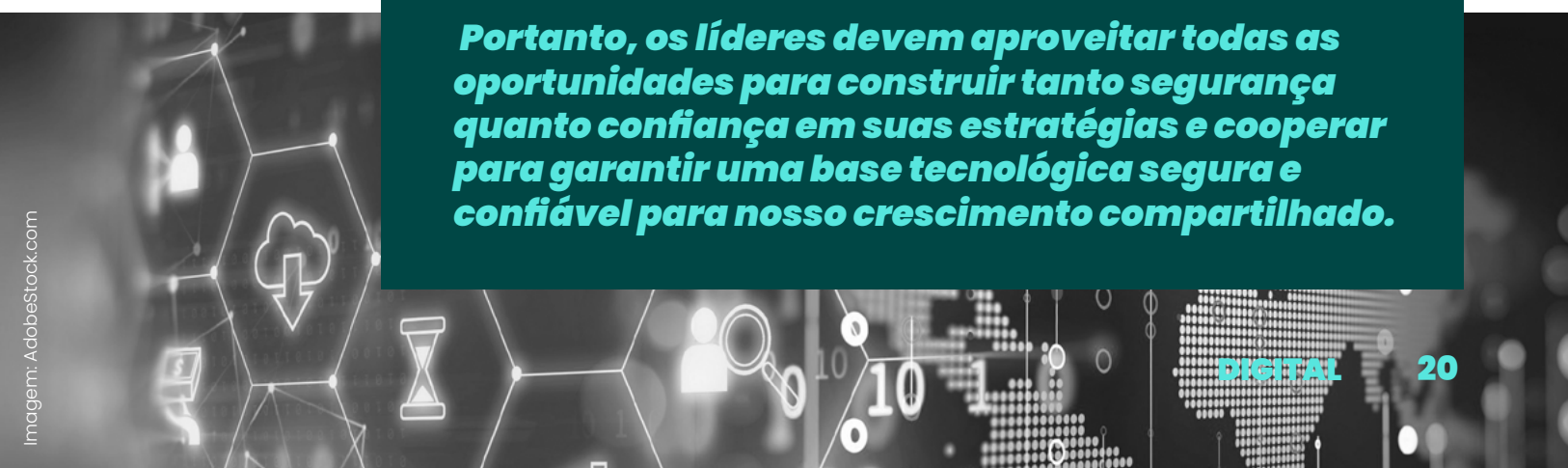
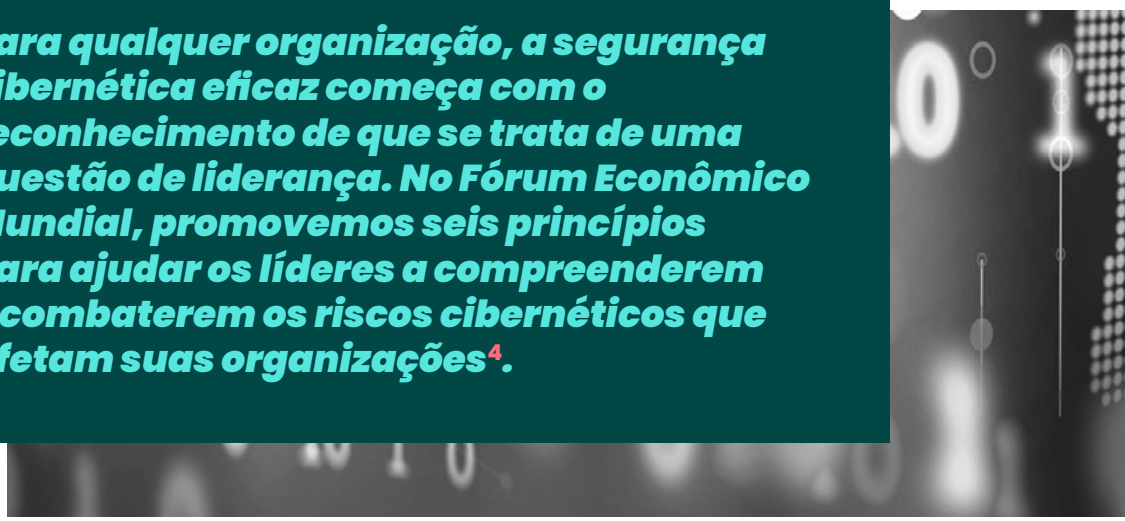


Imagem: AdobeStock.com

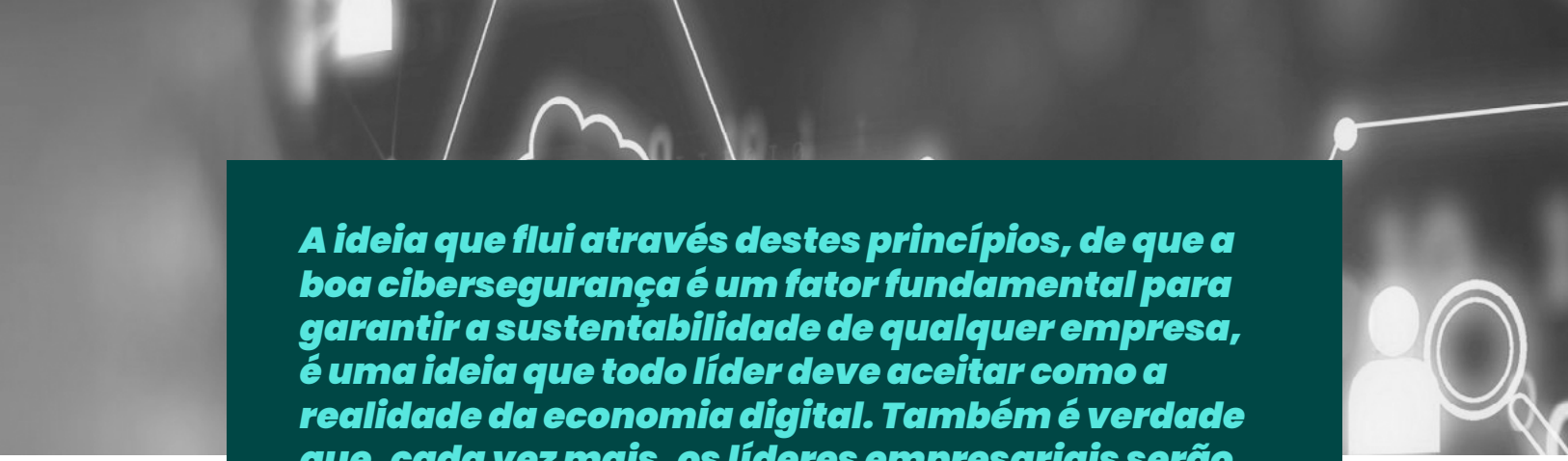
PROMOVENDO A SEGURANÇA CIBERNÉTICA

Para qualquer organização, a segurança cibernética eficaz começa com o reconhecimento de que se trata de uma questão de liderança. No Fórum Econômico Mundial, promovemos seis princípios para ajudar os líderes a compreenderem e combaterem os riscos cibernéticos que afetam suas organizações[4].



Esses princípios são:

- **Reconhecer que a cibersegurança é um capacitador estratégico de negócios**: a cibersegurança organizacional contribui diretamente tanto para a preservação do valor quanto para novas oportunidades de criação de valor para a empresa e para a sociedade em geral.
- **Entender o impacto econômico do risco cibernético**: para que as organizações tomem decisões empresariais eficazes, as determinações de risco devem se concentrar no impacto financeiro que terão, incluindo os *trade-offs* entre transformação digital e risco cibernético.
- **Alinhar o gerenciamento de risco cibernético com as necessidades comerciais**: a governança eficaz de qualquer empreendimento requer um alinhamento claro entre o gerenciamento de risco cibernético e os objetivos comerciais em todas as facetas da tomada de decisão.
- **Assegurar que o projeto organizacional apoie a segurança cibernética**: as organizações devem projetar uma estrutura de governança interna que aborde a segurança cibernética em toda a empresa.
- **Incorporar a experiência em segurança cibernética na governança da diretoria**: os líderes devem se valer de diversas fontes de experiência e conhecimento em segurança cibernética.
- **Fomentar a resiliência sistêmica**: os líderes devem reconhecer a natureza interligada do risco cibernético e encorajar respostas unificadas a ele.



A ideia que flui através destes princípios, de que a boa cibersegurança é um fator fundamental para garantir a sustentabilidade de qualquer empresa, é uma ideia que todo líder deve aceitar como a realidade da economia digital. Também é verdade que, cada vez mais, os líderes empresariais serão responsabilizados, por seus acionistas, pelos reguladores e por seus clientes por garantir uma boa cibersegurança.

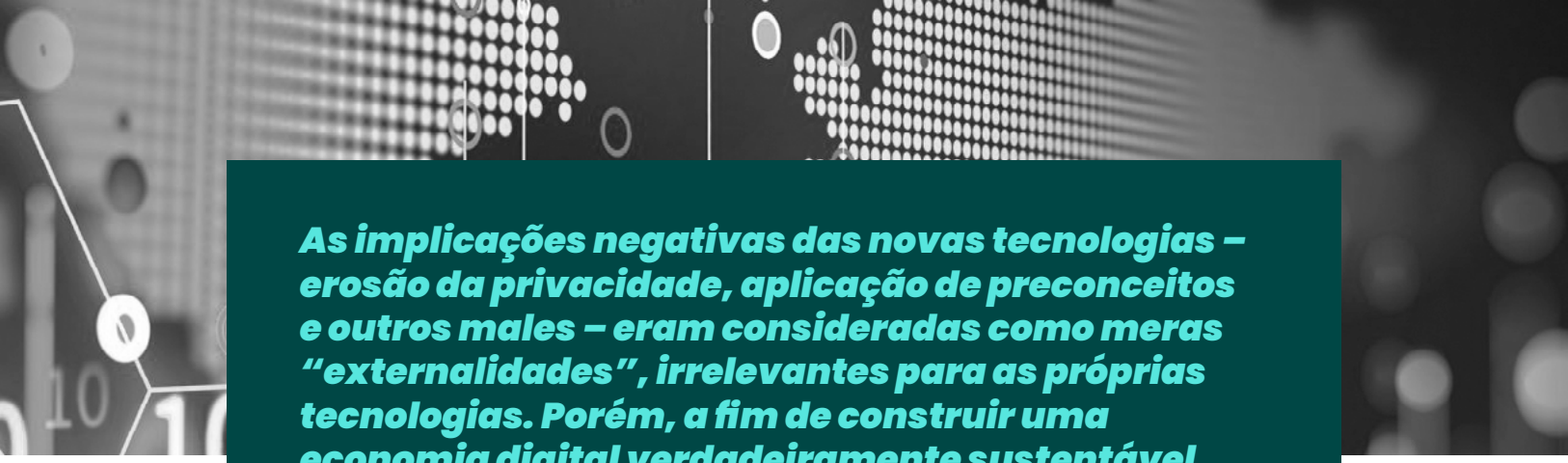
Na prática, a boa segurança cibernética exige que aqueles que estão na liderança e na linha de frente se concentrem continuamente em identificar e proteger seus ativos mais vitais e desenvolver práticas de continuidade comercial cibernéticas para garantir que a organização possa suportar os ataques cibernéticos mais prováveis[5].

GARANTINDO UMA TECNOLOGIA RESPONSÁVEL

Embora vital para garantir a confiança, a segurança cibernética só protege contra ataques maliciosos externos à tecnologia e aos sistemas.

Devemos também garantir que esses sistemas sejam confiáveis em sua implementação e uso planejados.

A fim de reforçar a confiança, que é vital para uma economia digital sustentável, devemos implementar tanto uma boa segurança quanto boas políticas e governança.[6] É aqui que entram as questões de responsabilidade, ética e responsabilidade. Para construir uma economia digital sustentável, devemos assegurar que seus fundamentos tecnológicos sirvam aos propósitos da sociedade como um todo.



As implicações negativas das novas tecnologias – erosão da privacidade, aplicação de preconceitos e outros males – eram consideradas como meras "externalidades", irrelevantes para as próprias tecnologias. Porém, a fim de construir uma economia digital verdadeiramente sustentável, estes aspectos negativos devem ser reconhecidos como resultantes de decisões humanas no desenvolvimento e aplicação de um conjunto diversificado de tecnologias.

Isto significa que novas regras e normas devem ser colocadas em prática para governar as tecnologias e orientar a inovação responsável. No mínimo, isto inclui avaliações de como essas tecnologias aderem às responsabilidades éticas geralmente reconhecidas. A tecnologia confiável também deve incluir proteções adequadas para valores compartilhados, por exemplo, privacidade, antes que essas tecnologias sejam implementadas e adotadas. Além disso, novos mecanismos de responsabilidade devem estar em vigor para garantir que os erros ou violações das expectativas compartilhadas tenham soluções eficazes.

Em última instância, isto exigirá que os líderes da economia digital adotem uma abordagem centrada no ser humano para a inovação tecnológica.

Mas temos mais a ganhar do que a perder em tal abordagem. As abordagens centradas no homem para o uso de dados já mostraram como todos os interessados podem prosperar sob tais decisões estratégicas e políticas[7].

COOPERANDO PARA UMA ECONOMIA DIGITAL DIGNA DE CONFIANÇA

Em toda a economia digital, seus benefícios e seus desafios estão altamente interligados. Portanto, as soluções para esses desafios e nossos esforços para moldar a economia digital em benefício de toda a sociedade humana devem começar com a cooperação. Do trabalho para combater o crime cibernético[8] ao aumento da confiabilidade dos dispositivos conectados à Internet[9], já começamos o processo compartilhado de reforço da confiança na economia digital. Cabe a cada líder e a cada tecnólogo continuarem esses esforços.

Se quisermos proteger a economia digital e expandir seus benefícios para incluir todas as partes interessadas, desde as empresas até o governo e os cidadãos, devemos oferecer tanto segurança quanto tecnologia confiável. Para isso, devemos optar por levar a segurança cibernética a sério e optar por manter a inovação tecnológica a serviço dos objetivos da humanidade. Devemos fazer a escolha pela confiança digital.

Daniel Dobrygowski

Daniel Dobrygowski é o Head de Governança e Confiança do Centro de Segurança Cibernética do Fórum Econômico Mundial (WEF). Advogado e educador, com duas décadas de experiência na interseção de tecnologia, direitos civis, legislação e política, ele supervisiona projetos e pesquisas relacionados à segurança cibernética, risco cibernético e governança corporativa e confiança digital. Como um dos fundadores do Centro de Segurança Cibernética do Fórum, ele lidera equipes responsáveis pelos esforços para compreender e moldar as normas, leis, regulamentos e padrões globais de segurança cibernética. Daniel também assessora o Fórum em questões jurídicas e políticas relacionadas à segurança cibernética e privacidade. Ele faz parte do conselho do Cyber Risk Institute e foi reconhecido pela National Association of Corporate Directors, em 2021, em seu NACD Directorship 100, como um dos líderes mais influentes na comunidade de governança corporativa.

Daniel possui um MPA da Kennedy School of Government da Harvard University, um JD da University of California, Berkeley, School of Law, onde foi editor do Berkeley Technology Law Journal, e um bacharelado da Johns Hopkins University. Antes de ir para o Fórum como Global Leadership Fellow, Daniel atuou como advogado em São Francisco e Washington, DC, aconselhando clientes em questões de antitruste / concorrência, proteção ao consumidor e privacidade. Daniel compartilha sua experiência em eventos e publicações como Harvard Business Review e Wired.

NOTAS E REFERÊNCIAS

1 Schwab, Klaus. 2016. The Fourth Industrial Revolution: what it means, how to respond. World Economic Forum Agenda. https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

2 World Economic Forum. 2021. The Global Risks Report, 16th edition. http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

3 Haerpfer, C., Inglehart, R., Moreno, A., Welzel, C., Kizilova, K., Diez-Medrano J., M. Lagos, P. Norris, E. Ponarin & B. Puranen et al. (eds.). 2020. World Values Survey: Round Seven - Country-Pooled Datafile. Madrid, Spain & Vienna, Austria: JD Systems Institute & WVSA Secretariat. doi.org/10.14281/18241.13 ; Edelman. 2021. Edelman Trust Barometer 2021. https://www.edelman.com/sites/g/files/aatuss191/files/2021-03/2021%20Edelman%20Trust%20Barometer.pdf

4 World Economic Forum. 2021. Principles for Board Governance of Cyber Risk. https://www.weforum.org/reports/136f100d-381a-4b09-a891-de2299144992

5 World Economic Forum. 2020. Cybersecurity Leadership Principles: Lessons learnt during the COVID-19 pandemic to prepare for the new normal. https://www.weforum.org/reports/cybersecurity-leadership-principles-lessons-learnt-during-the-covid-19-pandemic-to-prepare-for-the-new-normal

6 Dobrygowski, Daniel & William Hoffman. 2019. We need to build up 'digital trust' in tech. Wired. https://www.wired.com/story/we-need-to-build-up-digital-trust-in-tech/

7 Bettinger, Kimmy. 2021. 12 ways a human-centric approach to data can improve the world. World Economic Forum Agenda. https://www.weforum.org/agenda/2021/08/12-ways-a-human-centric-approach-to-data-can-improve-the-world/

8 World Economic Forum. 2020. Partnership against cybercrime. https://www.weforum.org/reports/partnership-against-cybercrime

9 World Economic Forum. 2021. Trustworthy IoT coalition. https://www.weforum.org/projects/trustworthy-iot-coalition

doi.org/10.52959/2021535403

INTERNET, A "ADMIRÁVEL REDE (NOVA)", PRECISA DE GOVERNANÇA?

Demi Getschko

Se é fato que a biologia dos humanos altera-se muito lentamente, o mesmo não pode se dizer quanto ao ambiente cultural que nos envolve. Sem que se discutam os méritos ou deméritos das mudanças, é patente que em 50 anos houve transformações maiores que, talvez, em séculos que nos precedem. Especialmente nesta época de pandemia, em que o acesso à rede para quase todas nossas transações quotidianas foi *sine qua non*, ambientes mudaram muito rapidamente. O quanto dessas transformações tem a ver, historicamente, com o aparecimento e a expansão da internet, é algo que deve ser examinado com mais detecção.

Atente-se inicialmente à gênese da rede, um projeto desenvolvido dentro da ARPA – Advanced Research Projects Agency, do Departamento de Defesa norte-americano. A pesquisa sobre rede que a ARPA montou, a partir dos anos 60, a ARPANET, certamente foi integralmente financiada por recursos militares e, assim, pareceria natural uma associação automática de suas características com o que se imaginaria associado à época da guerra fria e das tensões internacionais de então . Entretanto, independentemente da origem dos recursos para ARPANET – que por sinal contava com pesquisadores de primeira linha, oriundos das melhores universidades norte-americanas –, não se pode esquecer o caldo cultural em que a academia também estava indefectivelmente embebida. A data que consta como início da operação para a ARPANET, quando houve a primeira troca de pacotes de dados entre um computador na UCLA – Universidade da Califórnia em Los Ângeles – e outro no SRI – Stanford Research Institute – é 29 de outubro de1969. E foi exatamente em agosto de 1969 que ocorreu, nos Estados Unidos, o famoso festival Woodstock de música, símbolo da contracultura daqueles tempos...

Fiel aos tempos, a ARPANET assim nasceu como uma rede aberta, com padrões a serem amplamente discutidos na própria comunidade e adotados espontaneamente, acessível a todos e sem limitações quanto ao conteúdo trafegado a seus emissores ou receptores.

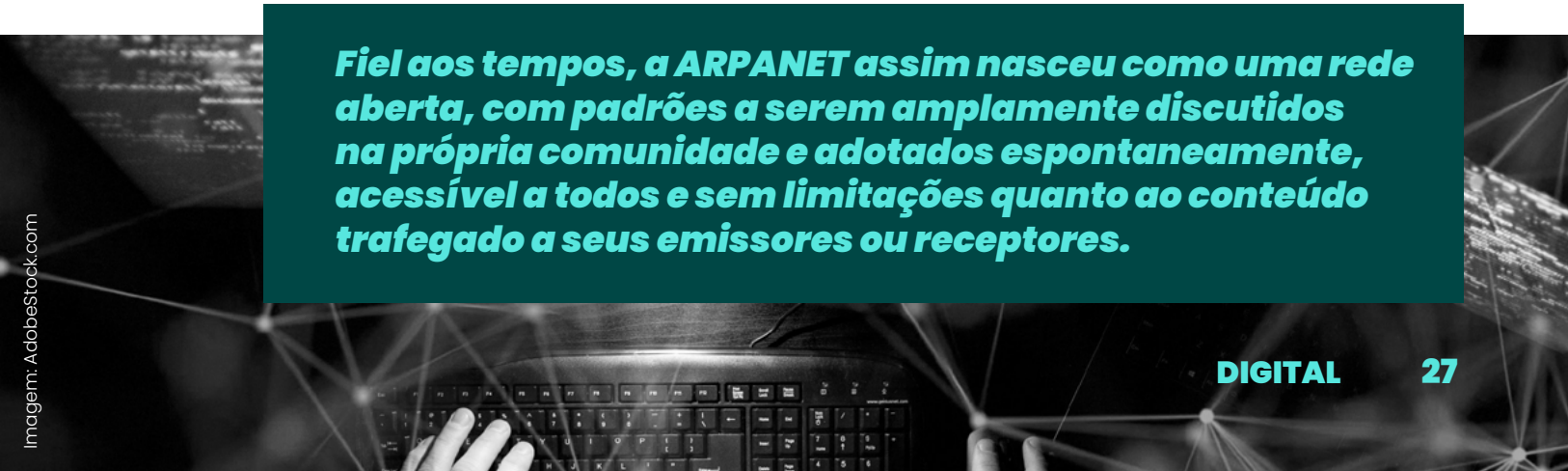


Imagem: AdobeStock.com

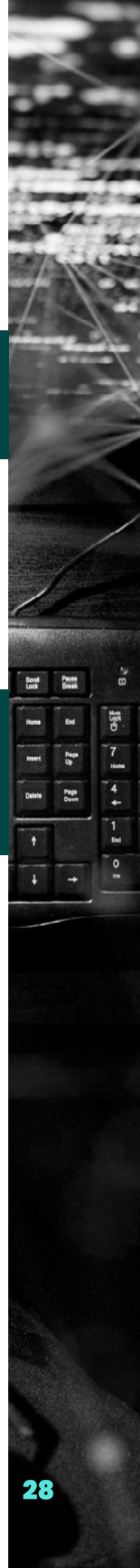
Essas características podem ser facilmente rastreadas nos documentos da época, ligados ao desenvolvimento do projeto. Por exemplo, o nome que foi dado às propostas sobre temas técnicos para a rede foi RFC (Request for Comments), ou seja, "eis aí uma proposta que solicita comentários da comunidade". O primeiro RFC, o RFC 1, é de abril de 1969, da autoria de Steve Crocker, pesquisador pioneiro envolvido no projeto ARPANET.

Outra característica fundante da rede que nascia foi a ausência de um centro de controle ou administração.

Excetuando-se a necessidade de atribuição de identidades unívocas aos elementos que se integrariam à rede, até para que houvesse condições técnicas de roteamento preciso dos pacotes entre a origem e o destino, nada mais dependeria de "autoridade central". A rede, portanto, até hoje, abstém-se de ter um controle centralizado e, menos ainda, de um "botão de desligamento".

Sua expansão sempre esteve associada apenas ao sucesso que teve em granjear adeptos e novos integrantes.

Em 1973, estava claro, até pelo acompanhamento dos RFC, que haveria necessidade de trocar o protocolo operando até então na rede, o chamado NCP (Network Control Program). Os pesquisadores que estavam a cargo do novo desenvolvimento eram Robert Elliot Kahn (Bob Kahn) e Vinton Gray Cerf (Vint Cerf). O protocolo proposto por eles foi o TCP (RFC 793, setembro de 1981– Transmission Control Protocol), cujo objetivo era garantir a transmissão segura e correta de mensagens na ARPANET. Além disso, queria-se manter o estímulo de conexão a quaisquer outras redes, que quisessem participar na troca de mensagens. Mantendo-se a autonomia de cada sub-rede, bastaria que ela estivesse de acordo quanto ao protocolo a se utilizar para que se integrasse ao conjunto ARPANET. Para implementar essa "costura", que transformasse os diversos retalhos constituintes da rede em um mosaico totalmente operacional, o TCP trabalharia sobre um componente especialmente importante: o protocolo "entre-redes", o IP (RFC 791, setembro de 1981- Internet Protocol). O conjunto, conhecido como TCP/IP, foi tão bem-sucedido que, em pouco tempo, tornou-se o "padrão de fato", deslocando o que seria o candidato oficial a ser usado em redes de computadores: a pilha ISO/OSI, desenvolvida pela UIT – União Internacional de Telecomunicações – como proposta de "padronização mundial" para o tema, e descrita no ISO-7498, de 1984.



A ARPANET original agora passava a ser apenas uma das muitas redes que constituíam o amplo conjunto que, muito justamente, passaria a ser conhecida pelo nome do protocolo que "colava" as sub-redes participantes: Internet.

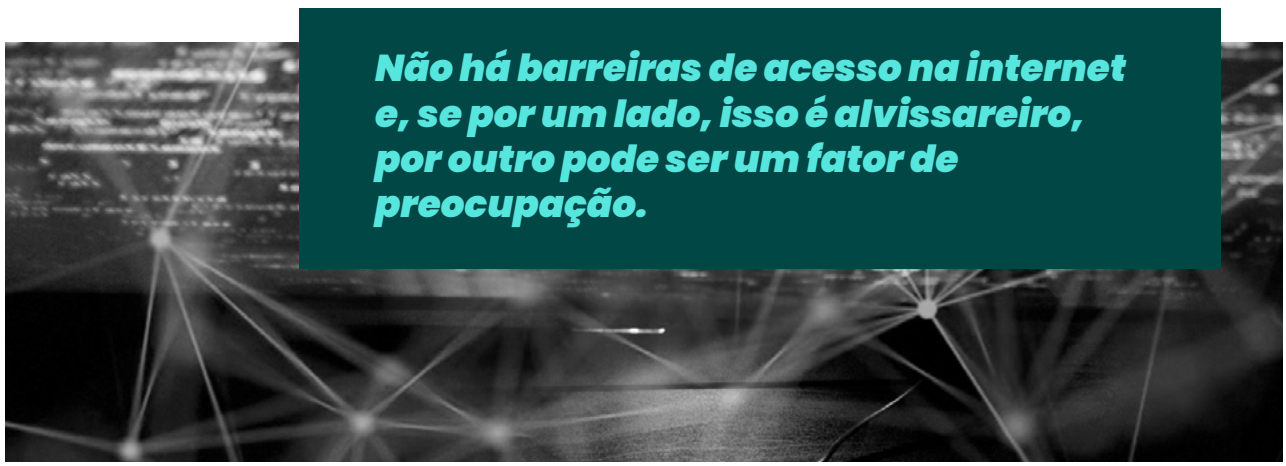
E a ARPANET seria oficialmente encerrada em julho de 1990, ficando sua parte acadêmica ligada à NSFNET (National Science Foundation Network) e a parte militar à MILNET (Military Network), além das diversas outras redes que já estavam se integrando ao conjunto global.

Quanto ao espírito inicial da rede, ele continuava cada vez mais vivo. Para ilustrar, há bordões representativos e que são muito conhecidos na "comunidade Internet", como a "lei de Postel" (Jon Postel), ou "princípio de robustez da rede: "sejamos conservadores no que enviamos, e liberais no que aceitamos dos outros"; e o lema do IETF (Internet Engineering Task Force), grupo de voluntários que se reúne três vezes ao ano para discutir RFC para a evolução da rede, e que foi enunciado por Dave Clark: "nós rejeitamos reis, presidentes e votações. Nós acreditamos apenas em mero consenso, e programação eficiente".

Em fevereiro de 1996, devido a algumas tratativas do governo norte-americano em criar legislação para o controle de conteúdos na internet, o futuro fundador da EFF (Eletronic Frontier Foundation), John Perry Barlow, escreveu o que ficou conhecido como a "Declaração da Independência do Ciberespaço", que, de várias formas, reflete o espírito fundador da internet. Em trechos de sua declaração, Barlow afirma que: "... o ciberespaço consiste de ideias, transações e relacionamentos próprios... o nosso mundo está, ao mesmo tempo, em todos os lugares e em lugar nenhum, mas não está lá onde as pessoas vivem. Estamos criando um mundo em que todos poderão entrar sem distinções ou preconceitos de raça, de poder econômico, de força ou de local de nascimento. Um mundo onde todos, de qualquer lugar, possam expressar suas opiniões, não importando o quão singulares elas sejam, sem o medo de serem coagidos ao silêncio ou à conformidade..."

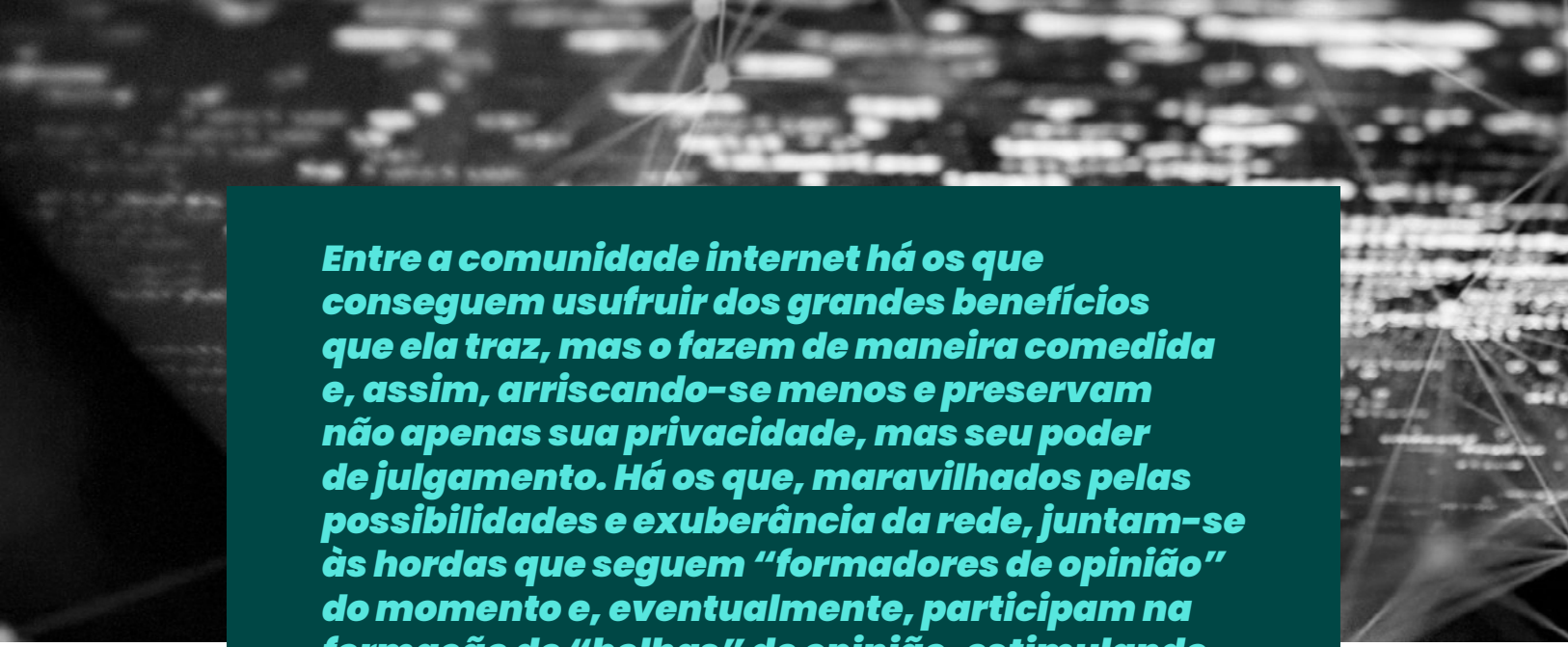
Muita água rolou desde 1996... A internet saiu do nicho original e passou a estar na vida de mais da metade dos habitantes do planeta. Algumas características dela tornaram-se, talvez, menos valorizadas... Por comodidade, ou pelo conforto que sentimos quando estamos em grupos homogêneos, a distribuição original, ampla e heterogênea da rede passou por uma intensa concentração: as redes sociais e os "jardins murados" criaram ambientes "acolhedores", onde nos sentiríamos mais aceitos pelos que lá coabitam. Com isso, a informação, que já estava muito potencializada pelo poder de disseminação da rede, passou, de alguma forma, a se amoldar mais e mais às nossas preferências. Claro que há muito de automação, informática e, eventualmente, inteligência artificial trabalhando aí e, com a quantidade enorme de dados pessoais disponíveis, certamente é sempre possível deduzir deles nossas preferências e gostos. E, claro, conhecer também nossos hábitos comerciais ou nossas posições políticas, com seus correspondentes vieses e incertezas.

Mais que isso, alguns mecanismos tradicionais que, de alguma forma, delimitavam a ação de cada indivíduo à sua área de interesse e especialidade, foram totalmente superados pela horizontalidade que a rede trouxe.



Não há barreiras de acesso na internet e, se por um lado, isso é alvissareiro, por outro pode ser um fator de preocupação.

Por exemplo, sempre houve uma tendência muito humana de seguir e imitar modelos, mas, no passado, esses eram raros e poucos. Com as redes e os novos "influenciadores", a potencialização no comportamento de se seguir alguém em relação a um tema – e com isso não se gastar tempo e esforço em organizar as próprias ideias – foi exponencial. E nada é mais fácil que repassar instantaneamente algo que se recebe de alguém, e que parece ir ao encontro de nossas convicções, ou assinalar claramente o apoio àquilo ("like"). Isso será usado pelos mecanismos da informática para que cada um receba "mais do mesmo", do que gostou e do que repassou: uma realimentação positiva. O perigo das realimentações positivas, como ensina a cibernética (e aqui usando essa palavra, cunhada por Norbert Wiener, em sua acepção original, que se relaciona à "teoria de controle"), é que elas podem conduzir a sistemas instáveis ou que se autodestruam.



Entre a comunidade internet há os que conseguem usufruir dos grandes benefícios que ela traz, mas o fazem de maneira comedida e, assim, arriscando-se menos e preservam não apenas sua privacidade, mas seu poder de julgamento. Há os que, maravilhados pelas possibilidades e exuberância da rede, juntam-se às hordas que seguem "formadores de opinião" do momento e, eventualmente, participam na formação de "bolhas" de opinião, estimulando acaloradas e na maioria das vezes inconsistentes discussões, onde os argumentos ad hominem são os que predominam. E há os que acabam de entrar na rede – o que é sempre positivo, visto que é fundamental que todos tenhamos acesso a ela – e, assim, podem ser potenciais e ingênuas vítimas das armadilhas e golpes que nela campeiam.

A vantagem de existir a internet e de poder usá-la livremente superam de longe os riscos que ela carrega. Entretanto, parece vital, não só para a sobrevivência da rede, mas também, e especialmente, para a preservação da civilidade nas relações humanas coletivas, e da morigeração no trato pessoal, que sempre observemos o princípio de Postel citado acima: "sejamos conservadores no que enviamos, e tolerantes no que recebemos".

Demi Getschko

Demi Getschko é Engenheiro eletricista, formado pela POLI/USP, com mestrado e doutorado em Engenharia, Conselheiro do CGI.br (Comitê Gestor da Internet no Brasil), Diretor-Presidente do NIC.br (Núcleo de Informação e Coordenação do Ponto br) e Professor Associado da PUC (Pontifícia Universidade Católica de São Paulo). Foi membro da diretoria da ICANN (Internet Corporation for Assigned Names and Numbers) pela ccNSO (Country Code Names Support Organization). Entre os seus reconhecimentos estão a eleição, em 2014, para o Hall da Fama da Internet na categoria "Conectores Globais", o prêmio "Cristina Tavares", da Sociedade Brasileira de Computação, e o prêmio "Personalidade da Tecnologia 2014", na categoria "Internet", do Sindicato dos Engenheiros no Estado de São Paulo, e a Ordem do Mérito das Comunicações no "Grau de Oficial". Desde 2014, publica uma coluna quinzenal no Caderno Link – Editoria de tecnologia e cultura digital do jornal O Estado de S. Paulo e do portal Estadao.com.br.

doi.org/10.52959/2021535404

A APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS É SUFICIENTE PARA GERAR SEGURANÇA E CONFIANÇA NA SOCIEDADE?

Miriam Wimmer e
Lucas Borges de Carvalho

A confiança é um recurso compartilhado e intangível que garante estabilidade e previsibilidade às relações sociais e econômicas, além de promover e incentivar o comportamento ético e cooperativo. Em particular no ambiente digital, trata-se de um elemento central para viabilizar a inovação e o desenvolvimento de novos negócios de forma sustentável e compatível com a garantia de direitos fundamentais, como a liberdade de expressão e a privacidade. Nesse sentido, um aplicativo que se propõe a substituir um serviço costumeiramente prestado em meio físico precisa, entre tantos outros desafios, demonstrar aos seus potenciais clientes que é confiável, sob pena de não obter êxito no mercado.

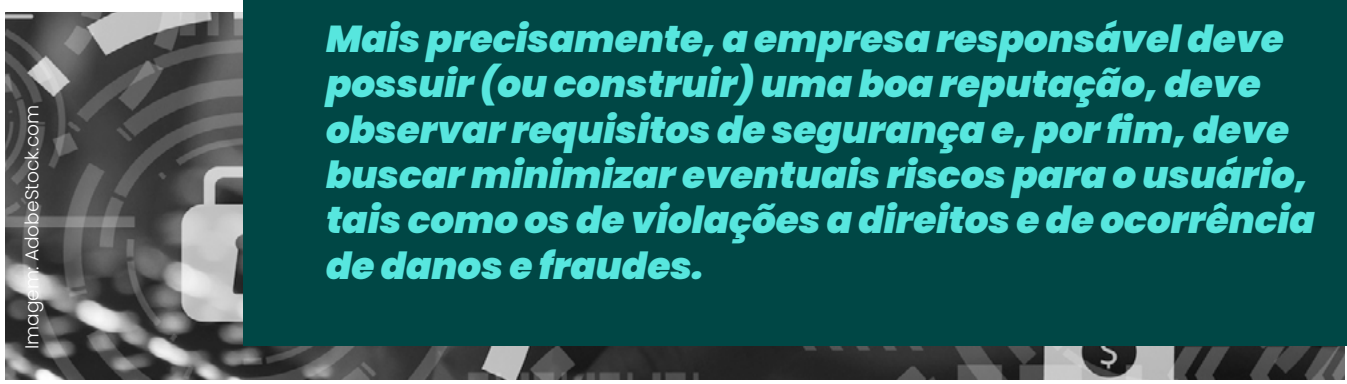


Imagem: AdobeStock.com

Mais precisamente, a empresa responsável deve possuir (ou construir) uma boa reputação, deve observar requisitos de segurança e, por fim, deve buscar minimizar eventuais riscos para o usuário, tais como os de violações a direitos e de ocorrência de danos e fraudes.

Considerando os três elementos mencionados, isto é, a reputação, a segurança e os riscos, pode-se afirmar que a principal base sobre a qual se erige a confiança no ambiente digital é a proteção de dados pessoais. Isso ocorre porque grande parte das novas tecnologias e aplicações, incluindo aquelas utilizadas pelo setor público, recorre ao tratamento automatizado de quantidades massivas de dados pessoais. Por isso, consumidores e usuários de serviços públicos estão cada vez mais conscientes e preocupados com as possíveis violações à sua privacidade e com o uso indevido de seus dados pessoais.[1] Ao mesmo tempo, cabe lembrar que o tratamento inadequado de dados pessoais pode gerar impactos adversos não apenas para os indivíduos afetados, mas também para as organizações envolvidas.

Daí que se compreende que o uso irrestrito e sem regras desse que é o grande ativo que mobiliza a economia do século XXI pode gerar efeitos negativos sistêmicos sobre todo o ecossistema digital, que podem ser comparados aos que decorrem da exploração desenfreada de recursos naturais ocorrida nas últimas décadas. Vale dizer, tanto num caso como no outro, que há o risco de ocorrer o que os economistas chamam de "tragédia dos comuns", situação na qual todos perdem e sofrem com os problemas gerados em razão do predomínio de decisões fundadas em considerações de curto prazo, que atingem e minam a sustentabilidade dos recursos coletivos no longo prazo, entre os quais a própria confiança[2].

Garantir e promover o uso transparente e sustentável dos dados pessoais, com a consequente ampliação da autodeterminação informativa dos titulares, constitui um dos principais propósitos da Lei Geral de Proteção de Dados Pessoais (LGPD). Promulgada em 2018 e com vigência plena a partir de agosto de 2021, a LGPD estabeleceu princípios e regras que garantem direitos aos titulares, delimitam o campo legítimo para o tratamento de dados pessoais e estabelecem obrigações para os agentes de tratamento, tudo sob a supervisão de uma autoridade nacional com autonomia técnica e decisória, a Autoridade Nacional de Proteção de Dados (ANPD).

Porém, a ausência de uma cultura de proteção de dados pessoais no país, associada ao caráter inovador e abrangente da lei, impõe uma série de obstáculos à sua implementação.

Embora estejam ainda em construção indicadores confiáveis para avaliar o grau de conformidade de organizações públicas e privadas à LGPD, pesquisas preliminares indicam, em geral, um baixo nível de maturidade no que tange ao tema[3]

Nesse contexto, a ANPD terá papel decisivo para orientar e estimular as organizações privadas e públicas a atuar em conformidade com a lei. O desafio é o de romper com a inércia e com a equivocada percepção, ainda comum em alguns setores, de que a nova lei trouxe apenas custos burocráticos e financeiros desnecessários. É fundamental, por isso, demonstrar que não há caminho possível para a inovação e para o desenvolvimento econômico, em particular no ambiente digital, que não a construção de uma "relação de confiança com o titular, por meio de atuação transparente", baseada no respeito à legislação de proteção de dados pessoais, conforme previsto no art. 50 da LGPD.

Essa é, de fato, a visão preconizada pela legislação, que aponta, entre seus fundamentos (art. 2º, LGPD), o desenvolvimento econômico e tecnológico, a inovação, a livre iniciativa e a livre concorrência, juntamente com outros princípios voltados à garantia da privacidade e de outros direitos fundamentais.

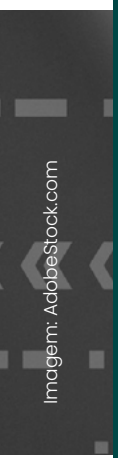


Imagem: AdobeStock.com

A preocupação em estabelecer uma relação dialética entre, de um lado, considerações relacionadas ao papel dos dados pessoais enquanto insumo econômico e, de outro, ao seu reconhecimento como projeção da personalidade humana, é visível também nos diversos dispositivos que indicam ser competência da ANPD estabelecer regulação diferenciada, mediante simplificação ou dispensa de obrigações, para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação.

Desse modo, elementos centrais a serem avaliados pela ANPD no estabelecimento de tais regras diferenciadas incluem não apenas a natureza e o porte da entidade em questão, mas também o risco que as atividades de tratamento de dados podem gerar para o titular de dados.

Importa observar que a LGPD alinhou-se às melhores práticas internacionais ao prever diferentes formas de participação social na construção do ambiente regulatório. Assim, para além da obrigatoriedade de realização de análises de impacto regulatório, consultas públicas e audiências públicas – instrumentos já empregados tradicionalmente por diversos órgãos da Administração Pública –, a Lei determina, de maneira genérica, que cabe à ANPD ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento (art. 55-J, inc. XIV, LGPD). O desempenho de tal atribuição tem se materializado, dentre outros instrumentos, pela publicação da Agenda Regulatória da ANPD, acompanhada de relatórios semestrais de implementação, assim como pela utilização de uma combinação de instrumentos formais e informais de interação com a sociedade, a exemplo de Reuniões Técnicas e Tomadas de Subsídios sobre temas contemplados na Agenda.

Aprofundando tal perspectiva de transparência e participação, a LGPD explicitamente abre espaço para a construção de mecanismos autorregulatórios e corregulatórios, reconhecendo que em muitas circunstâncias os próprios agentes de tratamento estarão mais bem posicionados para identificar as especificidades de seu setor e, a partir daí, formular regras de boas práticas e de governança que levem em consideração uma abordagem baseada em riscos.

Nessa linha, vale destacar o princípio da responsabilização e prestação de contas (art. 6º, X, LGPD), que atribui aos agentes de tratamento a obrigação de adotar medidas visando ao eficaz cumprimento das normas de proteção de dados pessoais.

Dessa forma, para além da atuação do órgão regulador, a lei expressamente conferiu às organizações um papel central a ser desempenhado no processo de construção de uma cultura da proteção de dados pessoais no país. Destacam-se aqui a adoção de boas práticas, a exemplo do privacy by design, de regras de transparência e de mecanismos que facilitem o exercício de direitos pelos titulares; e a implementação de mecanismos adequados de governança, que viabilizem o monitoramento contínuo de riscos e a avaliação periódica das ações da organização, incluindo as medidas de prevenção e segurança implementadas.

Em conclusão, pode-se dizer que a aplicação prática da LGPD e a consequente proteção dos cidadãos constituem um empreendimento de natureza coletiva, cuja execução se protrai no tempo e cujo êxito demanda o compromisso e a colaboração ativa de todos os atores sociais relevantes, em especial a ANPD, as empresas e os órgãos públicos. Somente assim será possível gerar e fortalecer a confiança social que viabiliza e impulsiona a criação e o uso de novas tecnologias e ferramentas digitais, sempre com o necessário respeito a padrões técnicos e jurídicos que assegurem a proteção de dados pessoais.

Miriam Wimmer

Miriam Wimmer é Doutora em Políticas de Comunicação e Cultura, pela Faculdade de Comunicação da UnB, e Mestra em Direito Público, pela UERJ. É professora do corpo permanente do Mestrado Profissional em Direito do IDP e professora convidada de Direito Digital e Proteção de Dados Pessoais em diversas instituições.

Lucas Borges de Carvalho

Lucas Borges de Carvalho é Doutor em direito, pela Universidade de Brasília (UnB), e Mestre em Direito, pela Universidade Federal de Santa Catarina (UFSC). Procurador Federal.

Imagem: AdobeStock.com

NOTAS E REFERÊNCIAS

1 Nos Estados Unidos, por exemplo, pesquisa do Pew Research Center identificou que 70% dos americanos acreditam que seus dados pessoais estão menos protegidos nos dias de hoje do que há cinco anos. Da mesma forma, 81% disseram que os riscos provenientes da coleta de dados por empresas superam os potenciais benefícios. PEW RESEARCH CENTER. Americans and Privacy: concerned, confused and feeling lack of control over their personal information, 24 nov. 2019. Disponível em: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/. Acesso: 26 ago. 2021.

2 ARIELY, Dan. Previsivelmente irracional: as forças invisíveis que nos levam a tomar decisões erradas. Rio de Janeiro: Sextante, 2020, p. 218-221; HOLMES, Stephen. SUSTEIN, Cass. O custo dos direitos: por que a liberdade depende dos impostos. São Paulo: Martins Fontes, 2019, p. 54-59.

3 Com efeito, pesquisa recente identificou que, embora 93% das empresas entrevistadas tenham manifestado algum conhecimento sobre a LGPD, somente 15% confirmaram estar prontas para atender às novas determinações legais. Além disso, dois terços sequer implementaram medidas básicas, como a criação de políticas de proteção de dados. CORACCINI, Raphael. Empresas não conseguem se adaptar à lei de proteção de dados, aponta pesquisa. CNN Brasil, 20 ago. 2021. Disponível em: https://www.cnnbrasil.com.br/business/empresas-nao-conseguem-se-adaptar-a-lei-de-protecao-de-dados-diz-pesquisa/?utm_campaign=newsletter_-_24082021&utm_medium=email&utm_source=RD+Station. Acesso: 26 ago. 2021.

doi.org/10.52959/2021535405

IDENTIDADE DIGITAL É O CAMINHO PARA DAR MAIS SEGURANÇA AOS CIDADÃOS E ÀS PEQUENAS EMPRESAS?

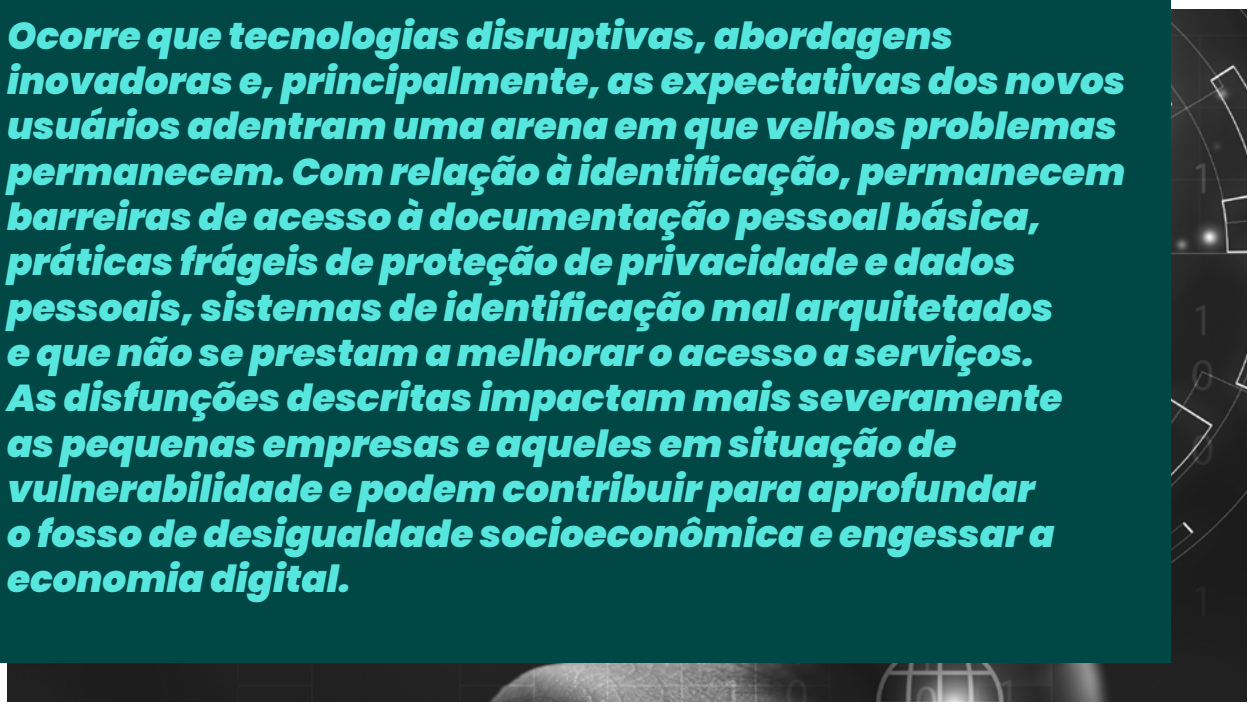
Janaina Costa
Celina Carvalho

As práticas de identificação estão presentes em diferentes setores da sociedade. Direito de voto, acesso à saúde, inclusão financeira, proteção social, direitos trabalhistas, acesso à justiça e à propriedade, entre outros, dependem da identificação das pessoas. São, portanto, chaves de acesso a muitos outros direitos.

Não é por coincidência que o direito à identidade legal está consagrado na Declaração Universal dos Direitos Humanos, sendo a universalização da Identidade Legal uma das metas da Agenda 2030 das Nações Unidas para o desenvolvimento sustentável (ODS 16.9). Com isso, há implicações diretas para a jornada de transformação digital, ao garantir que todos possam verificar a sua identidade perante o setor público e privado.

As inovações digitais em identidade trazem novas oportunidades para entregar serviços mais bem administrados, transparentes e confiáveis. Possuem também a capacidade de distribuir e interpretar quantidades significativas de informações sobre as pessoas e suas comunidades. Dessa forma, redefinem oportunidades em todo o mundo para desenvolver novos valores econômicos, para governar e servir em sociedades mais acessíveis e para empoderar indivíduos. A identidade digital é, portanto, crucial na transformação digital da conjuntura econômica e social. Devemos ser facilmente capazes de comprovar (ou demonstrar) digitalmente quem somos. Nesse diapasão, a OCDE[1] aponta a identidade digital como um dos pilares da transformação digital do setor público e da economia. Em relação ao Brasil, o Relatório da Mckinsey Global Institute[2] indica que a economia do país pode crescer 13% se ajustar seu déficit de identidade digital. Isso coloca o Brasil como o país que mais pode crescer, no mundo, com investimentos em identidade digital.

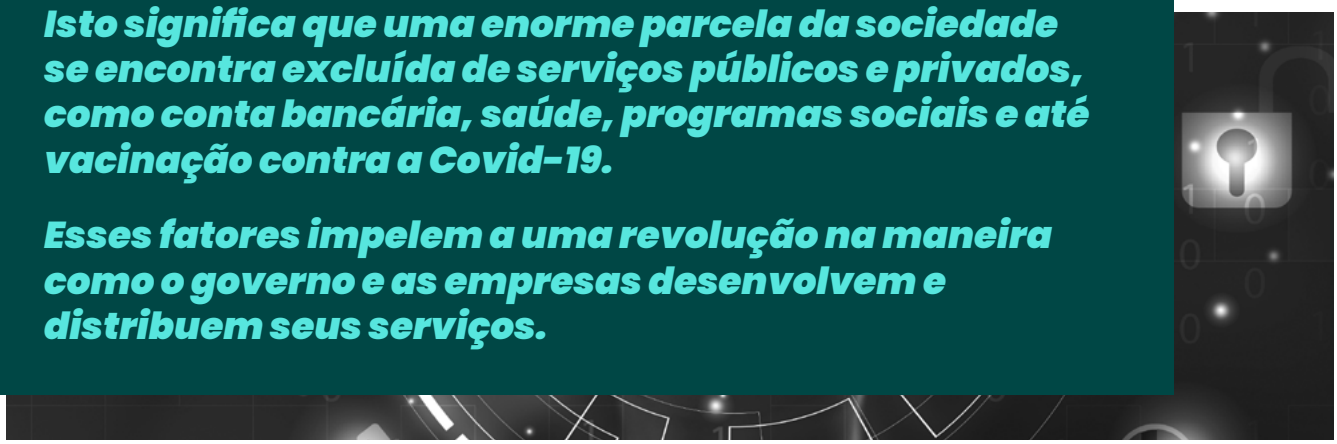
Ocorre que tecnologias disruptivas, abordagens inovadoras e, principalmente, as expectativas dos novos usuários adentram uma arena em que velhos problemas permanecem. Com relação à identificação, permanecem barreiras de acesso à documentação pessoal básica, práticas frágeis de proteção de privacidade e dados pessoais, sistemas de identificação mal arquitetados e que não se prestam a melhorar o acesso a serviços. As disfunções descritas impactam mais severamente as pequenas empresas e aqueles em situação de vulnerabilidade e podem contribuir para aprofundar o fosso de desigualdade socioeconômica e engessar a economia digital.



O Banco Mundial estima que existam ainda 1 bilhão de pessoas sem acesso à identificação oficial no mundo. No Brasil, segundo dados do IBGE, esse número corresponde a 3 milhões de pessoas. São brasileiros que chegam à vida adulta sem sequer certidão de nascimento – registro obrigatório para qualquer outro documento.

Isto significa que uma enorme parcela da sociedade se encontra excluída de serviços públicos e privados, como conta bancária, saúde, programas sociais e até vacinação contra a Covid-19.

Esses fatores impelem a uma revolução na maneira como o governo e as empresas desenvolvem e distribuem seus serviços.



É preciso encontrar meios para suprir a demanda dos cidadãos ainda sem acesso à identificação formal e também inovar para solucionar os gargalos encontrados pelas pequenas empresas para adentrar a economia digital e melhorar a experiência do cliente, sem jamais olvidar da proteção de dados pessoais.

É nesse cenário que a identidade digital se mostra como um caminho para dar mais segurança aos cidadãos e às pequenas empresas no Brasil. Para explorar propriamente o potencial da identidade para segurança, é necessário compreender que existem tipos de identidade diferentes para acessar serviços diferentes. Veja-se que sua definição pode ser estabelecida, por exemplo, por um conjunto de atributos armazenados e capturados eletronicamente (nome, sexo, data de nascimento e dados biométricos), e/ou credenciais que identificam exclusivamente uma pessoa (cartões de identificação, PINs, aplicativos móveis). A diferença entre sistemas impacta desde a forma como o serviço será prestado até a segurança dele. Por ser tão complexo, é importante analisar as práticas para entender e planejar o sistema de identidade mais adequado.

O que estamos pretendendo aqui é sugerir utilizar a identidade digital como plataforma para dar mais segurança.

Existem já várias complexidades no gerenciamento de identidade tradicional. Indiscutivelmente, em formato digital alguns dos desafios podem ser potencializados. O primeiro passo para atingir esse objetivo é incentivar a visão holística sobre identidade digital. A compreensão de que ela pode ir além de uma tecnologia ou um aparelho deve ser pensada em conjunto com uma estratégia, como plataforma para a sociedade digital, fundada em uma instituição responsável, uma legislação consistente e meios técnicos que permitam sua interoperabilidade com diferentes sistemas de informação.

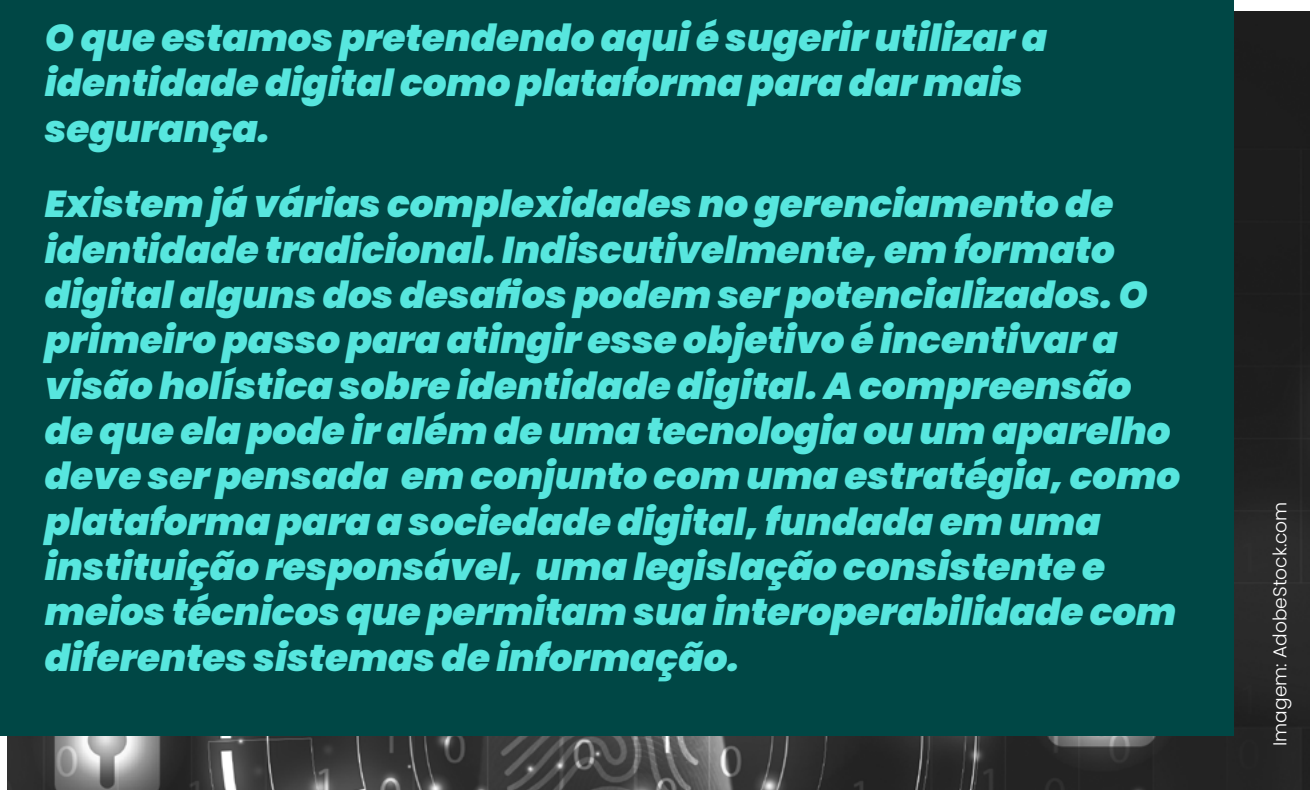
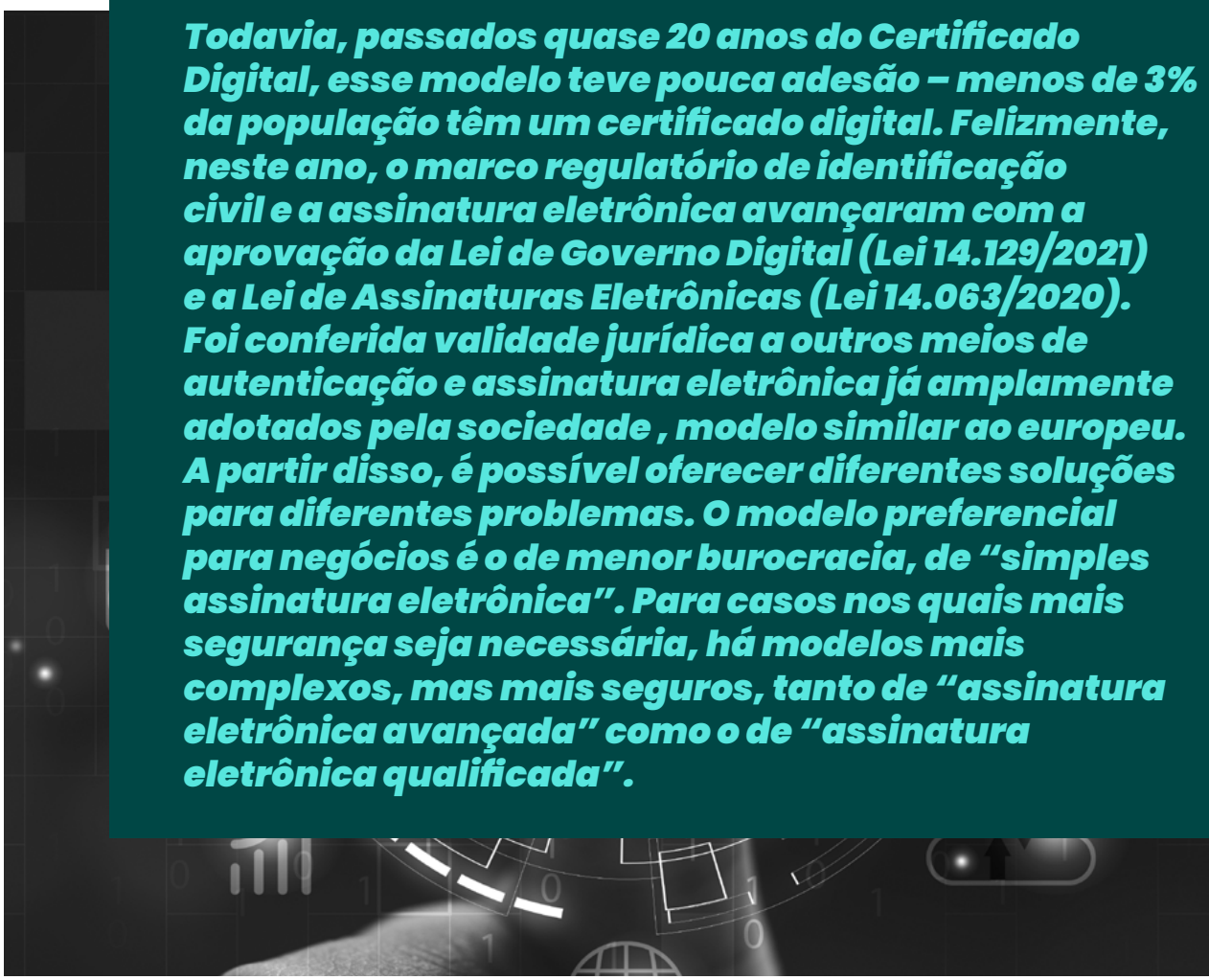


Imagem: AdobeStock.com

Cabe mencionar os riscos presentes no processo de implementação da identidade digital. No que tange aos dados utilizados, existem diferentes conjuntos de dados mínimos para fins de setores e serviços específicos. Uma prática comum é a captura de mais dados para registro do que é necessário para sua finalidade original . Isso compromete a segurança, porque a quantidade de dados coletados é proporcional ao risco de desvio de finalidade e aos possíveis danos à privacidade dos usuários em caso de vazamento, uso indevido ou compartilhamento não autorizado. Por exemplo, não deve ser negligenciado o fato de que os dados financeiros e de saúde, exigidos em usos setoriais da identificação digital, são muito sensíveis e seu uso indevido ou vazamento podem levar à exclusão e discriminação.

Para citar apenas alguns riscos, a exposição a um status de doença ou situação de vulnerabilidade econômica pode significar ter crédito negado ou taxas mais altas em seguros de saúde, perpetuando a exclusão socioeconômica e de acesso a serviços em vez de reduzi-las.

Desde a ampliação do uso da internet, os governos tentaram definir uma forma segura de identificar indivíduos no mundo digital. Um exemplo dessa adoção precoce foi a criação da Infraestrutura de Chaves Públicas (ICP-Br) no Brasil, em 2001. A MP 2.002–2, que criou a ICP-Br, estabeleceu um marco fundamental e deu segurança para entrada de novos atores em diversos setores da economia no mundo digital.



Todavia, passados quase 20 anos do Certificado Digital, esse modelo teve pouca adesão – menos de 3% da população têm um certificado digital. Felizmente, neste ano, o marco regulatório de identificação civil e a assinatura eletrônica avançaram com a aprovação da Lei de Governo Digital (Lei 14.129/2021) e a Lei de Assinaturas Eletrônicas (Lei 14.063/2020). Foi conferida validade jurídica a outros meios de autenticação e assinatura eletrônica já amplamente adotados pela sociedade , modelo similar ao europeu. A partir disso, é possível oferecer diferentes soluções para diferentes problemas. O modelo preferencial para negócios é o de menor burocracia, de "simples assinatura eletrônica". Para casos nos quais mais segurança seja necessária, há modelos mais complexos, mas mais seguros, tanto de "assinatura eletrônica avançada" como o de "assinatura eletrônica qualificada".

Com isso, abriu-se caminho para que seja implementada uma identidade digital pensada como plataforma, confiável, e que possa ser utilizada para acessar múltiplos serviços de maneira fácil e garantir uma maneira simples e segura de controlar a quantidade de informações que o cidadão deseja compartilhar com serviços que exigem o compartilhamento de informações, nos moldes estabelecidos pela LGPD.

Em um cenário em que a identidade digital é pensada como plataforma e em que o cidadão tem o controle de seus dados e decide quanta informação compartilhar sobre si mesmo, com quem e com que propósito, é uma oportunidade única de garantir maior segurança ao cidadão e às empresas e facilitar a adequação das empresas à Lei Geral de Proteção de Dados (LGPD).

Nesse sentido, é importante entender os elementos necessários para construir uma identidade digital como uma plataforma no Brasil. Isso significa que a identidade deve ser vista como uma infraestrutura para uma boa governança do Estado, pois permite que todos os indivíduos sejam reconhecidos perante o governo e a sociedade, provendo meios de autenticação para acesso a serviços e benefícios. A partir dessa perspectiva, deve-se entender as formas que o sistema de identidade digital pode contribuir para o futuro do crescimento econômico e do aprimoramento na prestação de serviços e políticas públicas. Em outras palavras, um sistema de identidade robusto e bem implementado é um importante passo para estabelecer confiança e segurança entre governo e sociedade e, a partir disso, desenvolver e explorar as oportunidades descritas.

Não se pode esquecer, todavia, que a implementação de um sistema robusto encontra certos desafios. Dentre eles, existem preocupações de proteção de dados que não devem ser ignoradas na construção de um sistema de identidade digital. Como se não bastasse a natural responsabilidade advinda de coletar e gerenciar dados pessoais, o próprio funcionamento das identidades digitais depende diretamente de um fluxo de informações de qualidade. É justamente nessa linha que se estabelece o princípio da qualidade dos dados da LGPD, que garante aos titulares exatidão, clareza, relevância e atualização dos dados.

Assim, o fortalecimento do ecossistema brasileiro de proteção de dados é chave para garantir a devida implementação da identidade digital e explorar seus benefícios.

Por sua vez, como vimos, a identidade digital tem o potencial de estimular a confiança nas relações entre os atores e também implicar em boas práticas de proteção de dados, visto que evitam por vezes o compartilhamento indevido de informações.

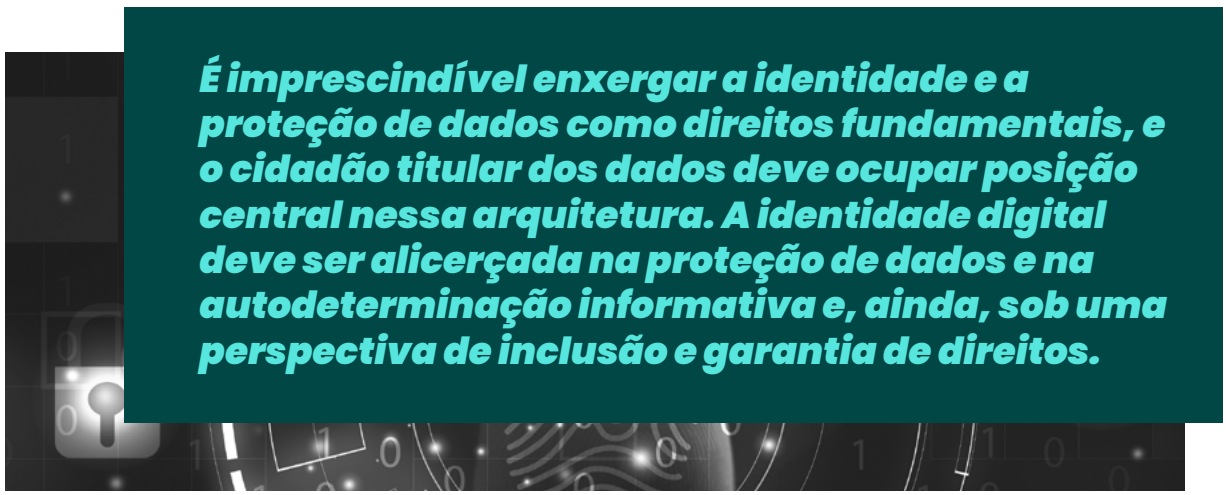
A identidade digital pode ser uma oportunidade para fomentar um ambiente seguro, acessível e confiável, a estimular o desenvolvimento da economia digital. É nesse sentido que o Serpro empregou[3] a identidade digital para dar mais segurança aos dados pessoais dos cidadãos.

Em particular, o contexto brasileiro poderia aproveitar dessa oportunidade, considerando o aparente crescimento de desconfiança mediante às frequentes notícias de vazamentos de dados , seja no vazamento que envolveu 220 milhões de brasileiros,[4] de 100 milhões de dados de celulares[5] ou no vazamento do Superior Tribunal de Justiça[6]. De forma semelhante, o ecossistema de inovação de pequenas e médias empresas brasileiro também apresenta características oportunas para usufruir dos benefícios da identidade digital impulsionar o crescimento da economia digital. Em 2018, o Brasil foi considerado o maior ecossistema de fintechs da América Latina, contando com 377 dessas startups. No entanto, a adequação à LGPD ainda é um motivo de grande preocupação para pequenas empresas – somente 37% das pequenas e médias empresas estão adequadas à Lei, segundo dados do Sebrae. Neste cenário, a identidade digital se destaca como um elemento essencial do futuro do país. É imprescindível facilmente provar (ou demonstrar) digitalmente quem se é e ter maior controle sobre nossos dados, bem traduzido pela LGPD como o princípio da autodeterminação informativa.

Um sistema de identificação digital bem implementado, que ofereça um alto nível de garantia e adote recursos e protocolos avançados de segurança para proteger dados de identificação de pessoas, é fundamental para usufruir dos possíveis benefícios. Isso inclui economizar dinheiro e tempo na execução de procedimentos burocráticos, mas também adicionar segurança e confiança para cidadãos e empresas, vis-à-vis a adequação aos preceitos da LGPD.

Considerando a sensibilidade de lidar com a proteção dos dados pessoais e das identidades digitais, recentemente, no Brasil, tem ocorrido uma ampla discussão em como assegurar a proteção dessas informações. A LGPD traz importantes salvaguardas para serem consideradas nos sistemas de identidade digital.

Diante do cenário apresentado, uma plataforma de identidade eficiente e segura pode elevar a transformação digital do Estado e do setor privado no Brasil a um novo patamar. Mas vai além de ser um instrumento de fomento da economia digital e oportunidade de inovação.



É imprescindível enxergar a identidade e a proteção de dados como direitos fundamentais, e o cidadão titular dos dados deve ocupar posição central nessa arquitetura. A identidade digital deve ser alicerçada na proteção de dados e na autodeterminação informativa e, ainda, sob uma perspectiva de inclusão e garantia de direitos.

Janaina Costa

Advogada. Pós-Doutoranda em Direito Digital (UERJ); Mestre em Desenvolvimento Econômico e Social pelo IEDES - Paris 1 Panthéon-Sorbonne; Bacharel em Direito (UFMG). Pesquisadora Sênior da área de Direito e Tecnologia no Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio).

Celina Carvalho

Advogada. Pós-Graduanda em Direito Digital (UERJ). Bacharel em Direito pela Universidade do Estado do Rio de Janeiro. Pesquisadora da área de Direito e Tecnologia no Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio).

Imagem: AdobeStock.com

NOTAS E REFERÊNCIAS

1 https://www.oecd.org/going-digital/strengthening-digital-government.pdf

2 https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.pdf

3 https://www.gov.br/casacivil/pt-br/assuntos/noticias/2020/setembro/serpro-emprega-identidade-digital-descentralizada-par-

4 https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml

5 https://www.uol.com.br/tilt/noticias/redacao/2021/02/10/vazamento-expoe-registros-de-mais-de-100-milhoes-de-contas-de-celular.htm

6 https://www.uol.com.br/tilt/noticias/redacao/2020/11/09/ataque-no-stj-hacker-continua-com-o-controle-de-documentos-sigilosos.htm

doi.org/10.52959/2021535406

POR QUE *CIBERSECURITY* DEVERIA SER PRIORIDADE PARA AS EMPRESAS?

Leidivino Natal

A transformação digital e o rápido avanço tecnológico dos últimos anos fizeram com que o setor de TI (tecnologia da informação) assumisse um papel estratégico nas organizações. Os dados utilizados para as tomadas de decisão se tornaram verdadeiros ativos e, consequentemente, precisaram ser gerenciados com mais eficiência.

O ano de 2020 ficou marcado como um ano atípico. De potencial virada econômica, o ano foi palco de uma crise sanitária e política sem precedentes jamais vista, de alcance global. O mundo do trabalho teve que se reinventar às pressas e transformações que estavam em vias de desenvolvimento paulatino tiveram um *speedup* repentino, que fizeram muitas empresas redesenharem suas estratégias. O digital não é mais uma opção, um *add-on* ou um benefício da rotina. É a realidade de muitas empresas. Com as mudanças, as pessoas em casa sendo os novos *targets* a serem alcançados, os dados ganharam um lugar de protagonismo nas estratégias.

O ritmo da transformação digital não foi acompanhado de proteção suficiente para um novo modelo de trabalho que tornou os dados das organizações mais vulneráveis, com acessos através de mais aparelhos móveis e conexões domésticas. A informação extrapolou o escritório e as organizações precisaram redesenhar suas políticas de segurança com o foco na proteção dos endpoints.

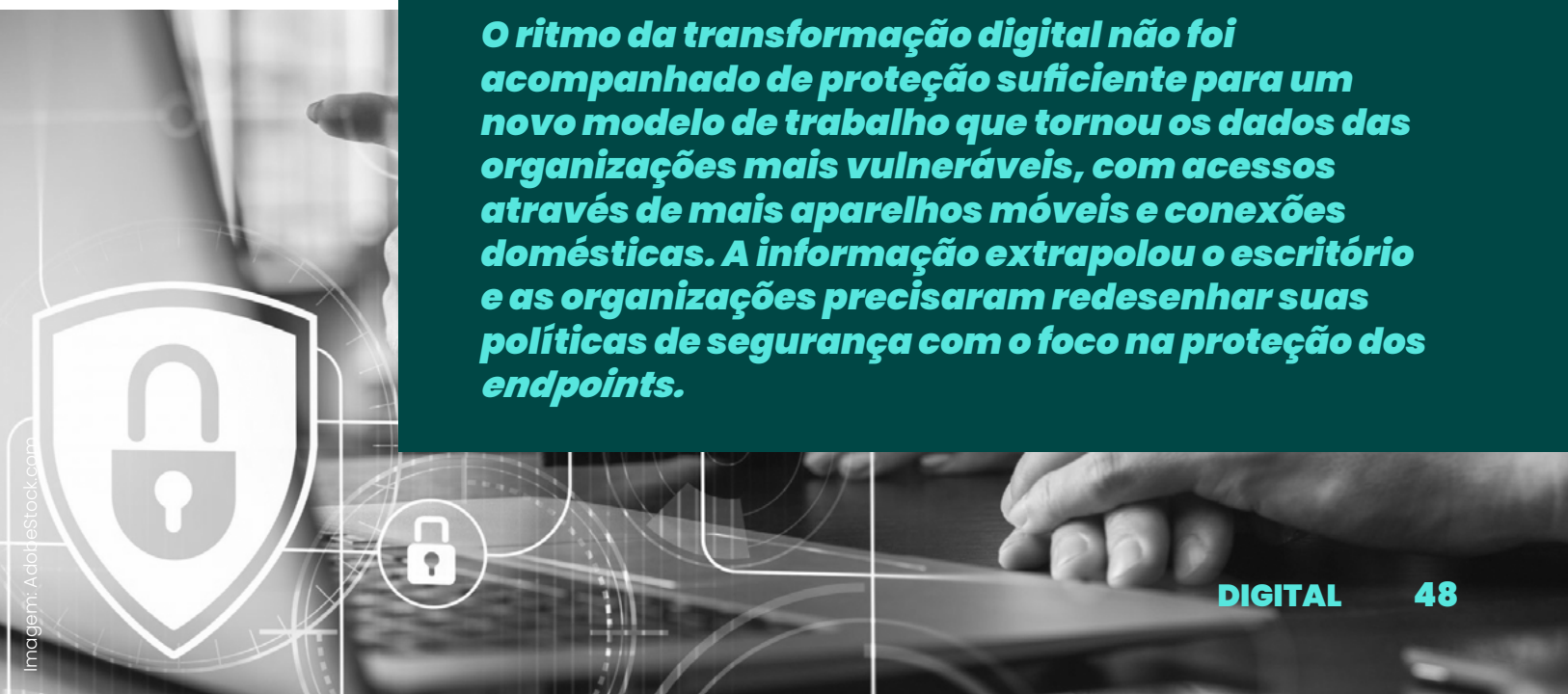
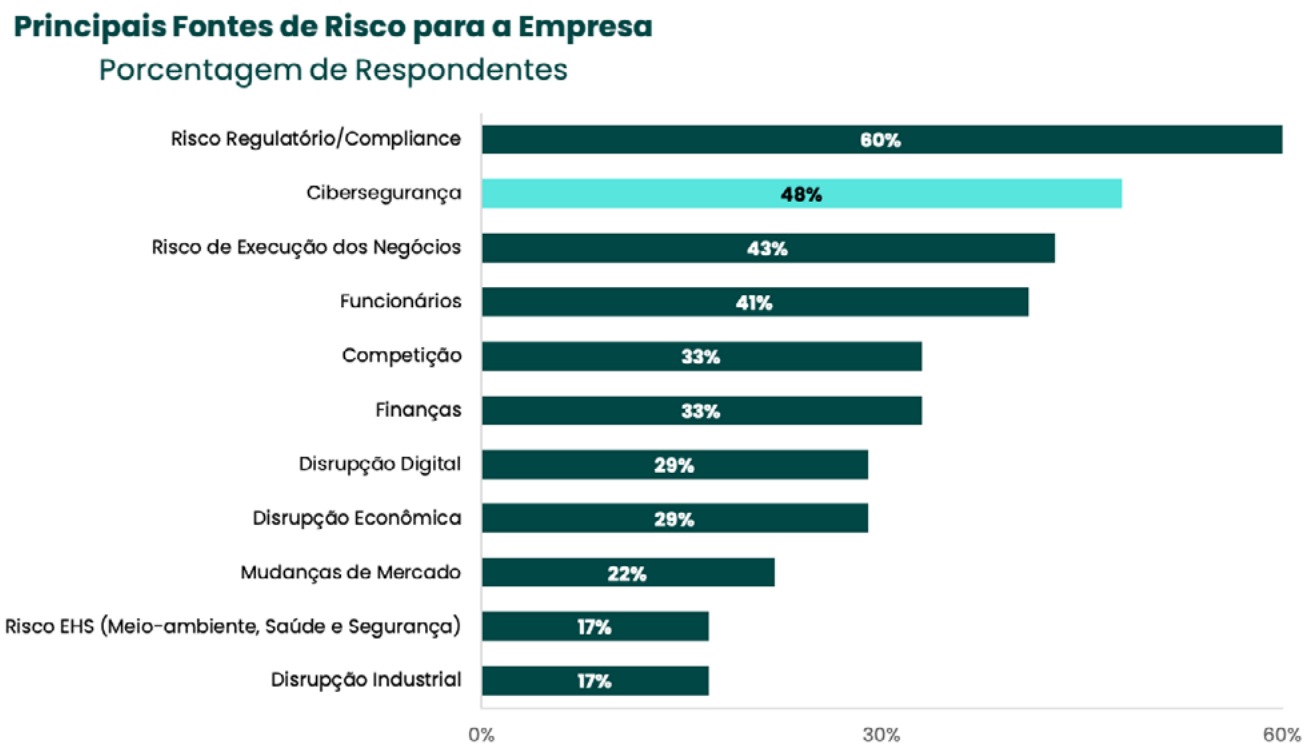


Imagem: AdobeStock.com

Todos nós, quase que semanalmente, lemos notícias sobre um grupo de *hackers* que invadiu sistemas empresariais, bancários ou até mesmo governamentais, causando caos e prejuízos financeiros. Somente no primeiro trimestre deste ano ocorreram 3,2 bilhões de ataques cibernéticos no Brasil, figurando o nosso país como líder no *ranking* de países latinos.[1]

Nesse cenário, a segurança da informação nas empresas ganhou destaque e passou de um item no *checklist* de projetos para a continuidade do negócio e posicionamento das organizações no mercado.

De acordo com pesquisa realizada pelo Gartner (2020), atualmente, a segurança cibernética é a 2ª maior preocupação dos Conselhos Estratégicos das organizações, ficando atrás apenas de compliance[2].



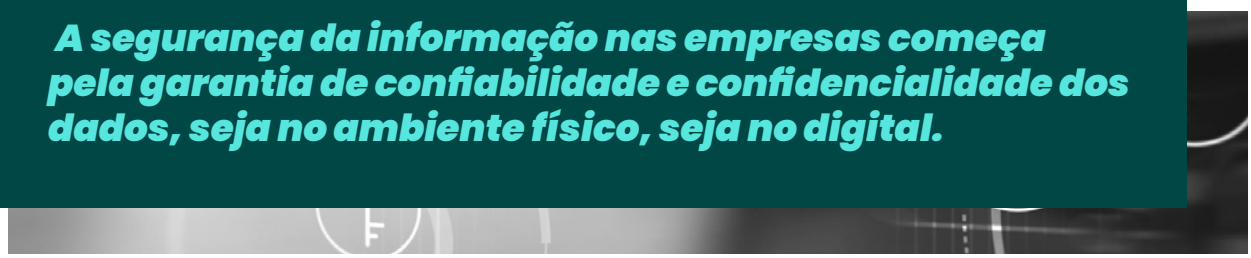
POR QUE A SEGURANÇA DEVE ESTAR NA SUA LISTA DE PRIORIDADES?

AMEAÇA À CONFIDENCIALIDADE DOS DADOS

A confidencialidade é muito mais do que simplesmente manter os dados da empresa protegidos a sete chaves. O conceito, que está entre os pilares da segurança da informação, não se trata de bloquear os dados, mas de se ter governança sobre quem são as pessoas autorizadas a acessá-los. A falta de atenção a este tópico pode acarretar severos prejuízos às organizações, pois além da possibilidade de um sistema sair do ar e prejudicar operações, o vazamento pode significar que pessoas estão acessando informações sensíveis e que sua gestão de segurança está vulnerável.

Se esse tipo de informação é roubado ou vaza de alguma forma, os clientes e parceiros da empresa são afetados diretamente. Consequentemente, isso pode resultar em prejuízos incalculáveis para sua organização, seja por um processo judicial por violação de privacidade ou quebra de contrato ou pelo comprometimento da sua marca perante o mercado e os consumidores.

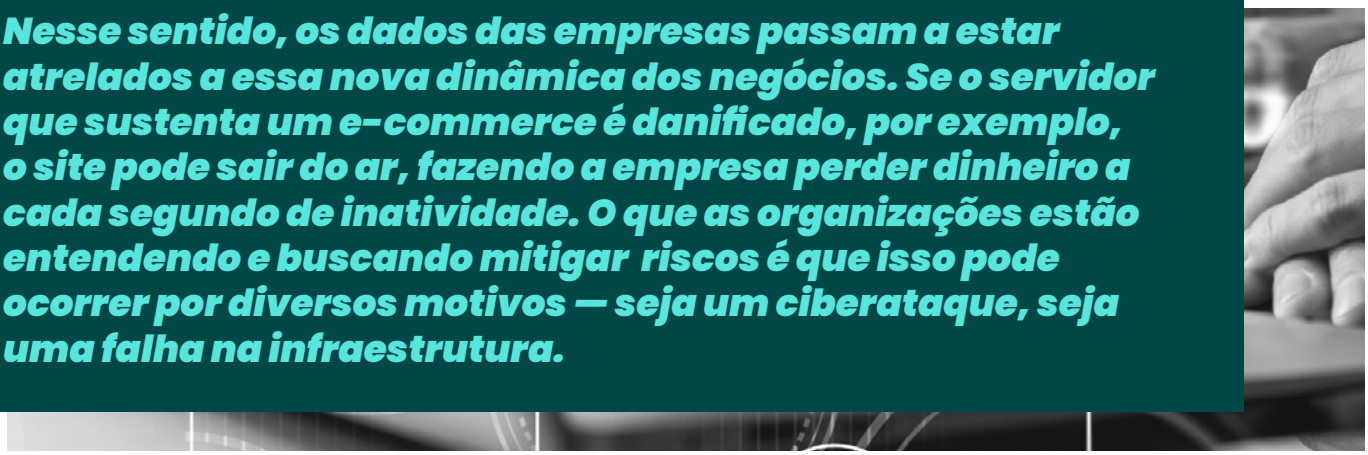
A segurança da informação nas empresas começa pela garantia de confiabilidade e confidencialidade dos dados, seja no ambiente físico, seja no digital.



COMPROMETIMENTO DA INTEGRIDADE

Com a digitalização dos negócios e o ambiente remoto se expandindo, o número de empresas que atuam 100% *online* está em constante crescimento. Mesmo setores historicamente baseados em atendimento e ambiente físico estão sendo forçados a migrar suas informações e dados para o cenário *online*.

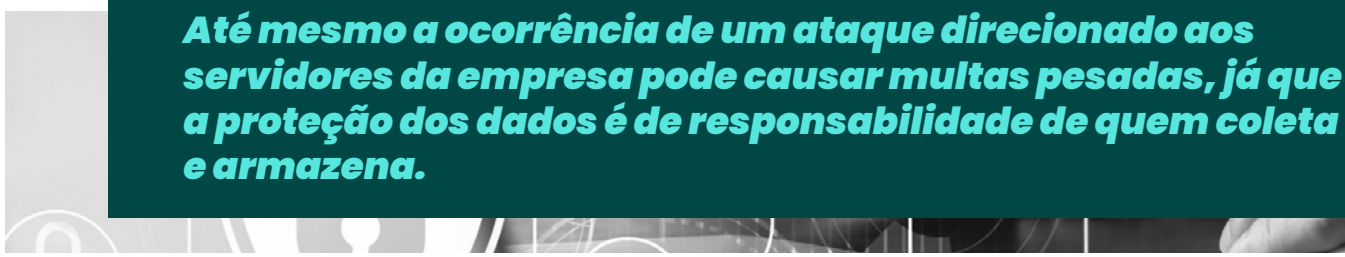
Nesse sentido, os dados das empresas passam a estar atrelados a essa nova dinâmica dos negócios. Se o servidor que sustenta um e-commerce é danificado, por exemplo, o site pode sair do ar, fazendo a empresa perder dinheiro a cada segundo de inatividade. O que as organizações estão entendendo e buscando mitigar riscos é que isso pode ocorrer por diversos motivos — seja um ciberataque, seja uma falha na infraestrutura.



RISCO DE INCONFORMIDADE

Um vazamento de dados pode ainda gerar um cenário de inconformidade jurídica. A Lei Geral de Proteção de Dados (LGPD) estabelece punições severas para quem não garantir a segurança das informações coletadas do consumidor. Por isso, toda empresa que registra dados de seus clientes deve garantir que eles não sejam repassados sem a autorização do titular.

Até mesmo a ocorrência de um ataque direcionado aos servidores da empresa pode causar multas pesadas, já que a proteção dos dados é de responsabilidade de quem coleta e armazena.

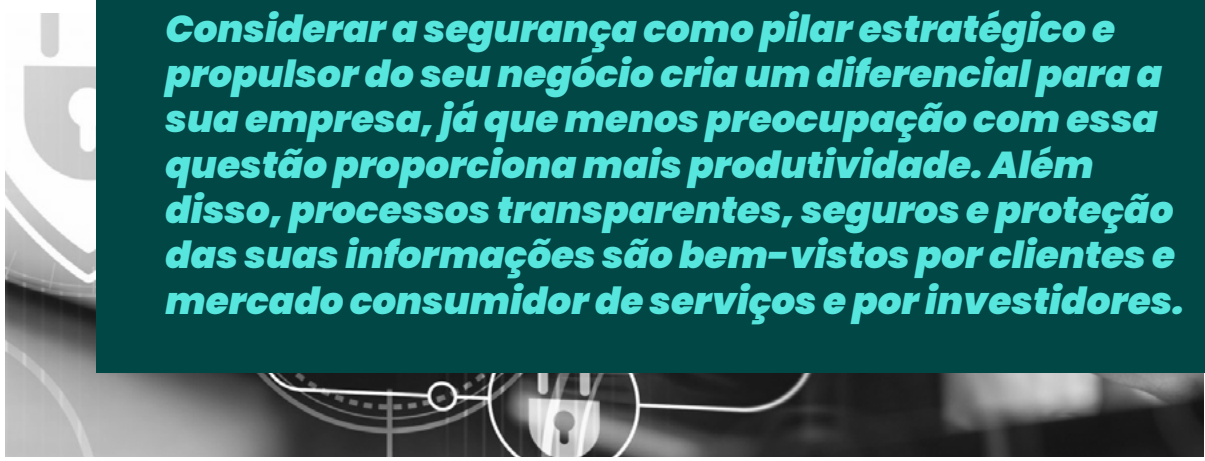


E o que podemos fazer para evitar que isso aconteça? Para começar, deve-se estabelecer uma política de segurança da informação nas empresas que considere os seus princípios básicos, sendo eles conformidade, disponibilidade, integridade, autenticidade, confidencialidade e irretratabilidade.

Tenha em mente que assunto não é de interesse apenas de grandes corporações. A LGPD é bem clara em relação à necessidade de adequação de todas as instituições (públicas e privadas) no território brasileiro.

DIFERENCIAL DE MERCADO

Considerar a segurança como pilar estratégico e propulsor do seu negócio cria um diferencial para a sua empresa, já que menos preocupação com essa questão proporciona mais produtividade. Além disso, processos transparentes, seguros e proteção das suas informações são bem-vistos por clientes e mercado consumidor de serviços e por investidores.



Nesse sentido, empresas que contam com profissionais especializados ou investem em parcerias estratégicas de confiança com vistas a assegurar o cumprimento de protocolos, boas práticas e assumem postura proativa tendem a se tornar mais resilientes – ou seja, caso venham a sofrer algum ataque, têm mais chances de se restabelecer com mais rapidez.

QUAL O PREÇO DO CIBERCRIME?

De acordo com previsões do Gartner e Julius Baer[3], a expectativa é que os gastos com cibersegurança cheguem a U$S 3 trilhões neste ano (2021). Somente no 1º semestre deste ano, o número de ataques cibernéticos a empresas brasileiras cresceu 220%, em comparação ao mesmo período em 2020 – tendo o *ransomware* (sequestro de dados) ocupado lugar de destaque como o ataque mais comum. Somente em junho, foram registrados 78,4 milhões de ataques em escala global, de acordo com relatório emitido pela SonicWall[4].

O setor de *banking* costumava ser alvo primordial dos cibercriminosos – de acordo com pesquisa realizada pela F5 Networks[5]. Entretanto, outros setores têm se tornado atrativos para os cibercriminosos. De acordo com pesquisa realizada pela IBM[6], em seu relatório global "Cost of a Data Breach Report", os três setores com o maior prejuízo advindos de um vazamento de dados são, em sequência: Saúde (U$S 7,13 MM), Energia (U$S 6,39 MM) e Financeiro (U$S 5,85 MM).

Vale ressaltar que com o advento da pandemia, o setor de saúde ganhou mais destaque e figurou nas mídias com sucessivos ataques a instituições que atuavam diretamente no combate à pandemia, como laboratórios e centros de pesquisas de desenvolvimento e distribuição de vacinas.

E por onde começar? Vejamos orientações para os setores com mais prejuízos:

SAÚDE

Adotar um modelo de segurança de confiança zero para criar sistemas e dados autodefensíveis, ao mesmo tempo em que dá suporte à conformidade com normas como a Lei Geral de Proteção de Dados (LGPD).

Documentar, comunicar e praticar um plano de resposta a incidentes em toda a empresa, incluindo participantes dos níveis de segurança, TI, jurídico, RH, relações públicas e diretoria.

ENERGIA

Adotar a análise de padrões de uso para avaliar a postura de segurança na IoT no setor (Internet das Coisas Industrial – IIoT).

Considerar a combinação da inteligência, monitoramento e operações de ameaças de segurança de TI e TO (Tecnologia Operacional).

FINANCEIRO

Minimizar a complexidade para proteger ambientes de TI e híbridos *multicloud* por meio da otimização de ferramentas e integrações de código aberto.

Impor controles rígidos de gerenciamento de identidade e acesso e aplicar os princípios de privilégio mínimo para dados e sistemas.

Essas recomendações certamente cabem em vários outros segmentos de mercado. Entretanto, antes de desenhar estratégias e propor investimento, é sempre importante considerar onde sua organização está em nível de maturidade de segurança – tanto em pessoas, processos e tecnologia, a tríade organizacional por onde a jornada de segurança da informação perpassa.

A importância da conscientização de segurança – a tão falada "*security awareness*"

É sabido que pessoas tendem a ser o elo "mais fraco" da cadeia de segurança cibernética. De acordo com pesquisa realizada pela IBM (2020)[7], o erro humano foi responsável por cerca de 95% das falhas de segurança. Corroborando com esta afirmação, temos o dado da CyberInc Insights[8] (2021), de que o erro humano tem 5 vezes mais probabilidade de causar uma violação do que outras fontes, como infraestrutura e desvios processuais, por exemplo.

A segurança da informação ainda não é uma pauta difundida nas escolas, desde o ensino fundamental. Não existe investimento em consciência de segurança do usuário como parte da educação básica, o que deveria ser primordial, considerando a massiva exposição de dados que ocorre hoje em dia, que pode ser perigosa e acarretar prejuízos para pessoas e organizações.

Os colaboradores são responsáveis por uma série de vulnerabilidades que ocorrem nas empresas, seja por estratégias mal implementadas, configurações erradas ou falta de atenção aos protocolos de segurança.

Segundo o Gartner,[9] apenas 16% dos novos contratados hoje possuem as habilidades necessárias para desempenharem suas funções atuais e futuras.

Diante disso, além de se atentar aos protocolos e investir em *softwares* e soluções de tecnologia de ponte, é urgente que as empresas invistam em treinamentos e aperfeiçoamento em relação às políticas de proteção de dados e segurança da corporação.

CONCLUSÃO

A crise instaurada pela pandemia, que impulsionou mudanças que estavam em curso na jornada de transformação digital das empresas, acendeu vários alertas no que tange ao âmbito da segurança cibernética. Com muitas organizações reformulando modalidades de trabalho para o ambiente remoto, os riscos inerentes as essas mudanças foram evidenciadas.

Realizar uma gestão segura *end-to-end*, que já era altamente desafiador em ambientes intra, tornou-se mais arriscado, pois agora o ambiente e a distribuição do negócio estão pulverizados.

As iniciativas tradicionais – testes de segurança, avaliações de riscos, avaliações de maturidade etc. – já não são mais suficientes. A segurança falha em um ponto crucial para avaliação de risco interno: o ponto de vista externo. Ciber criminosos ou *hackers* estão sempre procurando uma maneira de entrar e, para isso, se utilizam de vulnerabilidades externas detectáveis. Ou seja, olham de fora para dentro do ambiente. O "ponto de vista *hacker*" deve ser adotado, pois possibilita aos times de segurança reavaliarem as brechas expostas.

A medida que a exposição digital das organizações aumenta, cresce também a necessidade de se olhar com mais atenção os riscos, vulnerabilidades e possíveis ameaças. Muitas brechas de segurança são descobertas todos os dias possibilitando ataques criminosos, comprometendo a integridade de dados bem como a marca das organizações.

A maior efetividade da proteção do ambiente de TI está na centralização e na criação de processos e metodologias que garantam que as tecnologias estejam efetivamente protegendo os vários ativos (endpoints, redes, aplicações, nuvem etc.), que as ameaças sejam monitoradas em tempo integral (24x7x365) e os incidentes tratados de forma integrada e rápida.

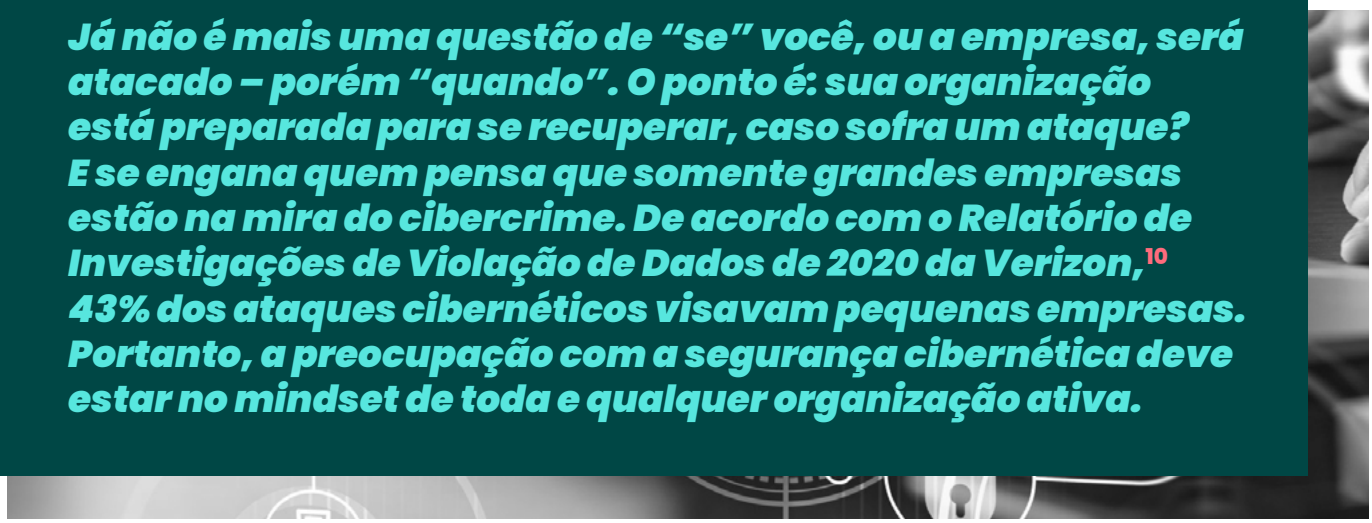
Um bom investimento é contar com um Security Operations Center (SOC) – uma solução focada em detecção e resposta a incidentes, que possibilita trabalhar a prevenção, identificação, o gerenciamento e a resolução de ameaças aos ambientes. É uma solução que conta com ferramentas como o SIEM (Correlacionador de Eventos) – que correlaciona *logs* de diversos *devices* e gera alarmes automáticos quando eventos suspeitos são detectados, além ferramentas de inteligência que monitoram redes abertas, *deep* e *dark web*.

Um SOC (Security Operations Center) é o único local capaz de monitorar e tratar em tempo real as questões de segurança da informação, de forma centralizada, dedicada e efetiva, pois em um SOC maduro, além de utilizar as melhores práticas descritas em diversos modelos de referência (NIST, ISO 27.001 etc), é lá que o CSIRT (Computer Security Incident Response Team) atua com prontidão para evitar que os incidentes gerem impactos negativos. É também lá que estão consolidados todo o conhecimento e técnicas (AI – Artificial Intelligence, SOAR – Security Orchestration

Automation and Response) para serem aplicados de forma inteligente para lidar com as ameaças.

Se sua organização está considerando evoluir sua resiliência cibernética, investir em um SOC é algo que deve estar no *roadmap* de avaliação.

Já não é mais uma questão de "se" você, ou a empresa, será atacado – porém "quando". O ponto é: sua organização está preparada para se recuperar, caso sofra um ataque? E se engana quem pensa que somente grandes empresas estão na mira do cibercrime. De acordo com o Relatório de Investigações de Violação de Dados de 2020 da Verizon,[10] 43% dos ataques cibernéticos visavam pequenas empresas. Portanto, a preocupação com a segurança cibernética deve estar no mindset de toda e qualquer organização ativa.



A estratégia é equilibrar a necessidade de proteger seus dados, ativos e ambientes com a necessidade de executar o negócio – ou seja, aumentar o seu nível de resiliência cibernética.

A boa notícia? A cibersegurança é o assunto do momento e, no mercado, existem ótimos *players* para te auxiliar nessa jornada de construção de resiliência cibernética.

Comece hoje! Considere a segurança como ponto de partida e balizadora de sucesso para sua estratégia e garanta a integridade do seu negócio.

Leidivino Natal

Leidivino Natal da Silva é CEO da Stefanini Rafael desde setembro de 2018. Possui ampla experiência em área de vendas para o mercado brasileiro e LATAM, tendo atuado em empresas multinacionais como Ericsson, Siemens e Vision-Box, auxiliando a alavancar negócios, adquirir novos clientes, ganhar mercado e mindshare por meio das atividades de marketing.

O executivo conta com grande conhecimento no mercado corporativo e de segurança da informação, atuando na definição de estratégia, posicionamento de mercado, gerenciamento de produtos, brand equity e equipes multifuncionais, priorizando o cumprimento de metas e o retorno sobre o Investimento (ROI) do negócio.

É formado em Engenharia Elétrica pela FEI (Faculdade de Engenharia de São Paulo) em 2002.

NOTAS E REFERÊNCIAS

1 Notícia: Brasil teve 3.2 bilhões de ataques online no 1º trimestre de 2021. https://www.tecmundo.com.br/seguranca/219734-brasil-teve-3-2-bilhoes-ataques-online-1-trimestre-2021.htm. Acesso em 14/09/2021

2 Gartner Top Security and Risk Trends for 2021

3 Investment Guide Outlook, Q3 2020: https://www.juliusbaer.com/fileadmin/content-hub/tendencias/investment-guide-outlook-q3-2020-es.pdf . Acesso em 14/09/2021

4 Notícia: Brasil é TOP 5 em ataques de ransomware e governo é o alvo dos Hackers.
Acesso pelo link: https://www.convergenciadigital.com.br/Seguranca/Brasil-e-top-5-em-ataques-ransomware-e-governo-e-o-alvo-dos-hackers-57672.html?UserActiveTemplate=mobile. Acesso em 14/09/2021

5 Notícia: Open Banking é principal alvo de ataque hacker no setor financeiro, diz pesquisa da F5: https://www.suno.com.br/noticias/open-banking-alvo-ataque-hacker-pesquisa/. Acesso em 14/09/2021

6 Cost of a Data Breach Report 2020; Ponemon Institute; 2020. Acesso pelo link: https://www.ibm.com/downloads/cas/QMXVZX6R. Acesso. Em 14/09/2021

7 Cost of a Data Breach Report 2020; Ponemon Institute; 2020. https://www.ibm.com/downloads/cas/QMXVZX6R. Acesso em 14/09/2021

8 Cyber Insights 2021. Cyberinc. https://cyberinc.com/thank-you-cyber-insights-report-2021/. Acesso em 14/09/2021

9 Press Release: Gartner Cautions HR and Recruiting Leaders that Only 16% of New Hires Have the Skills Needed Both for Their Current and Future Roles. https://www.gartner.com/en/newsroom/press-releases/2020-09-10-gartner-cautions-hr-and-recruiting-leaders-that-only-16-percent-of-new-hires-have-the-skills-needed-both-for-their-current-and-future-roles. Acesso em 14/09/2021

10 The 2020 Verizon Data Breach Investigations Report. https://www.cisecurity.org/wp-content/uploads/2020/07/The-2020-Verizon-Data-Breach-Investigations-Report-DBIR.pdf. Acesso em 14/09/2021

doi.org/10.52959/2021535407

COMO DEMOCRATIZAR O ACESSO DE MICRO E PEQUENAS EMPRESAS BRASILEIRAS A A RESILIÊNCIA CIBERNÉTICA?

Larissa de Freitas Querino e
Ricardo Gonzaga Martins de Araújo

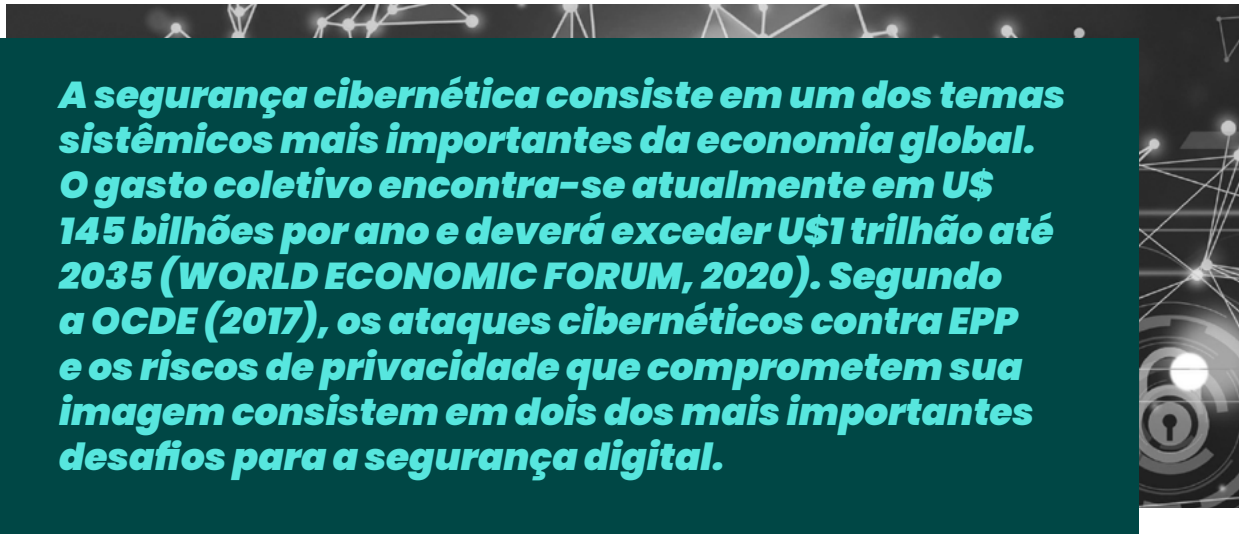
INTRODUÇÃO

O presente artigo procura discutir a importância da conscientização de micro e pequenas empresas acerca dos riscos cibernéticos e de privacidade para o setor produtivo, bem como as formas de democratização do acesso de microempresas (ME) e de empresas de pequeno porte (EPP) brasileiras a soluções – tecnológicas, de capacitação de recursos humanos e de gestão – que promovam o aumento da resiliência cibernética.

Conforme a OCDE (2017), ME e EPP são estruturas críticas para o crescimento econômico, uma vez que promovem competição e inovação, além de contribuir para a criação de empregos. Esses perfis de empresas enfrentam desafios distintos na gestão de segurança digital e de riscos de privacidade, que são prejudiciais para sua imagem. Por outro lado, as ME e EPP, conscientes do risco cibernético, podem demonstrar práticas robustas de gestão de segurança e privacidade digital e ter vantagens competitivas na busca de oportunidades de parcerias com organizações maiores.

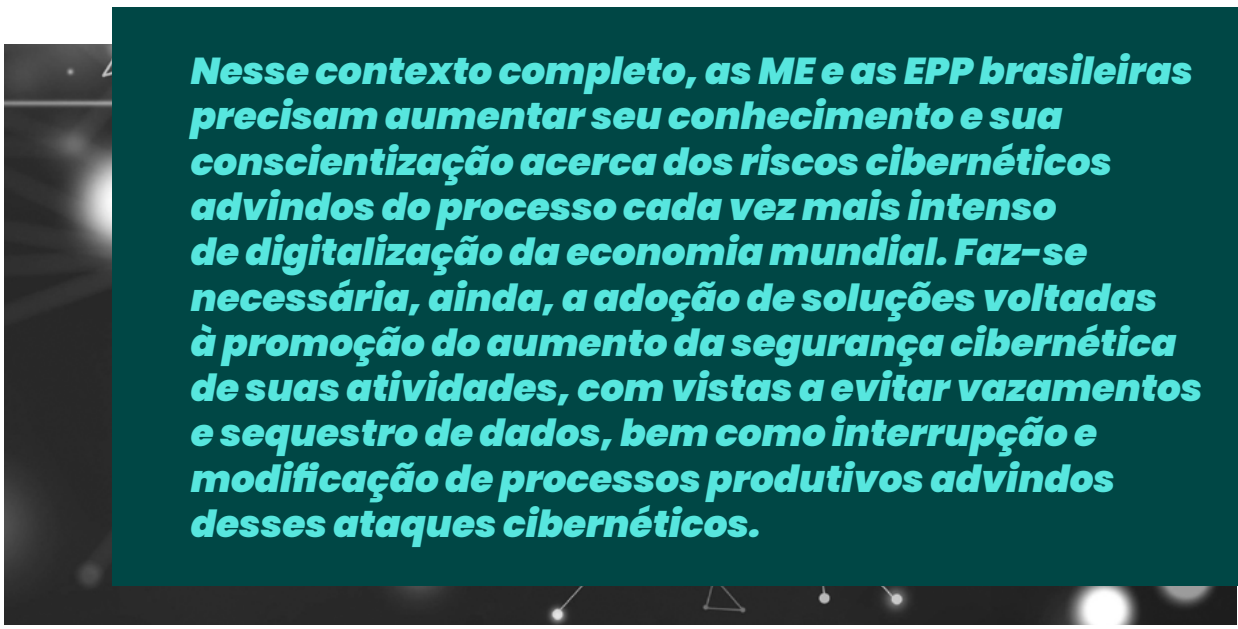
O processo de transformação digital da economia e da sociedade em nível mundial promove o aumento substantivo da utilização de redes interligadas de computadores e a transferência da gestão de processos produtivos para tais redes. Dessa forma, empresas, governos e cidadãos estão cada vez mais expostos a ataques em suas redes – caracterizados por sua sofisticação, especificidade e continuidade. Tais ataques impactam significativamente atividades sociais e econômicas.

Imagem: AdobeStock.com



A segurança cibernética consiste em um dos temas sistêmicos mais importantes da economia global. O gasto coletivo encontra-se atualmente em U$ 145 bilhões por ano e deverá exceder U$1 trilhão até 2035 (WORLD ECONOMIC FORUM, 2020). Segundo a OCDE (2017), os ataques cibernéticos contra EPP e os riscos de privacidade que comprometem sua imagem consistem em dois dos mais importantes desafios para a segurança digital.

Ademais, a Lei Geral de Proteção de Dados (Lei 13.709/2018), em vigor desde agosto de 2021, objetiva assegurar que os dados pessoais sejam tratados de forma a proteger a liberdade, a privacidade e o livre desenvolvimento das pessoas. Essa lei traz impactos significativos nas áreas jurídica, administrativa e de segurança da informação das organizações, uma vez que determina que empresas e órgãos públicos adaptem as formas de coletar, armazenar e utilizar os mencionados dados.



Nesse contexto completo, as ME e as EPP brasileiras precisam aumentar seu conhecimento e sua conscientização acerca dos riscos cibernéticos advindos do processo cada vez mais intenso de digitalização da economia mundial. Faz-se necessária, ainda, a adoção de soluções voltadas à promoção do aumento da segurança cibernética de suas atividades, com vistas a evitar vazamentos e sequestro de dados, bem como interrupção e modificação de processos produtivos advindos desses ataques cibernéticos.

A fim de contextualizar o presente artigo, tomaremos a seguir algumas definições ou compreensões acerca de conceitos a serem abordados, a saber, ataques cibernéticos e resiliência cibernética . Conforme a Accenture (2019), ataques cibernéticos consistem em atividades maliciosas conduzidas contra organizações, por meio de sua infraestrutura de Tecnologia da Informação, via redes internas, externas ou a internet. Incluem, ainda, ataques contra sistemas de controle industrial.

Já a resiliência cibernética pode ser entendida como a habilidade de sistemas cibernéticos de antecipar, de continuar a operar corretamente, de recuperar-se, de evoluir e de adaptar-se diante de ameaças cibernéticas (BODEAU et al, 2015). O termo remete à preparação e à adaptação às mudanças de condições, além das capacidades de resistência e de recuperação rápida diante de ataques cibernéticos. Dessa forma, pressupõem-se a manutenção de nível aceitável de serviço diante de várias falhas e desafios à operação normal (BODEAU et al, 2015).

Presso (2020)[1] define resiliência cibernética como

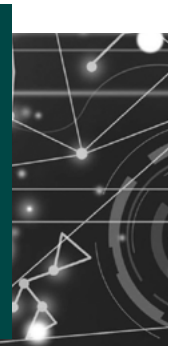
> *"um conjunto de métodos, práticas recomendadas e tecnologias que atenuam os riscos nos processos e fluxos de trabalho de negócios, a fim de proteger a organização. Devem abordar ameaças externas (hackers) e internas (funcionários mal-intencionados ou negligentes)".*

Essa resiliência nas empresas abrange o tripé tecnologia, pessoas e processos de governança, assim como define como lidar com um ataque, como manter os negócios operacionais durante a violação e a rapidez da evolução e do preparo para um eventual próximo incidente.

Portanto, o aumento da resiliência cibernética abrange fatores ligados à adoção de soluções de segurança da informação nas empresas, à qualificação constante de profissionais dedicados à segurança cibernética, à sensibilização e ao engajamento dos demais perfis profissionais da empresa, à adoção de processos de gestão interna para monitoramento de riscos e à definição de protocolo de respostas a incidentes.

Dessa forma, faz-se necessário despertar a consciência de pequenas empresas de todos os setores econômicos acerca dos riscos e dos potenciais impactos em seus negócios advindos de ataques cibernéticos que visam o roubo, o vazamento de dados e a interrupção de atividades.

É necessário também desenvolver a capacidade dessas empresas em lidar com os riscos dos ataques, por meio da democratização do acesso a soluções de prevenção, de detecção e de resposta a incidentes cibernéticos, assim como conscientizar sobre o uso ético e responsável de dados.



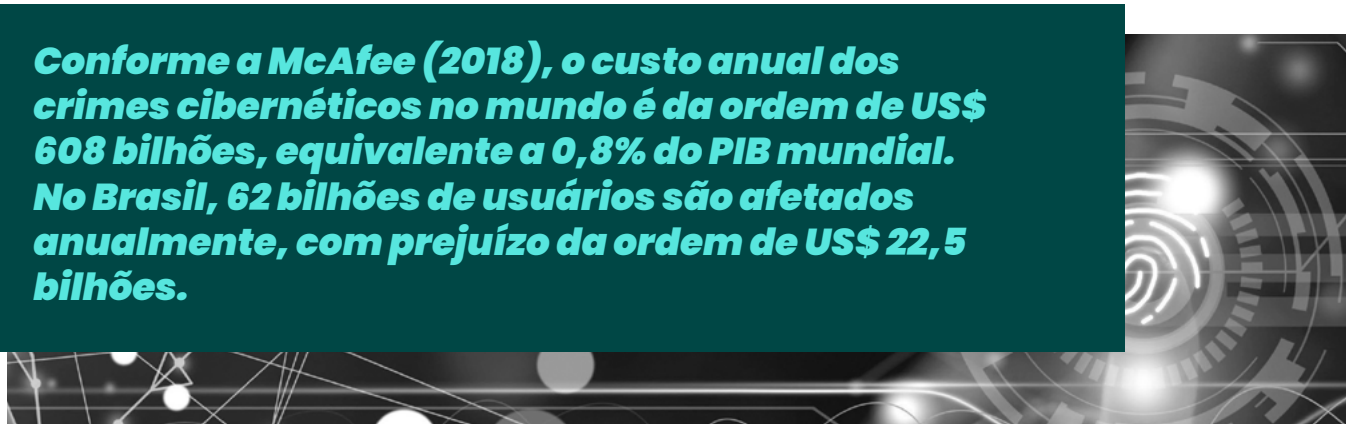
O CENÁRIO ATUAL DAS AMEAÇAS CIBERNÉTICAS NO BRASIL E NO MUNDO VERSUS A REALIDADE DAS PEQUENAS EMPRESAS

Segundo a OCDE (2017), os maiores desafios de segurança digital que afetam as atividades econômicas e digitais consistem em ataques cibernéticos contra pequenas empresas, que interrompem ou impedem atividades econômicas e sociais, bem como espionagem e crimes cibernéticos que envolvem o roubo de propriedade intelectual digital e de ativos.

Nos últimos anos, houve mudança real na escala e no escopo desses riscos cibernéticos, no que diz respeito à segurança digital e à privacidade. Tal situação impõe impactos significativos em atividades sociais e econômicas, uma vez que incidentes de segurança digital podem afetar a reputação, as finanças e os ativos intelectuais e físicos de uma empresa ou organização, pois podem gerar a queda de sua competitividade, de sua capacidade de inovar e de modificar sua posição no mercado (OCDE, 2017).

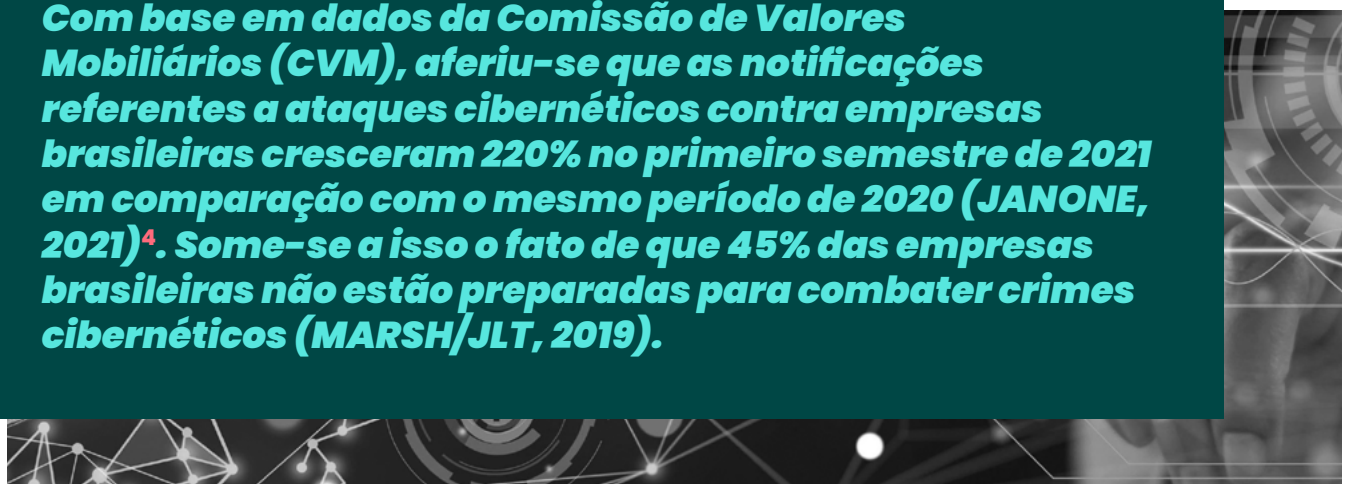
De acordo com a Kaspersky, somente em abril de 2020, o Brasil foi alvo de mais de 60% dos ataques identificados pela companhia na América Latina. Em seguida vem a Colômbia, com 11,9 milhões de ataques, o México (9,3 milhões), o Chile (4,3 milhões), o Peru (3,6 milhões) e a Argentina (2,6 milhões) (ROLFINI, 2020)[2].

Conforme a McAfee (2018), o custo anual dos crimes cibernéticos no mundo é da ordem de US$ 608 bilhões, equivalente a 0,8% do PIB mundial. No Brasil, 62 bilhões de usuários são afetados anualmente, com prejuízo da ordem de US$ 22,5 bilhões.



O relatório *Midyear Cybersecurity Roundup* também identificou aumento das ameaças cibernéticas no Brasil no primeiro semestre de 2020, em especial devido à pandemia de coronavírus. Durante o primeiro semestre de 2020, o Brasil foi o oitavo país que mais recebeu ameaças por e-mail com temas relacionados ao novo SARS-CoV-2. No total, foram 132 mil mensagens eletrônicas com arquivos maliciosos. Ademais, houve aumento do risco para as empresas devido a falhas de segurança criadas por uma força de trabalho em grande parte remota (TREND MICRO, 2020)[3].

Com base em dados da Comissão de Valores Mobiliários (CVM), aferiu-se que as notificações referentes a ataques cibernéticos contra empresas brasileiras cresceram 220% no primeiro semestre de 2021 em comparação com o mesmo período de 2020 (JANONE, 2021)[4]. Some-se a isso o fato de que 45% das empresas brasileiras não estão preparadas para combater crimes cibernéticos (MARSH/JLT, 2019).

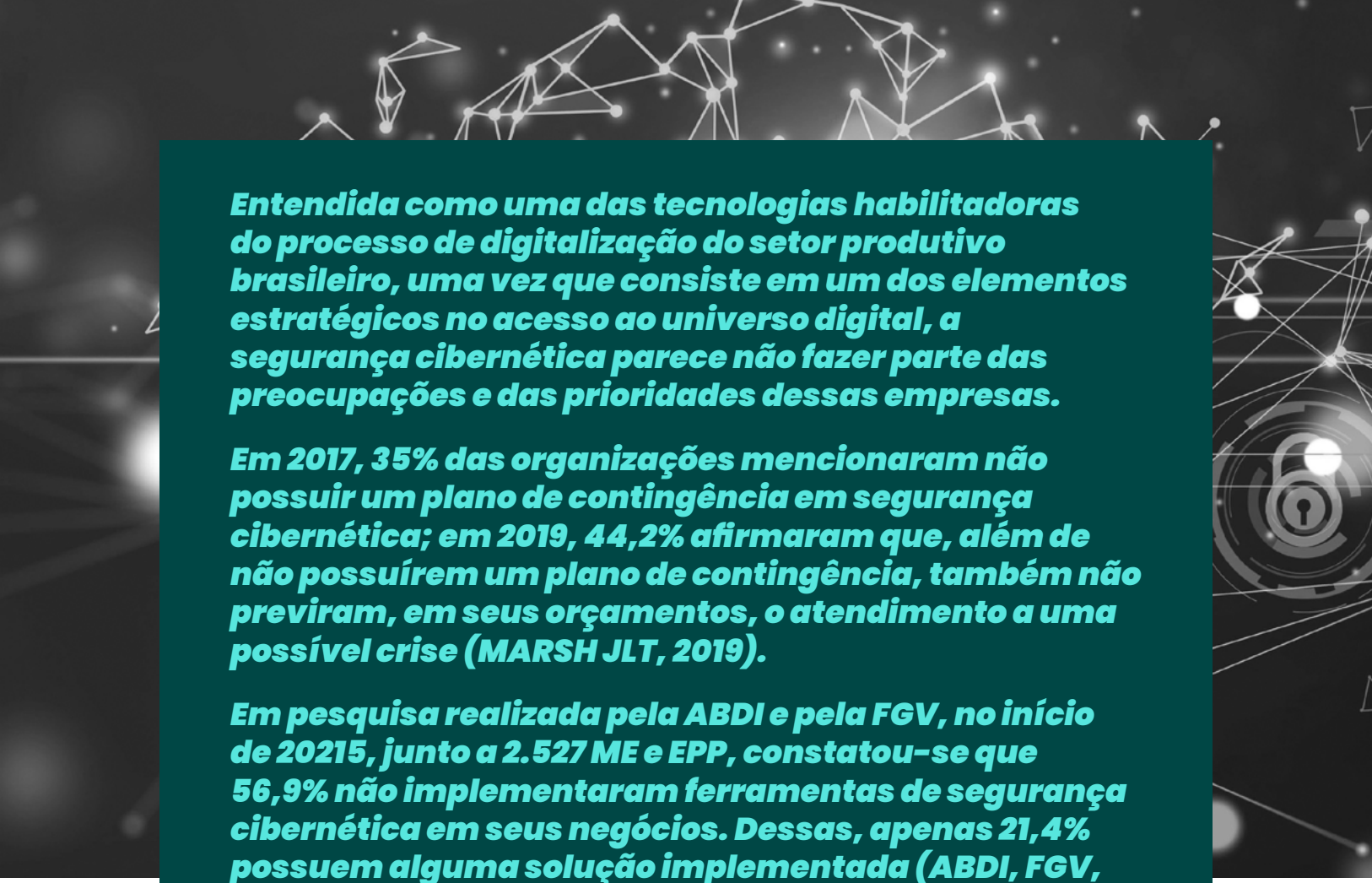


As quase cinco milhões de microempresas (ME) e empresas de pequeno porte (EPP) brasileiras correspondem a 98,5% do total de empresas privadas no Brasil, respondem por 27% do PIB e proporcionam 54% do total de empregos formais brasileiros (SEBRAE, 2018).

Mais de 45% das ME e das EPP concentram-se nas atividades de Comércio e mais de 33% atuam no setor de Serviços. As atividades do comércio varejista em que mais predominam mais as ME e EPP consistem em artigos de vestuário, produtos alimentícios, lanchonetes, restaurantes, acessórios para veículos automotores, materiais de construção, equipamentos de informática, produtos farmacêuticos e bebidas. Já as atividades de serviços concentram-se em transporte rodoviário e de cargas, contabilidade, escritório e apoio administrativo, manutenção e reparação mecânica de veículos, consultoria em gestão empresarial, atividade médica restrita a consultas, preparação de documentos e apoio administrativo, serviços de engenharia e cabeleireiro e manicure (SEBRAE, 2018).

No contexto atual de ameaças cibernéticas crescentes, a Estratégia Nacional de Segurança Cibernética – E-Ciber, aprovada pelo Decreto Nº 10.222/20 – pontua a importância de as organizações públicas e privadas estabelecerem políticas e procedimentos de segurança cibernética periodicamente revisados e de atenderem à evolução tecnológica, ao aperfeiçoamento de processos e à necessidade de capacitação contínua e estruturada para todos os colaboradores (GOVERNO FEDERAL, 2020).

No entanto, o cenário atual nas microempresas (ME) e nas empresas de pequeno porte (EPP) brasileiras parece não observar a realidade imposta pelos riscos cibernéticos, tampouco as recomendações da E-Ciber.



Entendida como uma das tecnologias habilitadoras do processo de digitalização do setor produtivo brasileiro, uma vez que consiste em um dos elementos estratégicos no acesso ao universo digital, a segurança cibernética parece não fazer parte das preocupações e das prioridades dessas empresas.

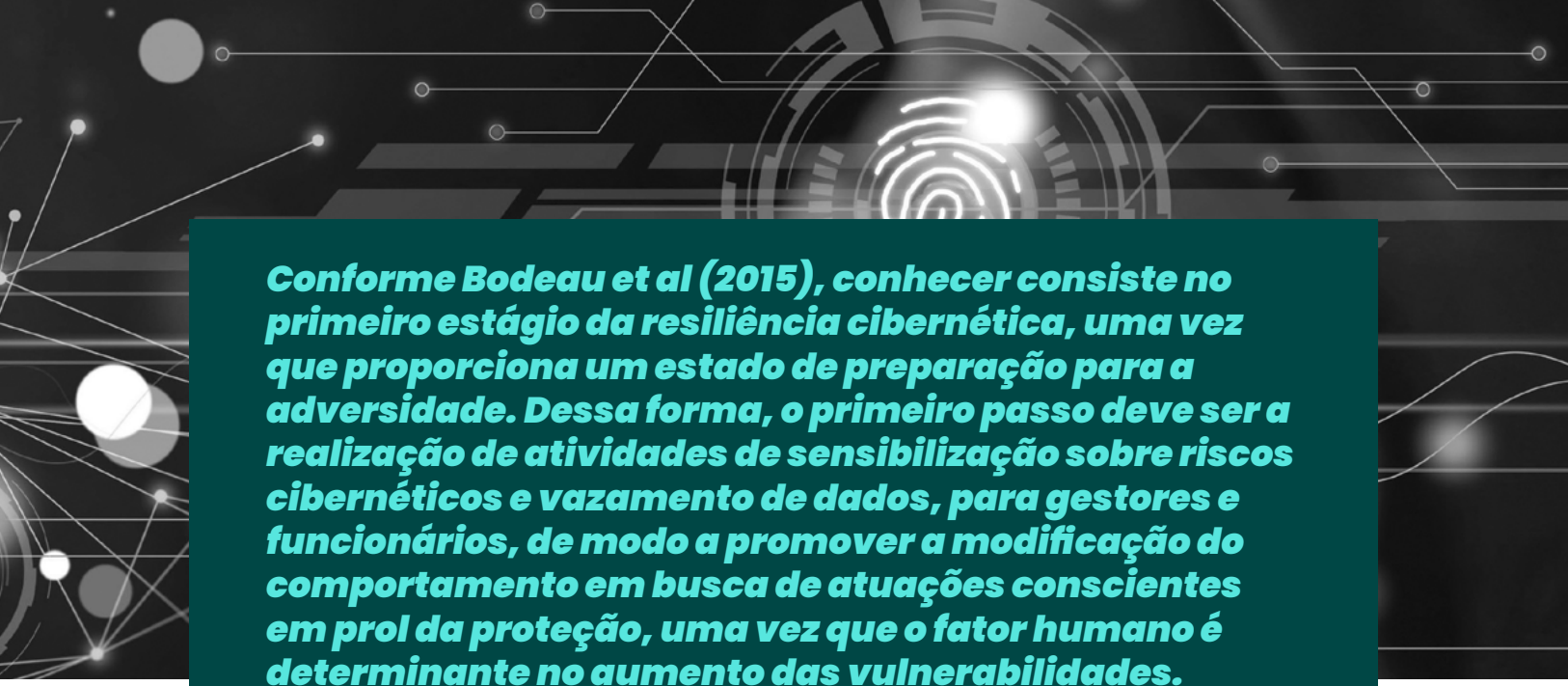
Em 2017, 35% das organizações mencionaram não possuir um plano de contingência em segurança cibernética; em 2019, 44,2% afirmaram que, além de não possuírem um plano de contingência, também não previram, em seus orçamentos, o atendimento a uma possível crise (MARSH JLT, 2019).

Em pesquisa realizada pela ABDI e pela FGV, no início de 20215, junto a 2.527 ME e EPP, constatou-se que 56,9% não implementaram ferramentas de segurança cibernética em seus negócios. Dessas, apenas 21,4% possuem alguma solução implementada (ABDI, FGV, 2021).

A DEMOCRATIZAÇÃO DO ACESSO A SOLUÇÕES VOLTADAS PARA O AUMENTO DA RESILIÊNCIA CIBERNÉTICA DE PEQUENAS EMPRESAS BRASILEIRAS

As prioridades de ME e EPP no Brasil encontram-se voltadas para a adoção de boas práticas digitais com foco em captação, engajamento e conexão de clientes, com menor interesse na adoção de soluções de segurança cibernética nos negócios. Essa negligência na adoção de medidas de segurança da informação adequadas em suas prioridades de negócios traz como consequência uma maior fragilidade frente a ataques cibernéticos.

Com vistas a reduzir essa fragilidade, a questão relevante consiste em como democratizar o acesso e a utilização de soluções cibernéticas para o aumento da resiliência nos pequenos negócios.

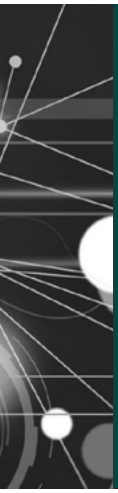


Conforme Bodeau et al (2015), conhecer consiste no primeiro estágio da resiliência cibernética, uma vez que proporciona um estado de preparação para a adversidade. Dessa forma, o primeiro passo deve ser a realização de atividades de sensibilização sobre riscos cibernéticos e vazamento de dados, para gestores e funcionários, de modo a promover a modificação do comportamento em busca de atuações conscientes em prol da proteção, uma vez que o fator humano é determinante no aumento das vulnerabilidades.

A conscientização sobre riscos cibernéticos e o entendimento claro sobre as necessidades digitais da empresa tornam-se indispensáveis para o aumento de sua capacidade de promover a proteção de suas operações, mesmo para empresas de pequeno porte, pois podem mitigar certos riscos de ataques cibernéticos, despertar para necessidade de intervenções de segurança cibernética e promover real aumento de resiliência cibernética.

De maneira prática, o conhecimento e a adoção de comportamentos simples podem mitigar significativamente os riscos cibernéticos de ME e EPP, a saber:

- Cuidados com a segurança da senha;
- Uso de Token;
- Cuidados com e-mails suspeitos/falsos;
- Instalação de barreiras tipo antivírus e *firewall*;
- Definição de regras de sites proibidos e habilitados;
- Autenticação (controle de acesso) baseada em 2 fatores;
- Atualização automática de sistema operacional e outros softwares;
- Cuidado com downloads de arquivos e programas;
- Cuidado com acesso a links recebidos em mídias sociais e e-mails;
- Estabelecimento de procedimentos e condutas para os funcionários;
- Gerenciamento de identidade e acesso de usuários.



Já as ações de resistência e de recuperação de ataques cibernéticos requerem maiores investimentos, tanto técnicos quanto financeiros. Faz-se necessária a oferta de consultorias que avaliem o patamar de digitalização da empresa, analisem sua realidade, realizem a gestão do risco cibernético e a identificação das vulnerabilidades do negócio, promovam o acesso e a adoção de ferramentas de segurança cibernética adequadas e específicas para a necessidade da empresa.

A demonstração dos prejuízos em situação de ataque, a compreensão clara das principais ameaças a sistemas operacionais, o conhecimento sobre os tipos e as formas de ataque mais frequentes, a adoção das tecnologias adequadas, o planejamento para mitigação de ameaças e a criptografia de dados são parte de estrutura de aumento de resiliência cibernética para a promoção da continuidade de realização das funções essenciais da organização e de seus negócios, apesar das adversidades resultantes de ataques cibernéticos.

Ademais, estratégias para a promoção da segurança cibernética nos negócios podem ser estimuladas pelo governo junto ao setor produtivo, conforme preconizado pela OCDE (2017) e pela Estratégia Nacional de Segurança Cibernética (BRASIL, 2018). Apresentam-se, a seguir, algumas dessas estratégias:

- ***Capacitação e desenvolvimento de habilidades profissionais, por meio da ampliação de cursos técnicos e acadêmicos sobre o tema.***
- ***Estímulo ao desenvolvimento de projetos de pesquisa e desenvolvimento voltados às necessidades de segurança do setor produtivo.***
- ***Promoção de incentivos fiscais para empresas que invistam em segurança da informação.***
- ***Definição de critérios técnicos mínimos de segurança cibernética a serem adotados por empresas e organizações que façam negócios com o governo.***
- ***Estímulo à criação de startups na área de segurança cibernética.***

CONCLUSÃO

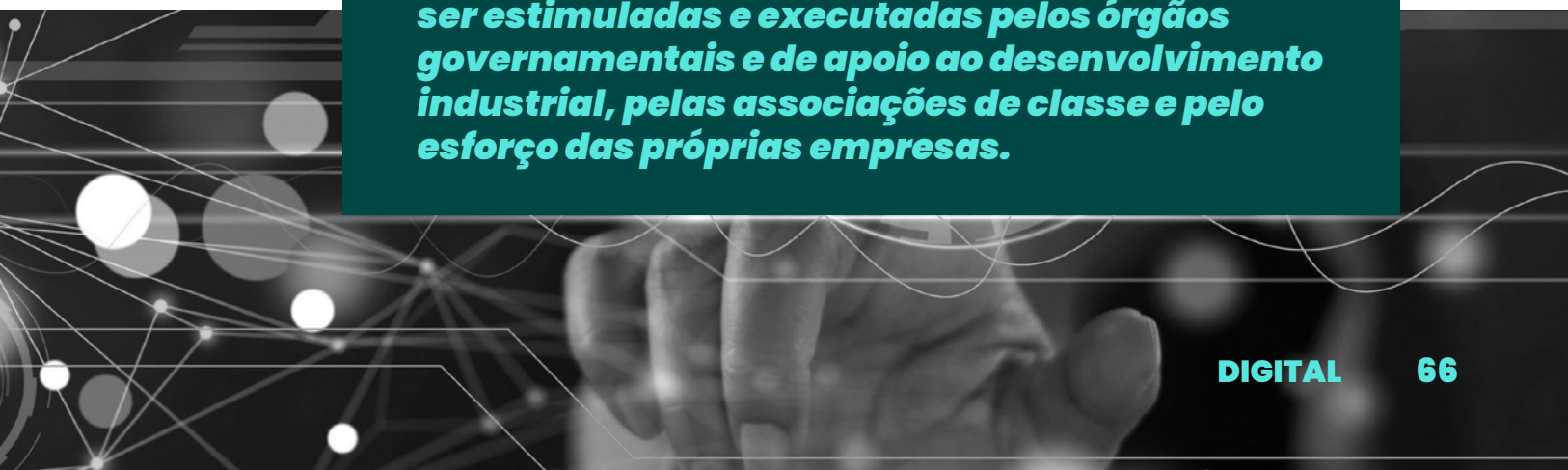
O aumento da velocidade do processo de digitalização da economia brasileira demanda a criação de ambiente propício para o aumento da maturidade digital do setor produtivo, por meio da remoção das barreiras externas que dificultam a adoção de tecnologias digitais pelas empresas. Nesse contexto, a promoção da segurança cibernética e da proteção de dados assumem papel fundamental no processo de tornar as empresas brasileiras mais digitais e, por consequência, mais produtivas.

É fato que, em um contexto de transformação digital da economia cada vez mais crescente, o setor produtivo estará cada vez mais vulnerável a ataques em suas redes, devido à aceleração da transição do modelo dos negócios, de analógico para digital. À medida que aumenta a digitalização dos processos produtivos, aumentam os riscos e a necessidade de implantar nas empresas, não importa o seu tamanho, soluções de segurança da informação, de forma a possibilitar o aumento de sua resiliência cibernética.

Adiciona-se a esse contexto a entrada em vigor da Lei de Proteção Geral de Dados – LPGD, que passou a exigir que empresas conectadas à internet promovam ações de prevenção e de contenção de ataques e de vazamento de dados. No entanto, a grande maioria das empresas brasileiras ainda não está sensibilizada e tampouco preparada para tal desafio.

Nesse contexto, tornam-se necessários esforços reais de democratização do acesso a soluções voltadas para o aumento da resiliência cibernética de ME e EPP brasileiras, com vistas a promover a conscientização e a adoção de estratégias de segurança para preparar empresas e aumentar sua confiança frente a potenciais ataques perpetrados via as infraestruturas de Tecnologia da Informação, de modo a reduzir suas vulnerabilidades.

Tais soluções devem concentrar-se no tripé necessário à redução dos impactos de ataques cibernéticos, a saber: de ordem tecnológica, de capacitação de recursos humanos e de gestão de pessoas e processos na empresa. E devem ser estimuladas e executadas pelos órgãos governamentais e de apoio ao desenvolvimento industrial, pelas associações de classe e pelo esforço das próprias empresas.



Atividades de conscientização e sensibilização sobre riscos cibernéticos para gestores e funcionários das pequenas empresas, oferta de consultorias que analisem a realidade da empresa e promovam o acesso e a implementação de ferramentas de segurança cibernética que modifiquem o comportamento dos funcionários, a sua capacitação na implementação de ferramentas de segurança cibernética são ações que devem ser adotadas de forma a se propagarem por todo o tecido econômico brasileiro.

A conscientização sobre riscos cibernéticos e o entendimento claro sobre as necessidades digitais da empresa tornam-se indispensáveis para o aumento na capacidade de promover a proteção das operações para as ME e as EPP. Nesse contexto, democratizar e promover o acesso e a utilização de soluções cibernéticas para o aumento da resiliência em seus negócios passam a ter um caráter primordial.

Com esse objetivo, a ABDI ampliará suas atividades voltadas para a capacitação de recursos humanos especializados em segurança cibernética, sensibilização a respeito de riscos cibernéticos e adoção de soluções tecnológicas em pequenos negócios.

A *Cyber Arena* promoverá, a partir de 2022, sensibilizações, para o público em geral, e capacitações para profissionais de TI, com a utilização de simulador hiper-realista de ataque e defesa cibernéticos, que consiste em ambiente virtualizado para treinamento, experimentação, avaliação de vulnerabilidades, trabalho em grupo, feedback em tempo real, experiências *on the job*, teste de novas ideias e solução de problemas cibernéticos, onde ataques cibernéticos são realizados em réplica de ambiente real de operação de uma organização, de maneira segura, controlada e confiável.

Já o *Cyber Solutions* promoverá, por meio de consultorias especializadas e individualizadas, a avaliação da maturidade cibernética de empresas brasileiras, bem como o acesso e a adoção de soluções tecnológicas em segurança cibernética, com vistas à mitigação de riscos e de vulnerabilidades.

A ABDI proporá, ainda, o desenvolvimento de modelagem de alto nível para a aferição e análise de Índice de Resiliência Cibernética (IRCiber) para o setor produtivo. O objetivo consiste em medir a evolução e o aumento dessa resiliência ao longo do tempo, além de incorporar a gestão de riscos cibernéticos.

Larissa de Freitas Querino

Larissa de Freitas Querino é Mestre em Economia com habilitação em Economia da Defesa pela Universidade de Brasília. É bacharel em Relações Internacionais pela Universidade de Brasília, possui Maestría em Desenvolvimento Econômico pela Universidade Internacional de Andalucía, na Espanha e MBA em Gestão de Comércio Exterior e Negócios Internacionais pela Fundação Getúlio Vargas. É a especialista em Indústria de Defesa da Agência Brasileia de Desenvolvimento Industrial (ABDI) desde 2011, onde realiza atividades de estruturação, negociação e implementação de projetos e agendas de trabalho no setor de Defesa, junto a parceiros dos setores público e privado. Coordenou, dentre outras publicações sobre o tema na ABDI, os trabalhos para o desenvolvimento e a publicação do Mapeamento da Base Industrial de Defesa (2016). Atualmente lidera os projetos de Segurança Cibernética e do Uniforme Inteligente.

Ricardo Gonzaga Martins de Araújo

Profissional com mestrado Strictu-senso em Gestão de Pessoas – FEAD, Pós graduado em Finanças Empresariais – Fundação Getúlio Vargas, Pós graduado em Engenharia Econômica – FDC, Pós graduado em Engenharia da Qualidade – IETEC/MG, Graduado em Engenharia Eletrônica e de Telecomunicação – PUC/MG. Com mais de 35 anos de atuação nas áreas industrial, administrativa, financeira, contábil, tendo sido responsável por uma planta industrial e proprietário de microempresa, Ricardo tem experiência em articulação público-privado na Agência Brasileira de Desenvolvimento Industrial - ABDI para formulação e aplicação de políticas públicas.

Imagem: AdobeStock.com

NOTAS

1 Disponível em https://balipodo.com.br/o-que-e-resiliencia-cibernetica-blogs-do-opentext/. Acesso em 17 de agosto de 2021.

2 Disponível em https://olhardigital.com.br/2020/07/03/seguranca/cibercrime-ataques-no-brasil-aumentam-mais-de-300-com-a-pandemia/. Acesso em 11 de setembro de 2020.

3 Disponível em https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/securing-the-pandemic-disrupted-workplace-trend-micro-2020-midyear-cybersecurity-report. Acesso em 11 de setembro de 2020.

4 Disponível em https://www.cnnbrasil.com.br/business/2021/07/22/ataques-ciberneticos-a-empresas-brasileiras-crescem-220-no-1-semestre-de-2021. Acesso em 17 de agosto de 2021.

5 ABDI, FGV. Mapa da Digitalização das MPEs Brasileiras – Resumo Executivo. Brasília, junho de 2021.

REFERÊNCIAS

ABDI, FGV. Mapa da digitalização das MPEs brasileiras – Resumo Executivo. Brasília, junho de 2021.

ACCENTURY SECURITY. Ninth Annual Cost of Cybercrime Study. Unlocking the Value of Improved Cybersecurity Protection. Accenture, 2019

BODEAU, Deborah et al. Cyber Resiliency Engineering Aid – The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques. The MITRE Corporation Bedford, MA: 2015.

BRASIL. Presidência da República. Decreto nº 10.222, de 05 de fevereiro de 2020. Estratégia Nacional de Segurança Cibernética.

BRASIL. Presidência da República. Lei 13.709/2018 - Lei Geral de Proteção de Dados (LGPD), de 14 de agosto de 2018.

JANONE, Lucas. Ataques cibernéticos a empresas brasileiras crescem 220% no 1º semestre de 2021. CNN Brasil. Disponível em https://www.cnnbrasil.com.br/business/2021/07/22/ataques-ciberneticos-a-empresas-brasileiras-crescem-220-no-1-semestre-de-2021. Acesso em: 17 agosto de 2021.

MCAFEE. Economic Impact of Cybercrime – No Slowing Down. Santa Clara: McAfee, 2018

MARSH JLT. Cyber View 2019: identificando oportunidades no mercado brasileiro. São Paulo: MARSH JLT, 2019.

OECD. Digital Economy Outlook 2017, Paris: OECD Publishing, 2017.

PRESSO, Luiz. O Que É Resiliência Cibernética? Balipodo. Disponível em https://balipodo.com.br/o-que-e-resiliencia-cibernetica-blogs-do-opentext/. Acesso em: 17 de agosto de 2021.

ROLFINI, Fabiana. Cibercrime: Ataques no Brasil Aumentam mais de 300% com a Pandemia. Olhar Digital. Disponível em https://olhardigital.com.br/2020/07/03/seguranca/cibercrime-ataques-no-brasil-aumentam-mais-de-300-com-a-pandemia/. Acesso em: 11 set. 2020.

TREND MICRO. Securing the Pandemic-Disrupted Workplace. Midyear Cybersecurity Report 2020. Disponível em https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/securing-the-pandemic-disrupted-workplace-trend-micro-2020-midyear-cybersecurity-report. Acesso em: 11 set. 2020.

WEF. Future Series: Cybersecurity, emerging technology and systemic risk. Insight Report, Novembro, 2020.

doi.org/10.52959/2021535408

A EXPERIÊNCIA DO BANCO CENTRAL DO BRASIL: COMO LIDAR COM OS DESAFIOS DE ESTIMULAR A INOVAÇÃO E A SEGURANÇA NAS OPERAÇÕES FINANCEIRAS DIGITAIS?

ENTREVISTA DE OTÁVIO DAMASO, DIRETOR DE REGULAÇÃO DO BANCO CENTRAL, A KRISHMA CARREIRA, DA FSB


Imagem: AdobeStock.com

Krishma Carreira: Como responsável pela área de regulação e normas no Banco Central do Brasil, qual é a sua visão sobre inovação e regulação?

Otávio Damaso: O primeiro aspecto que a gente tem que reconhecer é que o sistema financeiro nacional sempre foi um dos principais segmentos da economia brasileira que investiu em inovação. Se olharmos o histórico do sistema financeiro, sempre houve muito investimento. Salvo engano, hoje é o setor econômico que mais investe em tecnologia. E, naturalmente, o BACEN sempre acompanhou o processo de regulação olhando esse aspecto também. A gente sempre apoiou a inovação no âmbito do sistema financeiro. O que diferencia, no meu ponto de vista, o que foi no passado do que tem acontecido atualmente, é o próprio advento das tecnologias que foram implementadas pelo sistema financeiro, a entrada de novos atores, principalmente as instituições de pagamento. Eu acho que também tem uma própria postura do BACEN em não só aceitar a inovação que estava vindo naturalmente do sistema financeiro, mas também de fomentá-la. Foi entre 2013 e 2014 que a gente começou a dar uma mudada na forma de encarar o processo de inovação.

Olhando pelo aspecto da regulação, eu diria duas coisas: tem a regulação bancária e a prudencial. A regulação bancária visa, entre outros aspectos, a tornar o sistema financeiro cada vez mais eficiente em todas as suas dimensões. Eficiente em termos de favorecer a inclusão de novos participantes e também a entrada de novos *players* no mercado. Então, eu diria que gente fez a lei e, depois, a regulação das instituições de pagamento, quando veio o advento das *fintechs*. Fomos muito proativos na criação das *fintechs* de crédito nas duas modalidades que existiam. E por aí vão vários outros movimentos que nós fizemos para endereçar nichos de participantes novos que estavam surgindo e a gente precisava fomentar a entrada deles aqui.

Trabalhamos bastante na regulação de produtos e o curioso desse aspecto é que a gente fez várias coisas, mas tem uma que é relativamente pequena e pontual e, muitas vezes, esquecida por todos, mas que do meu ponto de vista talvez tenha sido uma das mais importantes, que foi quando permitimos que as instituições financeiras abrissem contas por meio remoto. Fazendo uma retrospectiva, logo após o Plano Real, várias instituições do varejo mundialmente conhecidas vieram ao Brasil e se instalaram aqui, buscando oportunidades. Mas passaram alguns anos e várias delas desistiram do país. Por quê? Porque existia uma grande barreira à entrada no sistema financeiro, que era a escala física. Era preciso ter agências no maior número de municípios e um maior número de agências também dentro de um mesmo município. Escalar isso era muito difícil no caso brasileiro!

Essa barreira de entrada foi rompida com a abertura de conta digital. Hoje, nós temos, no âmbito do sistema financeiro, bancos, *fintechs* ou *e-pays*, instituições de pagamento, que sequer têm uma agência física, mas muitos delas já têm correntistas em muitos dos municípios brasileiros. Isso era impensável. E isso foi um importante *driver* na parte de competição. Por isso, considero esse normativo muito importante para favorecer o que nós temos hoje, que é o sistema financeiro com a participação de novos *players*.

Na parte bancária a gente olha eficiência, inclusão, aperfeiçoamento de produtos, o que está acontecendo de mais moderno em tecnologia e em nenhum momento nós deixamos de cuidar das questões prudenciais. Então, sempre olhamos com muita atenção para isso. Todas as instituições financeiras e instituições de pagamentos estão sujeitas a requerimentos prudenciais, só que nós adotamos também, no Brasil, o que chamamos de regulação proporcional. Ela é proporcional ao porte e ao risco que a instituição financeira impõe ou representa para o sistema financeiro. Até as instituições menores, que no conjunto não representam parcela significativa, mas que são inúmeras, já têm uma regulação prudencial muito mais simples, porém 100% compatível com o risco que elas representam para o sistema financeiro.

KC: Quais são as principais fontes de inovação para vocês?

OD: Eu diria que todas as instituições financeiras, independentemente do porte, olham para tecnologia e para potenciais inovações. Todas elas apostam muito nesse caminho. Então, é difícil eu falar que as *fintechs* têm uma pegada de inovação maior do que os bancos incumbentes. Eu acho que, hoje, no sistema financeiro, todo mundo olha isso como uma oportunidade de gerar novos negócios e de aumentar produtividade.

De nossa parte, estamos plenamente integrados junto aos fóruns internacionais de instituições financeiras. A gente olha muito o que está acontecendo lá fora. E, em muitos casos, somos referência no que está acontecendo lá fora. Eu diria que dois de nossos principais projetos, o *Open Banking* e o próprio PIX, são *benchmarkings* para o mundo. O *Open Banking*, pelo seu escopo e abrangência, e o PIX, pela eficiência que traz para o sistema financeiro. Eu desconheço um sistema de pagamento tão eficiente como o PIX, mas isso é também fruto de a gente conhecer o que está acontecendo lá fora, em todos

os países, analisar o que tem de bom e de ruim em cada projeto. Na questão do PIX, olhamos para Suécia, China, para outros países que estavam adotando pagamentos instantâneos e vimos o que tinha de aspectos positivos e negativos e sobre como a gente poderia adaptar para o Brasil.

A mesma coisa no *Open Banking*. Olhamos para o modelo europeu, para o inglês e para várias experiências na Ásia e na Oceania. Eu acho que esse é o caminho que a gente tem seguido e o que a gente vê as instituições financeiras seguindo também.

KC: O senhor já falou um pouco, mas qual é o peso efetivo das tecnologias e dos negócios digitais?

OD: Primeiro, foi superimportante, na fase anterior à pandemia, incentivar as instituições financeiras a adotarem inovações. Imagina se a gente tivesse essa pandemia 20 anos atrás? O que seria da nossa vida sem todo o aparato digital que propiciou que a gente suavizasse os impactos da pandemia no nosso dia a dia? O sistema financeiro foi uma solução, ajudou nesse processo. E aí, quando veio a pandemia, naturalmente, toda essa parte de inovação de digital, de remoto, cresceu muito. É curioso que tínhamos projetos na prancheta que estavam planejados para serem implementados em dois, três, quatro, cinco anos. Alguns tiveram que ser implementados em um, dois, três meses. E da mesma forma que fizemos com uma velocidade muito grande, o mesmo ocorreu com as instituições financeiras; e a tecnologia respondeu bem.

KC: O mercado financeiro tem uma grande concentração. Como o senhor tem visto isso e o que tem sido feito para atrair novos players?

OD: O sistema financeiro brasileiro não é diferente em termos de composição de outros países com o mesmo porte do Brasil. Quando a gente olha para os nossos pares, como Canadá, Austrália, que são sempre países de referência para nós, e mesmo alguns mais avançados, como França, Espanha e Inglaterra, o número de instituições sistemicamente importantes é em torno de quatro ou cinco e você tem depois bancos médios, pequenos, financeiros, *fintechs*. O que distoa um pouco é os EUA, que, mesmo assim, se você for contar, os grandes bancos americanos não são tantos que destoem muito do mercado brasileiro. Mas dito isso, o que a gente viu recentemente foi o incremento de novos participantes entrando no mercado financeiro, por um lado motivado pelo BACEN, por outro lado, identificando oportunidades de negócio. Essas oportunidades de negócio, algumas vezes, eram para contestar produtos e serviços financeiros oferecidos pelos próprios bancos incumbentes e, por outras vezes, para preencher *gaps*. *Gaps* que a gente reconhecia que existiam no nosso mercado, como financiamento de uma parcela da população que não estava incluída, de micro e pequenas empresas, de alguns segmentos econômicos ou mesmo de algumas regiões do nosso país.

KC: O senhor poderia falar sobre os programas de estímulo à inovação?

OD: Eu acho que a própria agenda do BACEN é cheia de estímulos à inovação. Quando a gente fala de PIX, *Open Banking*, isso é estímulo à inovação. Quando a gente fala de *SandBox*[1] é estímulo à inovação. E aí, inovação é tanto sobre absorção de tecnologia quanto inovação em termos de produtos e modelos de negócios também. É importante ter isso em mente. Muitas vezes, a gente olha para um processo que é inovador porque está fazendo de uma forma diferente ou está entrando em um campo que antes não era explorado, mas não está necessariamente fazendo isso de forma intensiva em tecnologia ou mesmo com alguma tecnologia de ponta inovadora. Só que está inovando na forma de relacionamento com o cliente ou no modelo de negócios que ele está implementando.

Nós também temos o Laboratório de Inovação Financeiras e Tecnológicas (LIFT[2]), que é uma iniciativa conjunta do Banco Central e da Fenasbac para fomentar a inovação no Sistema Financeiro Nacional com o incentivo à criação de protótipos de soluções tecnológicas. Ele é focado em empresas e ou pessoas que trazem novas ideias de empreendedorismo para o mercado.

Acho que a demanda da sociedade é outra fonte de inovação importante. Hoje, o cidadão brasileiro é muito aberto a esses processos digitais. Ele demanda eficiência, praticidade, conveniência e relacionamento. Muitos dizem que o próprio contato físico entre o cliente e o banco era um negócio complexo. Às vezes, entrar para pedir crédito envolvia um certo constrangimento, existia uma barreira natural do ser humano. Com a tecnologia isso ficou muito mais fácil e mais mecânico do que antes. A população demanda isso. E ela demanda também soluções financeiras no momento e no local onde ela está e não soluções financeiras que ela precisa se deslocar para uma agência que, às vezes, fica distante da residência dela.

E outra fonte de inovação é a própria chegada de várias tecnologias. O mobile é uma fonte de inovação. Essa capacidade que a gente tem hoje no nosso celular foi uma fonte de inovação, porque agora, dentro dele, você consegue desenvolver vários aplicativos com uma velocidade e capacidade de processamento imensa, mas também com segurança. Blockchain e DLT [Distributed Ledger Technology] são inovações e tecnologias que estão direcionando vários investimentos das instituições financeiras.

IA, aprendizado de máquina e um outro que eu acho que está para chegar é IoT [internet das coisas]. Eu vejo as tecnologias do 5G e a do IoT como grandes potenciais de transformação do sistema financeiro nos próximos anos.

KC: E a questão de segurança nesse aspecto? Até com IoT, porque tem esse lado que é fantástico, mas sempre tem um risco a mais. Como estamos nos preparando em relação a isso?

OD: Acho que essa pergunta é muito oportuna.

O sistema financeiro vive de credibilidade, aqui e em qualquer lugar no mundo. A sociedade precisa ter confiança no sistema financeiro, confiança de que seu dinheiro vai retornar, confiança no sigilo daquelas informações, confiança nas soluções tecnológicas. Se a gente voltar para aquelas perguntas iniciais de "o sistema financeiro inova? Investe em tecnologia?", eu posso garantir para você que uma parcela significativa do investimento em tecnologia é tecnologia da informação e segurança cibernética. Tanto é que você não tem casos de vazamentos de dados diretamente do sistema financeiro, pois ele tem um zelo enorme com as questões de fraudes. Então, ele é muito reativo e proativo em todos os sentidos para manter a imagem e a veracidade de que é extremamente seguro.

Não obstante, esse é um ponto que o BACEN olha com muita atenção e há algum tempo. Em 2017, iniciamos um processo de construção de uma política de segurança cibernética. Foi uma norma que a gente discutiu bastante com o sistema financeiro e que é única no mundo. Foi muito importante naquele momento e chamou a atenção de todas as instituições financeiras para a importância de você ter uma política consistente de segurança cibernética, que é difundida em toda a empresa. É muito importante também que não só a alta direção da instituição financeira esteja 100% ciente das diretrizes e dos comandos em relação à segurança cibernética, mas que todos os participantes, funcionários e *stakeholders* que têm acesso ao sistema estejam cientes sobre como proceder para assegurar o máximo de segurança cibernética. Eu diria o seguinte: o investimento é extremamente pesado. Todas as instituições financeiras que são reguladas pelo Banco Central do Brasil são extremamente conscientes e investem bastante para manter a credibilidade que têm quanto à segurança dos seus sistemas.

KC: Em relação ao PIX, a gente teve, recentemente, uma onda de sequestros relatada pela imprensa. Será feita alguma mudança por causa disso?

OD: Acho que o primeiro ponto é que qualquer evento que afete pessoas é relevante, mesmo que seja um em um milhão de situações.

O PIX é um sistema extremamente seguro. Em termos de segurança do instrumento, a gente não está questionando isso. O instrumento é extremamente seguro e cumpre o papel de ser um mecanismo de transferência de recursos de pagamentos de contas digitais de extrema eficiência, credibilidade e segurança cibernética. Mas estamos falando agora da relação da sociedade com o uso. O que a gente fez e anunciou após os relatos foi a criação de mecanismos para tentar endereçar pontos de eventual uso ou ação de contraventor e bandidos que usavam as pessoas e os meios de pagamentos para executar a transferência. Isso tem ocorrido não só com o PIX, mas com outros instrumentos, com o cartão de crédito, débito, TED e DOC. É um conjunto de instrumentos, no qual o instrumento em si mantém toda a sua robustez em termos de segurança. A gente não está discutindo aqui segurança cibernética, falha de sistema, mas dado o contexto da sociedade, os bandidos estão explorando esse aspecto.

As medidas são para tentar adequar isso, como já foi feito no passado em relação ao volume de saques durante o final de semana e no período noturno. A gente faz algumas ações assim para tentar evitar isso, minimizar e eliminar esses inconvenientes que estão surgindo para a população.

KC: E o senhor acredita que possa ter algum impacto no sentido de reduzir o número de pessoas usando o PIX? Tem alguma expectativa nesse sentido ou não?

OD: Não!

Eu acho que a sociedade brasileira adorou o PIX porque ele é um produto de fato inovador, eficiente e muito conveniente. A sociedade vai se adaptar à essa regra e vai continuar usando. A gente só vê o uso do PIX crescendo ao longo dos próximos tempos, mesmo porque existe uma agenda evolutiva, em que estamos agregando funcionalidades ao instrumento base.

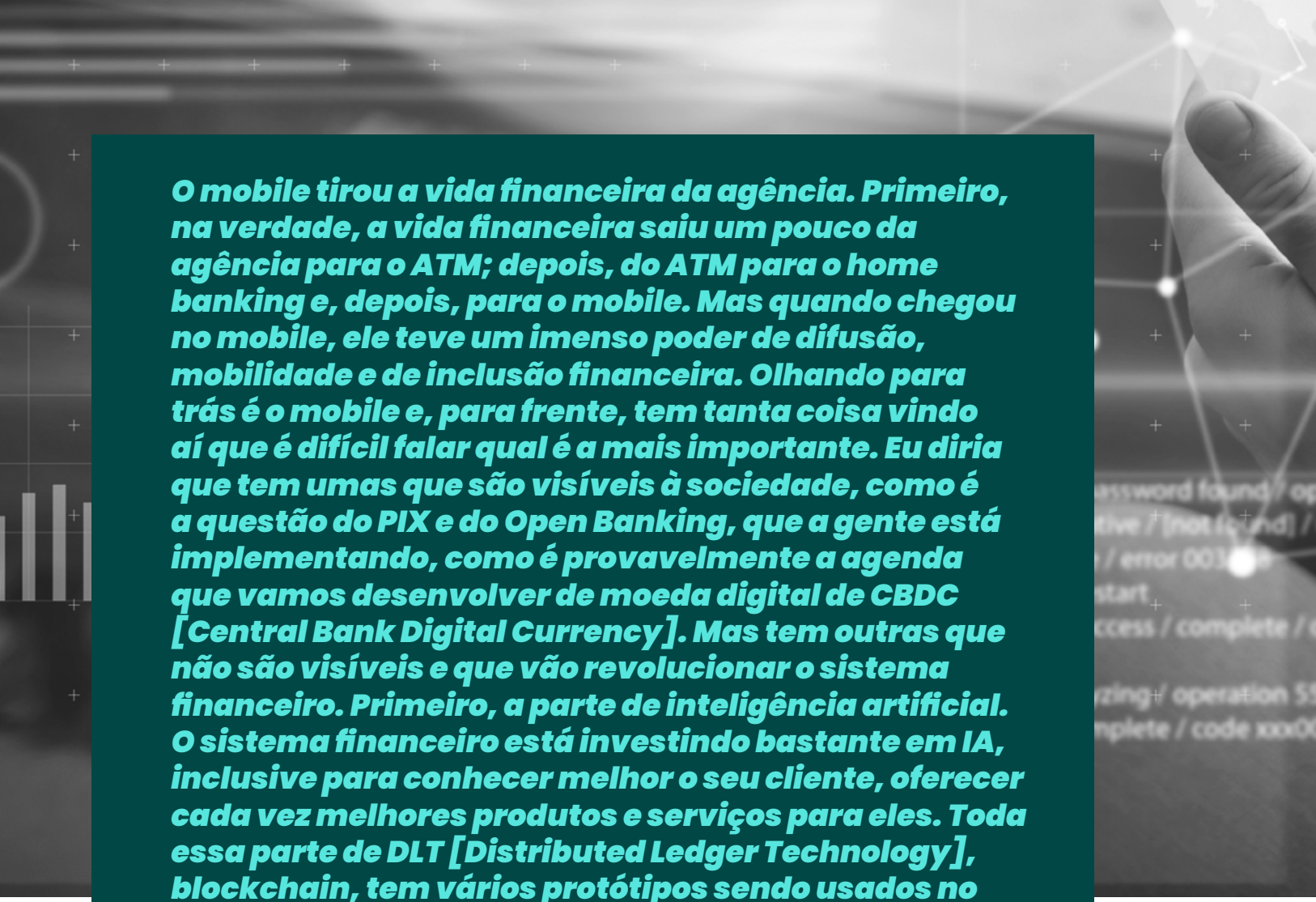
KC: Voltando à questão do estímulo à inovação. Em toda inovação há pessoas que você atrai, mas tem outras que ficam meio perdidas no processo. Neste sentido, quem o senhor acha que tem sido impactado positiva e negativamente pelos programas de estímulo à inovação do BACEN?

OD: Vamos olhar para a economia como um todo e depois a gente vem com o âmbito do sistema financeiro. Quem tem sido impactado é quem não vê a tecnologia chegando e as mudanças acontecendo a tempo. Você teve vários segmentos econômicos, no mundo e aqui, que a tecnologia mudou a forma de operar aquele produto ou aquele serviço, como o transporte. Com a chegada dos aplicativos de locomoção, o segmento de táxis sofreu bastante. Por quê? Porque entrou uma nova tecnologia e alguns não se adaptaram. Depois de um tempo, os táxis começaram também a usar esses aplicativos ou mecanismos de comunicação. Quem não soube se adaptar, ou quem não conseguiu ver com um pouco de antecedência esse processo de mudança, realmente ficou para trás. E isso vale para todos os segmentos econômicos. A gente poderia aqui listar vários deles e voltar no tempo com casos clássicos, como é o caso da máquina fotográfica da Kodak, que foi muito pioneira. Chegou a ter o protótipo de maquininha digital, mas não soube aproveitar e depois vieram as máquinas e deslancharam.

Enfim, o que eu vejo no âmbito do sistema financeiro é que, talvez até pela sua característica intrínseca de estar sempre olhando para frente para tentar trazer valor em tudo, sempre viu esses processos com muita antecedência em relação à sociedade como um todo e em relação a outros segmentos. A gente vê um projeto de adaptação muito interessante no âmbito do sistema financeiro e em todas as discussões. Naturalmente, quando você tem uma instituição que está começando agora, o seu investimento em tecnologia é em tecnologia de ponta. Ela tem uma vantagem comparativa nesse aspecto em relação a um incumbente que tem um legado de uma tecnologia que não é adaptável com muita facilidade para outras mais novas. Mas, mesmo os incumbentes, o que eles fizeram? Eles se mexeram. Você tem um incumbente que criou um novo banco digital e está atuando em paralelo à transformação que está ocorrendo. Teve banco que fez a transformação digital em cima do seu próprio legado e é muito bacana ver como foi se adaptando. Enfim, todos eles perceberam esse processo e buscaram alternativas, mas eu diria que o denominador comum é que todos eles investiram muito em tecnologia e em muita inovação.

KC: Pensando nas tecnologias digitais, quais são as mais úteis, na opinião do senhor, para o sistema financeiro? Quais são as principais apostas?

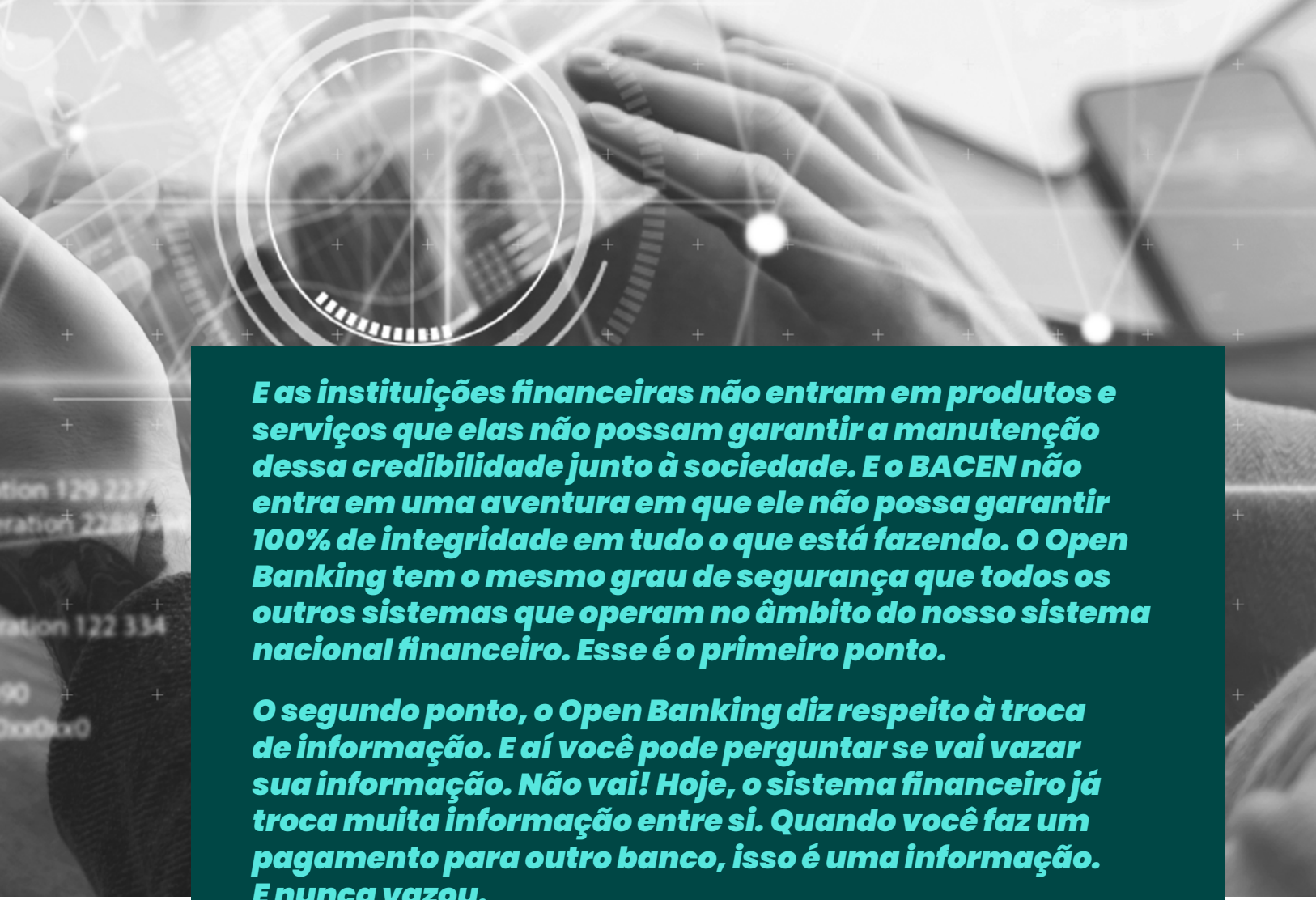
OD: Olha, se a gente olhasse para trás um pouco, eu te diria que a mais revolucionária foi o *mobile*.



O mobile tirou a vida financeira da agência. Primeiro, na verdade, a vida financeira saiu um pouco da agência para o ATM; depois, do ATM para o home banking e, depois, para o mobile. Mas quando chegou no mobile, ele teve um imenso poder de difusão, mobilidade e de inclusão financeira. Olhando para trás é o mobile e, para frente, tem tanta coisa vindo aí que é difícil falar qual é a mais importante. Eu diria que tem umas que são visíveis à sociedade, como é a questão do PIX e do Open Banking, que a gente está implementando, como é provavelmente a agenda que vamos desenvolver de moeda digital de CBDC [Central Bank Digital Currency]. Mas tem outras que não são visíveis e que vão revolucionar o sistema financeiro. Primeiro, a parte de inteligência artificial. O sistema financeiro está investindo bastante em IA, inclusive para conhecer melhor o seu cliente, oferecer cada vez melhores produtos e serviços para eles. Toda essa parte de DLT [Distributed Ledger Technology], blockchain, tem vários protótipos sendo usados no âmbito do sistema financeiro. É intra e interinstituições financeiras. Muita coisa está sendo desenvolvida para facilitar o dia a dia do backoffice que acaba tendo reflexo para frente, com o machine learning e, volto a falar, com o 5G e IoT, que vão mudar a forma de serviços e produtos financeiros para o cidadão no seu dia a dia.

KC: O que o senhor pode dizer mais sobre os benefícios e riscos do Open Banking?

OD: O grau de segurança, que a gente tem para todos os sistemas que operam no âmbito do sistema financeiro, é o mesmo que a gente vai ter para o *Open Banking*. Volto a falar, o principal valor de uma instituição financeira é a credibilidade que ela tem com a sociedade. No dia que ela perde aquela credibilidade, deixa de ter valor.



E as instituições financeiras não entram em produtos e serviços que elas não possam garantir a manutenção dessa credibilidade junto à sociedade. E o BACEN não entra em uma aventura em que ele não possa garantir 100% de integridade em tudo o que está fazendo. O Open Banking tem o mesmo grau de segurança que todos os outros sistemas que operam no âmbito do nosso sistema nacional financeiro. Esse é o primeiro ponto.

O segundo ponto, o Open Banking diz respeito à troca de informação. E aí você pode perguntar se vai vazar sua informação. Não vai! Hoje, o sistema financeiro já troca muita informação entre si. Quando você faz um pagamento para outro banco, isso é uma informação. E nunca vazou.

O quanto você mandou dinheiro para o pai, irmão, um amigo, o seu extrato, o seu cartão de crédito, isso são informações que estão dentro do sistema financeiro. Então, a troca de informação e a de valor são práticas do dia a dia das instituições financeiras. E não tem por que ser diferente com o *Open Banking*!

Terceiro aspecto é que os bancos e as instituições financeiras estão sujeitos ao sigilo bancário. É uma lei complementar e a quebra de sigilo bancário é um crime, não é nem uma punição administrativa. Esse é um aspecto que é muito importante. Um outro é que só podem participar do *Open Banking* as instituições reguladas e autorizadas pelo Banco Central do Brasil. Então, a instituição A pode ter que mandar o dado para a instituição B, mas uma vez que ela transferiu isso dentro do escopo do *Open Banking*, a instituição B tem todos os deveres em relação àquelas informações, inclusive o sigilo bancário. Ela é responsável.

E tudo hoje na tecnologia é rastreável, eu sei de onde veio e sei para onde foi. Como são instituições que são reguladas, autorizadas e, principalmente, supervisionadas pelo BACEN, se tiver alguma falha de conduta, o primeiro a entrar pesado vai ser o próprio BACEN, responsabilizando quem tiver que ser responsabilizado. Então, o sistema financeiro funciona e a gente não vê esse tipo de coisa acontecendo dentro dele. E agrego a isso a discussão sobre segurança cibernética, que vai valer da mesma forma para o Open Banking.

O Open Banking guarda muitas semelhanças com a internet. Qual é a grande semelhança? No início da internet, há 30 anos, você não fazia ideia de como aquilo ia mudar a vida da sociedade mundial. O Open Banking é um pouco disso, a gente vai se reunir daqui a uns 10 anos, olhar para trás e pensar sobre como era possível existir um sistema financeiro sem o Open Banking. E qual é a diferença? Talvez com a internet, 30, 40 anos atrás, a gente não tivesse ideia do que ela poderia transformar. Mas com Open Banking, eu posso falar que ele tem um imenso potencial de transformação. Eu consigo dar vários exemplos que são passíveis de serem entregues pelas instituições financeiras. Por quê? Porque assim como a internet, o Open Banking é uma plataforma (diferentemente do PIX, que é um produto). O que a gente está entregando para o sistema financeiro, para quem for entrar para o sistema financeiro, é uma plataforma de desenvolvimento de produtos e serviços financeiros.

Por isso, a gente tentou alinhar muito as expectativas com o lançamento do *Open Banking* em relação ao lançamento do PIX. O PIX, no dia seguinte, a imprensa vinha e perguntava quantas transações foram feitas, se tinha condições de falar 1 milhão, 2 milhões, 3 milhões, tantos milhões. Com o *Open Banking*, a gente está entregando uma plataforma em fases para as instituições começarem a desenvolver produtos e serviços financeiros para ela.

Olhando para frente, a gente tem uma convicção de que o *Open Banking* vai transformar a forma de operar do sistema financeiro. O que vai ser entregue eu não sei. Vou dar um exemplo para PF [pessoa física] e para PJ [pessoa jurídica]. Exemplo para PF: você hoje tem um limite de cheque especial, que é caro, apesar do BACEN ter feito algumas medidas recentes. Por que que o limite do cheque especial é caro? Porque ele é um produto muito associado à sua conta corrente. Você não pega um cheque especial, hoje, em um outro banco porque ele é um limite emergencial. E você não consegue trazer concorrência para o cheque especial. O que é que o *Open Banking* vai permitir? Se você é uma pessoa que, volta e meia, precisa acessar o cheque especial, mas não tem certeza quando e em qual magnitude, e você gosta do seu banco, mas acha ele está cobrando um pouco caro, poderá muito bem autorizar que um terceiro banco, um IE [investimento no exterior] ou IP [instituição de pagamento] ou uma financeira tenham acesso aos dados da sua conta corrente todo dia e verifiquem se vai entrar ou não em cheque especial. Se isso acontecer, você pode autorizá-lo a te conceder um crédito para cobrir seu cheque especial. Perceberam que você entrou em cheque especial e, automaticamente, transferem o dinheiro para você. Quando é que você vai fazer isso? Quando esse terceiro oferecer para você uma taxa melhor. Eu estou trazendo concorrência para o cheque especial. Para isso, é preciso operar dentro do *Open Banking* com a autorização para esse terceiro ter acesso à sua conta.

Agora, vamos para o exemplo da pessoa jurídica. Hoje, qualquer empresa pequena de porte, às vezes, tem conta em dois, três, quatro bancos, porque precisa ter produtos e serviços diferentes. Mas ela tem uma dificuldade imensa de ter um fluxo de caixa unificado, porque nenhum dos bancos fornece ou deixa ter acesso aos dados dela de uma forma padronizada e digital. A empresa pode ter seu fluxo de caixa unificado se pegar os extratos, as bases de dados, digitar e fazer algo. Mesmo assim, vai ter problema, porque as informações não vêm em volume digital. Já com o *Open Banking*, a empresa poderá permitir que as instituições financeiras onde possui conta tenham acesso às suas informações, entregando-lhes um único extrato. Mas, mais do que isso, elas poderão indicar, por exemplo, que hoje é melhor pagar no banco B, porque ele tem saldo. Ou sinalizarem para não pagar no banco A, pois vai entrar nele uma fatura que está programada e, com esse pagamento, a conta vai ficar "no vermelho". Então, o *Open Banking* vai trazer facilidade para você, para o seu dia a dia.

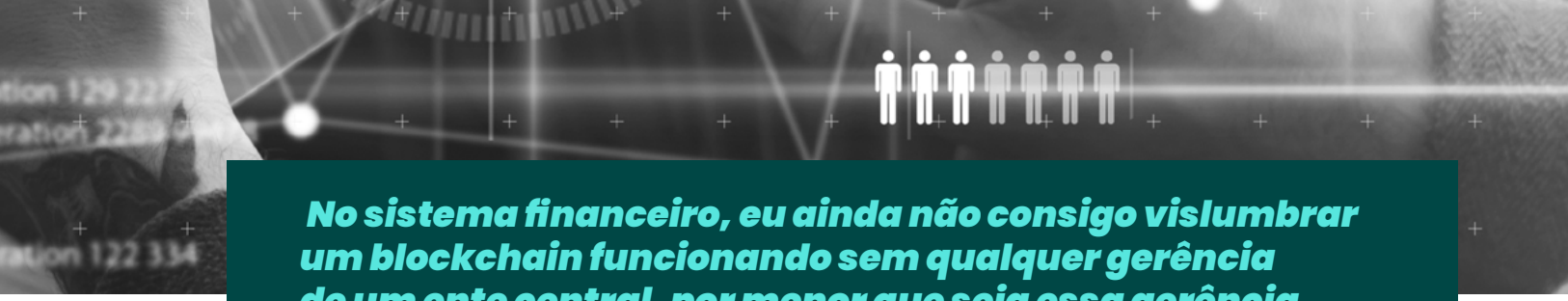
Vamos voltar de novo para a pessoa física. Eu quero comprar um imóvel. Meu banco me oferece R$ 100.000 a uma taxa de x%. Eu estou achando caro e preciso mais que R$ 100.000. Eu posso muito bem permitir que outras instituições e mesmo um *player* do sistema financeiro peguem as minhas informações e consultem todos os bancos, vendo quem oferece maior volume e a menor taxa ou prazo mais longo. Hoje, eu não consigo fazer isso, sabe por quê? Porque o banco C, D, E, F, G, H não me conhecem, eles não sabem quem é o Otávio, não sabem se eu tenho dinheiro e qual é a minha capacidade de pagamento. Mas com o *Open Banking,* eles vão poder saber.

O Open Banking, nesse aspecto, vai atacar de frente um dos principais problemas no âmbito das finanças, que é a assimetria de informação.

KC: O senhor citou como um dos elementos de transformação o blockchain. Já falaram que o blockchain vai substituir as agências reguladoras, inclusive, os bancos centrais. O que não aconteceu, felizmente, porque muito do que você trouxe sobre a confiança do sistema financeiro é provida pelo papel do Banco Central. Como é que o blockchain pode mudar o papel de um órgão como o BACEN, como agente controlador desse universo financeiro?

OD: Primeiro, a gente vai usar tecnologias como o *blockchain* e o DLT ao nosso favor. Dentro do BACEN, a gente tem alguns projetos-piloto de uso interno de troca de informações usando *blockchain* e DLT. O que a gente vê dentro das instituições financeiras, internamente, são vários processos de *backoffice* usando a ferramenta de DLT, de *blockchain*, e isso passa despercebido para o cidadão comum e, às vezes, até para o próprio funcionário da instituição financeira. E também tem alguns projetos-piloto, no âmbito do sistema financeiro, de troca de informações entre eles, usando o *blockchain*.

A gente desenvolveu, no Brasil, um sistema de registro muito eficiente. O que são essas registradoras? Você tem uma entidade que governa aquelas informações, padroniza, autentica, tem a guarda e faz também arbitragem quando as informações são registradas de formas diferentes (a mesma ideia que você teria de *blockchain*). E por que a gente tem esse sistema muito bem desenvolvido no Brasil? Porque durante muitos anos, nas décadas de 80, 90, o Brasil teve várias crises, algumas envolvendo crises bancárias, e para cada fraude que ocorria, a gente ia aperfeiçoando os mecanismos de registro. Hoje em dia, a gente é mais proativo e não espera a crise. Foi criando um sistema de registro que hoje o BACEN tem condições de fazer um levantamento das instituições financeiras em *real time*, às vezes, mais preciso do que a própria instituição financeira é capaz de fazer. Eu consigo montar um balanço diário, pois todas as informações do sistema financeiro estão registradas. E parte dessas informações está aqui no BACEN, e outra, em entidades privadas. É o que a gente chama de infraestruturas do mercado financeiro. Essas entidades privadas são, na verdade, como um *blockchain*, só que com alguma governança. Mas o *blockchain*, na verdade, tem uma governança definida por ele mesmo. Eu acho assim, dentro de uma instituição você pode ter uma DLT funcionando em um modo mais liberal, sem qualquer governança, com o próprio sistema se autogovernando, ou sendo governado pela maioria dos pares, dentro de uma instituição financeira.



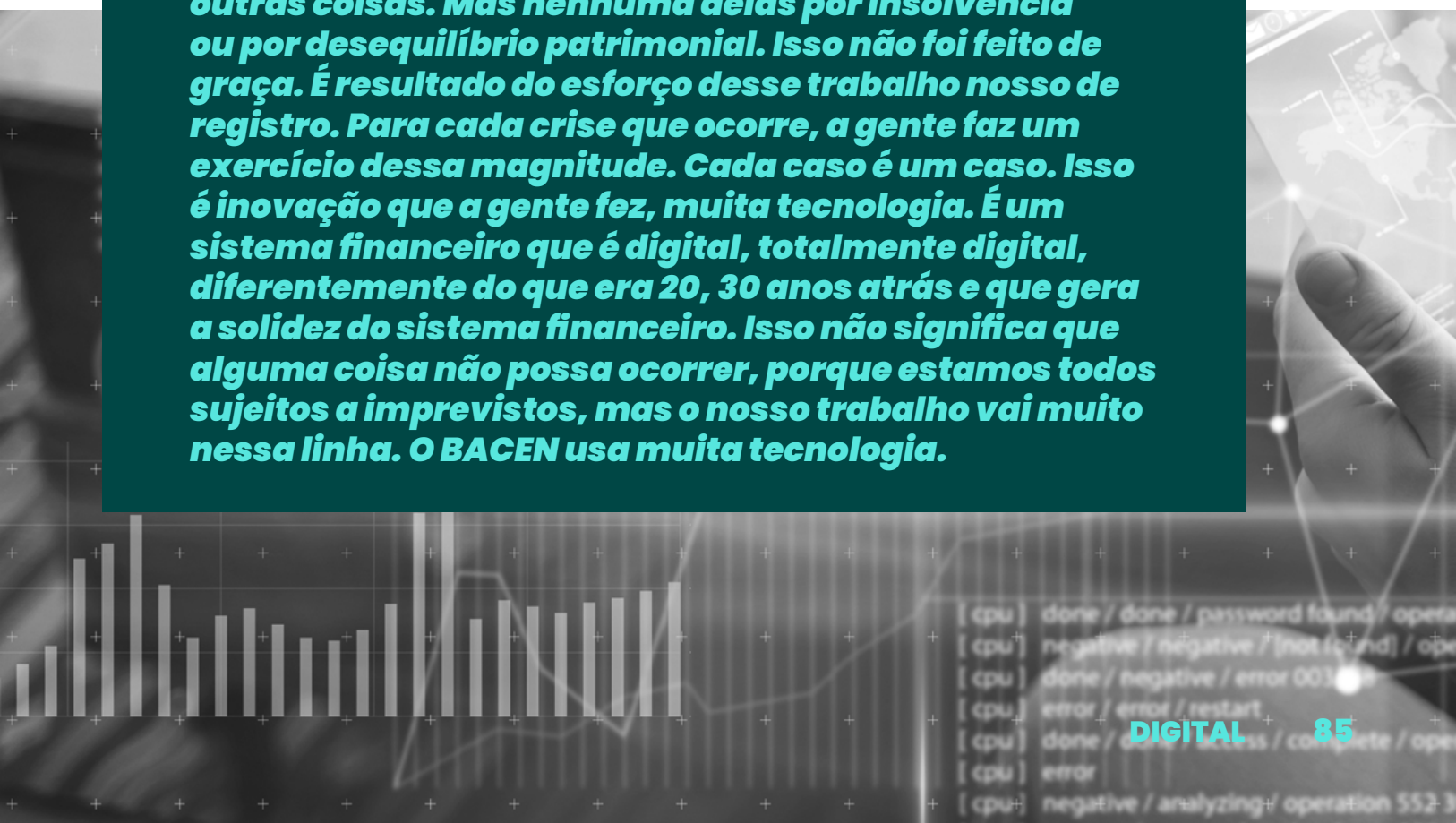
No sistema financeiro, eu ainda não consigo vislumbrar um blockchain funcionando sem qualquer gerência de um ente central, por menor que seja essa gerência. Agora, a tecnologia como um todo está crescendo e vai ser desenvolvida. Onde vai estar essa ingerência, essa gestão como um todo, aí eu não sei te dizer.

Agora, só para contar uma história legal, que pouca gente tem noção de como a coisa funciona e qual a importância desse sistema de registro para a economia brasileira. Como eu disse, hoje, a gente tem um monitoramento pleno do sistema financeiro. Vamos voltar para 2014, quando a Lava-Jato explodiu. Tem uma decisão da Petrobras, naquela época, que foi a seguinte: vamos parar todos os pagamentos da empresa até a gente verificar se eles faziam parte ou não de algum processo de corrupção ou de algum processo que tivesse questionamento. Naquele dia, acendeu um sinal vermelho aqui no BACEN. Imagina o que é um ente do tamanho da Petrobras, numa cadeia de petróleo, que vinha em um processo de investimento imenso e falar assim: "não vou pagar mais ninguém até eu ter certeza de que estou pagando somente processos."

A gente começou um processo de supervisão, que mais tarde foi publicado em um relatório de estabilidade financeira, acho que em 2017, quando passou a crise, graças ao nosso sistema de registro (e aí por trás tem muita tecnologia, muito digital e muita inovação). O que a gente fez foi olhar dentro da Petrobras e, através do sistema de pagamentos, ver para quem ela pagou suas contas, pois como ela não opera nada em dinheiro, tudo é digital. Então, eu fui no sistema de pagamento e verifiquei todos os pagamentos nos últimos 12, 24 meses da Petrobras. Para cada um dos fornecedores diretos, eu qualifiquei aquele fornecedor a partir do grau de dependência dele da Petrobras. Eu olhei para cada um deles, o que que ele recebia de outras empresas e o que que ele recebia da Petrobras. Então, teve grupo que recebia 100% da Petrobras, outros 10%. Eu fiz isso para toda a cadeia, de cada um desses fornecedores. Tudo isso por causa das informações que a gente tem. Depois disso, fui na RAIS e peguei todos os funcionários dessas empresas e todas as operações de crédito que essas empresas tinham com alguma instituição financeira e toda a operação de crédito que algum funcionário tinha com as instituições financeiras. Eu mapeei toda a dependência de uma instituição financeira, a cadeia direta e indireta da Petrobras.

E aí começou o nosso trabalho de supervisão. Identifiquei vários bancos que tinham um problemão de liquidez ou de crédito, porque eles tinham, mesmo sem saber, alto grau de concentração na cadeia da Petrobras. A gente começou um processo de acompanhamento individual com cada banco. E isso foi feito, naturalmente, com sigilo. O nosso trabalho é sigiloso para conseguir chegar no banco e falar assim: "deixa eu te mostrar uma coisa. Você está com teu fluxo de pagamentos aqui dependente dessa empresa, que é hiperdependente da empresa B, que é hiperdependente da empresa A, que depende toda a sua receita da Petrobras e ela falou que não vai pagar mais nada enquanto não apurar. O negócio é o seguinte: você está com isso para receber dessa empresa de crédito ou dos funcionários dessa empresa e, se isso se concretizar, terá problemas de fluxo de caixa e de liquidez. Vamos fazer o seguinte: vamos preparar você para esse cenário de estresse. Reduza isso, faça aquilo, capte no mercado, diminua o seu passivo, aumente o seu ativo, etc. Para cada uma dessas instituições financeiras, a gente foi trabalhando em conjunto com ela para apoiar a gestão. E muitas delas não sabiam do impacto que poderiam sofrer.

Enfim, passamos todo o período de 2014, 2015 e 2016 sem uma instituição financeira no mercado brasileiro quebrar. Nenhuma quebrou. A gente liquidou 15 instituições financeiras por conduta, porque elas participaram de forma ativa em atos ilícitos no âmbito da Lava Jato, com operações de câmbio, entre outras coisas. Mas nenhuma delas por insolvência ou por desequilíbrio patrimonial. Isso não foi feito de graça. É resultado do esforço desse trabalho nosso de registro. Para cada crise que ocorre, a gente faz um exercício dessa magnitude. Cada caso é um caso. Isso é inovação que a gente fez, muita tecnologia. É um sistema financeiro que é digital, totalmente digital, diferentemente do que era 20, 30 anos atrás e que gera a solidez do sistema financeiro. Isso não significa que alguma coisa não possa ocorrer, porque estamos todos sujeitos a imprevistos, mas o nosso trabalho vai muito nessa linha. O BACEN usa muita tecnologia.



Otávio Ribeiro Damaso

Otávio Damaso é Diretor de Regulação do Banco Central do Brasil. Já ocupou os cargos de Chefe de Gabinete do Presidente do Banco Central e de Secretário-Adjunto de Política Econômica no Ministério da Fazenda. Presidiu os Conselhos de Administração da Caixa Econômica Federal, do IRB Brasil RE e do Banco do Estado do Ceará. Formado em Economia na Universidade de Brasília, é funcionário de carreira do Banco Central desde 1998.

Imagem: AdobeStock.com

NOTAS E REFERÊNCIAS

1 https://www.bcb.gov.br/estabilidadefinanceira/sandbox

2 https://www.bcb.gov.br/estabilidadefinanceira/lift

PARTE II

OS ASPECTOS HUMANOS E SOCIAIS DA CONFIANÇA NA ECONOMIA DIGITAL

doi.org/10.52959/2021535411

QUAIS OS LIMITES E DESAFIOS ÉTICOS NOS NEGÓCIOS DIGITAIS?

Luís Lamb

A ECONOMIA DO CONHECIMENTO E A INTANGIBILIDADE

Nos últimos 50 anos, o desenvolvimento da ciência da computação e suas consequentes tecnologias contribuiu fortemente para uma transformação da vida humana. Particularmente, o surgimento da web nos anos 1990 e a crescente utilização de tecnologias como a Inteligência Artificial (IA) levaram a mudanças paradigmáticas na sociedade (Brynjolfsson & McAfee, 2014; O'Neil, 2016; Sperling, 2020). Se, no passado industrial, gestores e empreendedores avaliavam a tecnologia como uma "ferramenta" de auxílio aos negócios, recentemente a percepção da sociedade (e de pesquisadores) é de que a tecnologia é central a qualquer atividade econômica.

A crescente relevância das tecnologias digitais também tem levado pesquisadores a repensarem, inclusive, como incluir novas riquezas, bens ou conhecimentos intangíveis no cálculo de produtividade das organizações, bem como os leva a introduzir (ou pelo menos analisar a possibilidade de incluí-los) nos próprios indicadores de produto interno bruto. Em uma publicação recente, Brynjolfsson et. al., 2019 refletem sobre a possibilidade (ou necessidade) de incluir no cômputo do produto interno bruto dos países o valor intangível dos bens digitais. Na atualidade, muitos destes bens digitais são construídos de forma a incrementar a produtividade de pessoas e organizações. Os autores descrevem experimentos nos quais os consumidores voluntários avaliam o preço dos bens digitais que consomem diariamente (mídias sociais, enciclopédias *online* como a wikipedia, entre outros). No artigo, os resultados indicam que os consumidores atribuiriam preços mensais que estariam dispostos a pagar. Uma das prováveis hipóteses a considerar em pesquisas futuras, sobre este tema, é como computar o valor agregado que estes bens digitais geram na economia contemporânea, pois esse valor ainda não é adequadamente considerado, conforme os autores.

Imagem: AdobeStock.com

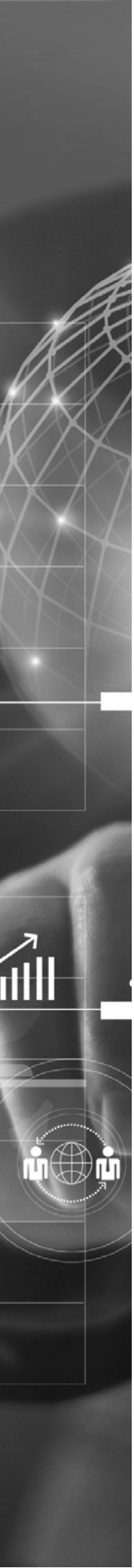
Neste canvas, o desenho da contemporaneidade tecnológica certamente levará economistas e pesquisadores a revisarem conceitos consolidados nesta ciência. Essa "nova" economia tem características marcantes, associadas mais ao raciocínio, conhecimento e cognição do que ao trabalho físico, marcante na era industrial. Aliado à crescente redução dos custos de transmissão e armazenamento da informação, bem como à crescente visibilidade das organizações nas mídias sociais digitais, um cenário desafiador se apresenta: como manter e adaptar os princípios, regras, leis e normas éticas (inclusive tácitas e culturais) definidas para e com o *mindset* da era industrial na moderna economia. Como bem postulado por Brynjolfsson & McAfee, 2014, estamos adentrando uma segunda era das máquinas, com domínio das ideias, da mente e do cérebro sobre a força física, bem ilustrado no seguinte trecho:

> *"Os computadores e outros avanços digitais estão fazendo pela força mental – a capacidade de usar nosso cérebro para entender e moldar nossos ambientes – o que a máquina a vapor e seus descendentes fizeram pela força muscular. Os computadores estão nos permitindo ultrapassar as limitações anteriores e nos levar para um novo território."* (Brynjolfsson & McAfee, 2014)

ÉTICA NOS NEGÓCIOS DA ERA DIGITAL: DA CONCENTRAÇÃO DE CONHECIMENTO ÀS IMPLICAÇÕES NO MERCADO DE TRABALHO

Estamos caminhando para um período em que as riquezas estarão cada vez mais concentradas nos países e organizações que concentram capital humano e conhecimento. Neste início de século XXI, sob o slogan popularizado pelo semanário britânico *Economist* (em reportagem de 2017), que afirma que "dados são o novo petróleo", as maiores empresas da nova economia passam a ser aquelas que têm acumulado dados, conhecimento e pessoas de alta formação acadêmica. Este constitui um capital humano diferenciado, educado e que, portanto, mais rapidamente se adapta a um período de mudança tecnológica (World Bank, 2019). Neste cenário, onde a utilização de volumes de dados pessoais é crescente, desafios relacionados à preservação da privacidade, vieses e preconceitos de gênero, raça, e identidade, entre outros e, notadamente, o impacto das tecnologias digitais (como IA e robótica) no mercado de trabalho tornaram-se pontos fundamentais no projeto e desenvolvimento responsável de novas tecnologias.

Também é necessário ressaltar que aqueles que adotarem as tecnologias de IAI mais cedo nos negócios ("early adopters") provavelmente terão vantagens competitivas. Esse mesmo cenário tem sido extrapolado para países; mais preocupante são os dados que já demonstram que a pesquisa científica, bem como as tecnologias digitais estratégicas estão se concentrando em poucos países de maior população e concentração de capital humano, como Estados Unidos, China, Reino Unido, Alemanha e Japão (Perrault et. al. 2019; Zhang et. al. 2021).



Assim, as consequências serão percebidas não somente sobre a concentração de capital, mas, notadamente, nas características dos postos de trabalho que demandam conhecimento de tecnologias como IA e aprendizado de máquina; estes podem vir a se concentrar majoritariamente nesses países.

O próprio Banco Mundial, em relatório sobre a mudança da natureza do trabalho, levanta questões sobre as implicações da concentração de conhecimento e capital humano sobre o mercado de trabalho (World Bank, 2019). Por outro lado, Brynjolfsson & Mitchell (2015) apresentam uma outra proposição a ser considerada neste contexto de domínio de tecnologias na economia. Eles apontam que a substituição de trabalhos por sistemas de aprendizado de máquina e IA ocorrerá de forma complexa, não sendo meramente uma substituição de postos de trabalho: implicações sobre a economia serão mais profundas, exigindo análises sob diversos aspectos. As tecnologias digitais – concluem – têm implicações profundas, mas não estamos migrando para o fim do trabalho.

Gene Sperling, conselheiro econômico de dois presidentes dos Estados Unidos, em recente publicação também ressalta outro aspecto a ser considerado decorrente do domínio da inovação tecnológica e digital nos negócios: a dignidade econômica. Sperling apresenta argumentos sobre a dificuldade de fazer previsões sobre os impactos da inovação no mercado de trabalho:

> *"Quando se trata de prever os impactos da inovação e da tecnologia nos empregos, vale a pena ser humilde. Poucos economistas no passado tiveram uma visão 20/20 sobre como a mudança tecnológica criará ou destruirá empregos mesmo vinte anos depois. No final do século XIX, 98% da mão de obra necessária para produzir tecidos tornou-se automatizada, mas isso levou a um aumento no número de trabalhos de tecelagem. [...] Um século depois, quando os caixas eletrônicos ATM reduziram o custo de operação de agências bancárias, muitos temiam que isso significasse uma grande redução nos empregos. Ao contrário, como o caixa eletrônico tornou mais barato operar uma agência bancária, mais agências foram abertas, levando a um aumento líquido nesses empregos. Às vezes, empregos inteiramente novos que operam ao lado do setor impactado são criados após a introdução de novas tecnologias. [...] Certamente, quando saí da Casa Branca em janeiro de 2000, não me lembro de ninguém prevendo que, se voltássemos apenas oito anos depois, todas as agências e departamentos - incluindo a Casa Branca e o Departamento de Estado - teriam vários novos empregos nas "mídias sociais".*
> *[Sperling, 2020]*

Em síntese, há diversos aspectos a considerar quanto às implicações éticas da transformação digital dos negócios e adoção de tecnologias como IA no que se refere ao impacto no mercado de trabalho. O primeiro se refere à necessidade de aprimoramento, melhor formação de capital humano e a distribuição dos postos de trabalho nas organizações e nos países. O segundo, mais recentemente analisado por economistas, se refere à temática da dignidade econômica, sob o viés da necessidade de oferecermos possibilidades a milhões de pessoas, em todos os países. Esses dois fatores certamente merecerão mais atenção de pesquisadores nos próximos anos, pela sua forte relação e dependência.

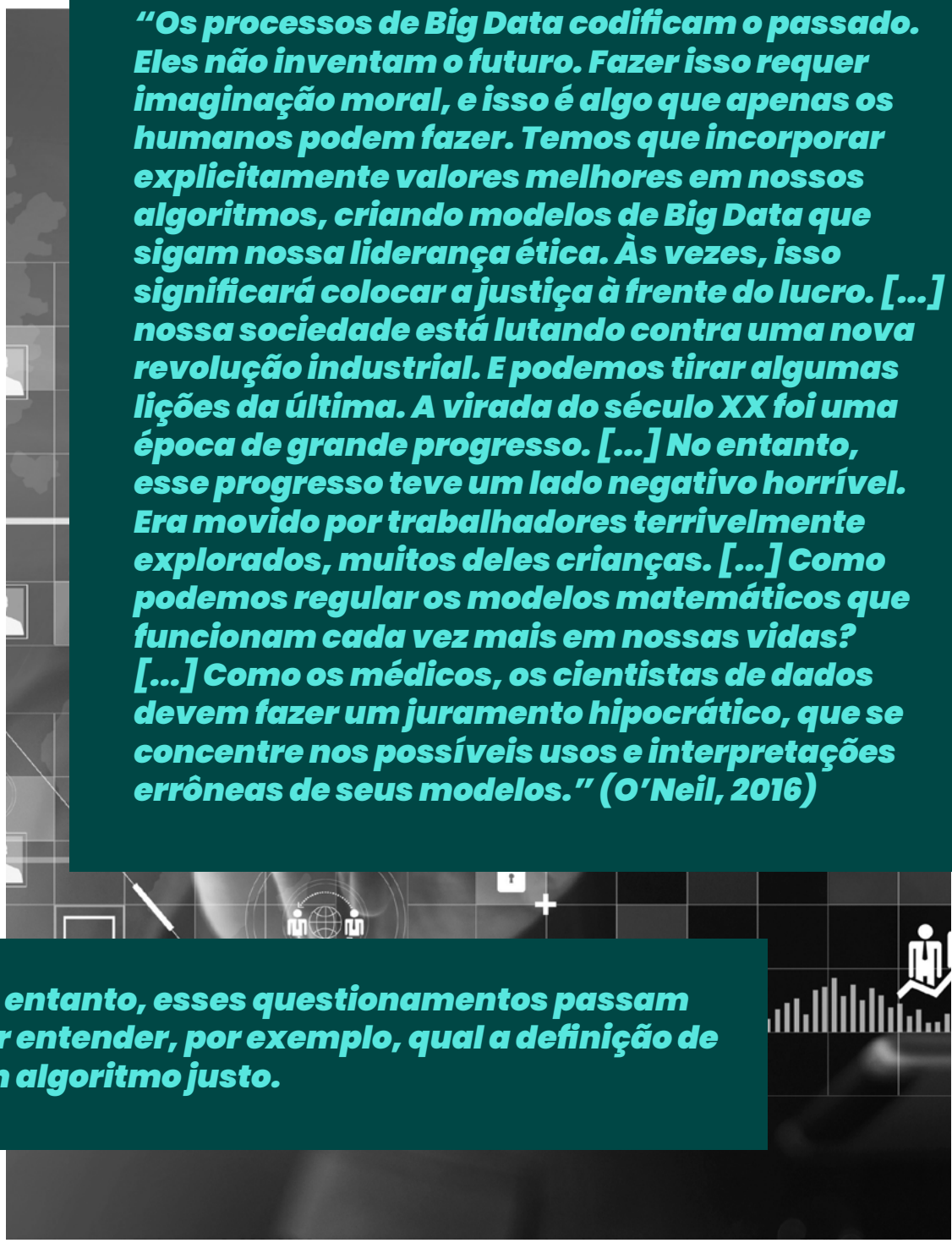
EM DIREÇÃO À AVALIAÇÃO DO IMPACTO ÉTICO DAS TECNOLOGIAS

Nesta sessão, abordamos brevemente a questão das métricas e avaliação das implicações éticas do uso de tecnologias. Nos últimos anos, diversos grupos de pesquisa iniciaram pesquisas para definir como medir o impacto ético das tecnologias e dos negócios digitais (Perrault et. al. 2019; Prates et. al. 2018; Zhang et. al. 2021).

Neste sentido, a concepção das tecnologias utilizadas nos negócios digitais considera aspectos fundamentais, iniciando pela construção de sistemas éticos desde as etapas iniciais de projeto (ethics by design). Isso permite considerar os diversos desafios que incluem o projeto de algoritmos e sistemas éticos, a (não) inclusão de vieses humanos e preconceitos nos dados e sistemas, a interação e mediação ética das tecnologias digitais com o ser humano e o uso dual da tecnologia nos negócios.

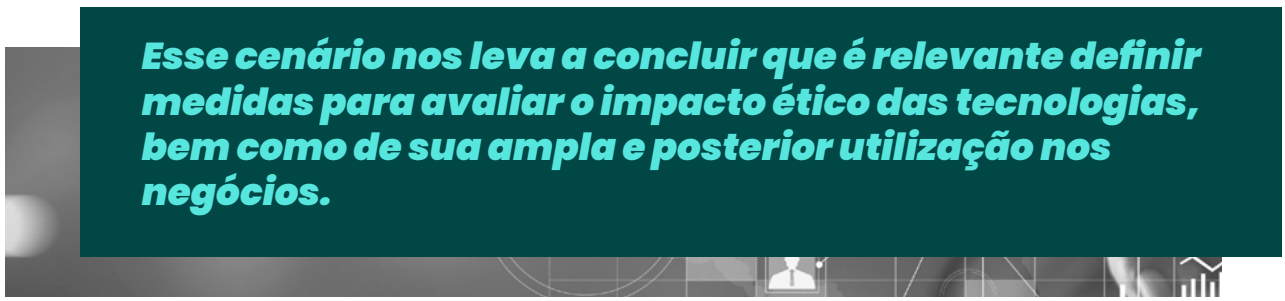
Esses aspectos apresentam uma série de desdobramentos que devem ser considerados por todos os *stakeholders*. O'Neil ilustra a importância de considerarmos diversos aspectos no uso de algoritmos, *Big Data* e tecnologias nos negócios:

"Os processos de Big Data codificam o passado. Eles não inventam o futuro. Fazer isso requer imaginação moral, e isso é algo que apenas os humanos podem fazer. Temos que incorporar explicitamente valores melhores em nossos algoritmos, criando modelos de Big Data que sigam nossa liderança ética. Às vezes, isso significará colocar a justiça à frente do lucro. [...] nossa sociedade está lutando contra uma nova revolução industrial. E podemos tirar algumas lições da última. A virada do século XX foi uma época de grande progresso. [...] No entanto, esse progresso teve um lado negativo horrível. Era movido por trabalhadores terrivelmente explorados, muitos deles crianças. [...] Como podemos regular os modelos matemáticos que funcionam cada vez mais em nossas vidas? [...] Como os médicos, os cientistas de dados devem fazer um juramento hipocrático, que se concentre nos possíveis usos e interpretações errôneas de seus modelos." (O'Neil, 2016)



No entanto, esses questionamentos passam por entender, por exemplo, qual a definição de um algoritmo justo.

Essa questão tem sido enfrentada por um número cada vez maior de cientistas da computação e pesquisadores de diversas áreas. A complexidade dos modelos de IA baseados em volumes gigantes de dados não necessariamente curados e – portanto – refletindo os vieses humanos em sua amplitude torna esta questão ainda mais desafiadora. Recentes estudos apontam que mesmo mecanismos de tradução automática de linguagem apresentam vieses de diversas formas, entre eles o de gênero (Prates et. al. 2020), na classificação de rostos, além do uso (criticado) de ferramentas com impacto na seleção de pessoas para postos de trabalho (Tambe et. al 2019).



Esse cenário nos leva a concluir que é relevante definir medidas para avaliar o impacto ético das tecnologias, bem como de sua ampla e posterior utilização nos negócios.

Por exemplo, Prates et. al. (2018) analisam e quantificam como temas relacionados à ética são apresentados e discutidos nos artigos nas principais conferências e periódicos de IA, aprendizado de máquina e robótica. As estatísticas levantadas foram calculadas em um conjunto de dados de um total de 110.108 artigos, abrangendo 59.352 conferências e 50.756 artigos de periódicos (revistas científicas). Ao longo desta ampla análise, concluímos que menos de 1% dos artigos levantava os impactos éticos e consequências dos trabalhos. Ressaltamos, no entanto, que isto se refere a um histórico de mais de 50 anos de publicações na área de IA, aprendizado de máquina e robótica. Recentemente, a área de ética em IA tem sido objeto de pesquisas por parte de um número maior de pesquisadores (Avelar et. al. 2021) e as próprias técnicas de IA auxiliam na análise de potenciais impactos destas tecnologias na sociedade. Iniciativas internacionais recentes também apontam para a crescente conscientização sobre as inúmeras questões decorrentes da ampla utilização de tecnologias como IA nos negócios (Perrault et. al. 2019; Zhang et. al. 2021).

Em síntese, neste artigo abordamos brevemente alguns aspectos relacionados à ética nos negócios digitais e seus desdobramentos. Há muitos aspectos a considerar, iniciando pela formação de uma nova geração de trabalhadores capacitados para o aprendizado dos valores e conhecimentos relacionados à economia digital e intangível; a reflexão sobre a garantia de dignidade econômica a gerações que terão de fazer a transição da era industrial para a moderna economia digital, bem como a definição de métricas, normas e princípios para o uso ético de tecnologias nos negócios. Há muitos outros aspectos a serem considerados, mas vemos esses desafios como prioritários na contemporaneidade, quando enfrentamos um novo paradigma de aceleradas transformações tecnológicas e econômicas.

Luís Lamb

Luís Lamb é Pesquisador e Professor em Inteligência Artificial, Ciência da Computação e Inovação há mais de 20 anos. PhD em Ciência da Computação pelo Imperial College London, Mestre e Bacharel em Ciência da Computação pela UFRGS. Certificado em Estratégia e Inovação e em Gestão e Liderança na MIT Sloan School. É um dos pioneiros da área de IA neurosimbólica no cenário internacional. Palestrante em eventos sobre IA e ciência da computação na Europa, Ásia, EUA e Canadá abordando resultados de pesquisas do grupo que coordena na UFRGS. Autor de dois livros e dezenas de publicações. Secretário de Inovação, Ciência e Tecnologia do RS; concebeu os programas INOVARS (um dos maiores programas de inovação regional do país), TechFuturo, StartupLab, Tec4Business e Produtos Premium, entre outros. Coordenador da implantação da Aliança para a Inovação UFRGS-PUCRS-Unisinos. É professor Titular da UFRGS.

Imagem: AdobeStock.com

NOTAS E REFERÊNCIAS

Pedro H. C. Avelar, Rafael B. Audibert, Anderson R. Tavares, Luís C. Lamb: *Measuring Ethics in AI with AI: A Methodology and Dataset Construction.* CoRR abs/2107.11913 (2021).

E. Brynjolfsson & A. McAfee: *The second machine age: Work, progress, and prosperity in a time of brilliant technologies.* WW Norton & Company, (2014).

E. Brynjolfsson & T. Mitchell: *What can machine learning do? Workforce implications.* Science, 358(6370):1530-1534. Sept. (2017).

Erik Brynjolfsson, Avinash Collis, W. Erwin Diewert, Felix Eggers, Kevin J. Fox: GDP-B: *Accounting for the Value of New and Free Goods in the Digital Economy.* NBER Working Paper No. 25695, March (2019).

Cathy O'Neil: *Weapons of Math Destruction*. Crown Publishing. 2016.

Raymond Perrault, Yoav Shoham, Erik Brynjolfsson, Jack Clark, John Etchemendy, Barbara Grosz, Terah Lyons, James Manyika, Saurabh Mishra, and Juan Carlos Niebles: *"The AI Index 2019 Annual Report."* AI Index Steering Committee, Human-Centered AI Institute, Stanford University, Stanford, CA, December (2019).

Marcelo O. R. Prates, Pedro H. C. Avelar, Luís C. Lamb: *On Quantifying and Understanding the Role of Ethics in AI Research: A Historical Account of Flagship Conferences and Journals.* Global Conference on Artificial Intelligence GCAI 2018, pages 188-201, (2018).

Marcelo O. R. Prates, Pedro H. C. Avelar, Luís C. Lamb:*Assessing gender bias in machine translation: a case study with Google Translate.* Neural Computing and Applications 32(10): 6363-6381, (2020).

Gene Sperling: *Economic Dignity*. Penguin Publishing Group (2020).

Prasanna Tambe; Peter Cappelli; Valery Yakubovich: "*Artificial Intelligence in Human Resources Management: Challenges and a Path Forward*". California Management Review. 61 (4): 15–42. (2019).

World Development Report 2019: "*The Changing Nature of Work*". The World Bank, Washington DC, (2019). doi: 10.1596/978-1-4648-1328-3.

Daniel Zhang, Saurabh Mishra, Erik Brynjolfsson, John Etchemendy, Deep Ganguli, Barbara Grosz, Terah Lyons, James Manyika, Juan Carlos Niebles, Michael Sellitto, Yoav Shoham, Jack Clark, and Raymond Perrault: "*The AI Index 2021 Annual Report*". AI Index Steering Committee, Human-Centered AI Institute, Stanford University, Stanford, CA, March (2021).

doi.org/10.52959/2021535412

QUAIS OS LIMITES ÉTICOS DA INTELIGÊNCIA ARTIFICIAL E COMO EVITAR VIESES DISCRIMINATÓRIOS?

ENTREVISTA COM SANDRA ÁVILA,
PROFESSORA E PESQUISADORA DA UNICAMP A
KRISHMA CARREIRA DA FSB

Krishma Carreira: Como você avalia o estágio do ecossistema de Ciência, Tecnologia e Inovação brasileiro? Ele está preparado para esse desafio enorme que temos em termos de pesquisa e capacitação, pensando em relação à inteligência artificial e às aplicações de *machine learning*, por exemplo?

Sandra Ávila: É uma visão bastante ampla. Vou responder até onde eu consigo enxergar e também com o que eu estou lidando. Eu acho que, talvez, seja mais interessante começar pela ciência, que é realmente o mundo no que estou bastante imersa. Em relação à ciência, na verdade, a perspectiva é um pouco negativa, pois o investimento está diminuindo drasticamente. Estamos todos, principalmente de dentro das universidades, sofrendo com isso. E a inovação sai bastante de lá. Queremos sempre ultrapassar a fronteira do conhecimento e nunca estamos satisfeitos apenas em resolver um problema. A gente quer resolvê-lo da melhor forma!

Um lado positivo é que, do ponto de vista de inovação das empresas, todo mundo já percebeu que está faltando muita gente para isso. Então, as próprias empresas estão começando a investir nas universidades para formar pessoas. A gente não tem nem programadoras e programadores, muito menos pessoas com um conhecimento mais especializado. É um cenário extremamente difícil e está sendo cada vez mais sucateado.

Mas eu fico muito impressionada com o que as pessoas fazem com tão pouco recurso. A criatividade (pensando nas soluções sem o recurso) é realmente muito impressionante! Você fica se perguntando: e se realmente tivesse investimento, imagina o que a gente faria?

Imagem: AdobeStock.com

KC: **Fazendo um gancho com o que você falou sobre a questão da redução de investimentos, pensando na Estratégia Brasileira de Inteligência Artificial (EBIA), você acha que ela avançou mesmo ou é ainda meio "*fake*"? Tem muito pano para manga?**

SA: Vou aproveitar sua fala, tem muito pano para manga... Tem muito pano para manga em muitos lugares. Tem alguns países em que as discussões já estão mais avançadas, isso não é uma coisa que está todo mundo sabendo como deve fazer. É muito recente mesmo! As aplicações começaram, de fato, como algo bastante promissor em 2012, 2014, 2015. Então, tem realmente muito pouco tempo. Essa discussão ainda vai durar bastante tempo, envolvendo até o que a gente deveria regular sobre inteligência artificial. Ainda estamos engatinhando.

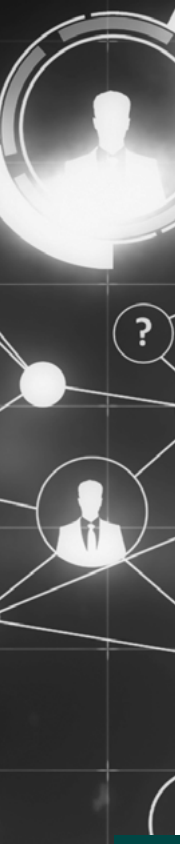
KC: É um roteiro de boas intenções, só falta saber como fazer?

SA: Todo mundo sabe que é necessário. E, assim, se você não estiver fazendo isso, vai ficando cada vez mais para trás. Virou realmente decisório.

KC: Só para pegar um ponto que você já citou quando falou sobre programadoras e programadores. Como atrair mais programadoras? Isso também é uma questão essencial. O que você acha que dá para fazer nesse sentido?

SA: Existem várias iniciativas das próprias mulheres programadoras mostrando que computação é legal. Se você saiu do colégio e vai entrar para uma universidade, ainda é uma pessoa muito nova para tomar essa decisão. E, na própria universidade, quando a mulher começa a ter contato com a programação é que ela descobre. Então, o que tem acontecido muito, inclusive, é mudança de carreira. As pessoas estão percebendo que programação é importante ou pelo menos que deveriam ter esse conhecimento, que trata de um raciocínio lógico de como se deve resolver um problema. E aí as pessoas acabam mudando.

Eu acho que as iniciativas que mostram o que você está fazendo acaba atraindo a atenção por si só. Quando você vai num lugar e vê um tanto de homem, você vai dizer assim: "nossa, eu, Sandra, não gostaria de trabalhar naquele lugar". Então, na hora que eu vejo um lugar diverso, eu digo: "poxa, aqui deve ser legal de trabalhar". Você fica com vontade de fazer aquilo. A gente tem (e eu falo "a gente" porque é um grupo) várias iniciativas nesse sentido, começando inclusive com as meninas pequenininhas. Tem um evento chamado Meninas SuperCientistas para meninas do sexto ao nono ano. Estamos sempre trazendo mulheres palestrantes, falando de suas respectivas pesquisas e trabalhos. Não tem nada dizendo assim: "olha, isso é para mulher". É mais no sentindo de "deixa eu mostrar o que eu faço". Só isso! Eu só estou mostrando o que eu faço. E na hora em que eu mostro o que eu faço, a pessoa olha e diz assim: "eu também posso fazer!" Então, esse mostrar faz parte, mas não só para as mulheres, mas para os homens também.



KC: Com a pandemia, houve um processo de aceleração do uso de algumas ferramentas. Os *chatbots* e outras interfaces com os clientes são alguns exemplos mais visíveis. Você acha que as pessoas já estão confiando mais nessas ferramentas? Acredita que elas venceram alguns preconceitos e medos em relação ao uso de robôs e tecnologias mais disruptivas?

SA: Se você está lidando com *chatbot*, tem muitas pessoas, inclusive, que se sentem mais à vontade de fazer determinadas perguntas. Mas há coisas diferentes do que eu posso tirar da sua pergunta.

Sobre as pessoas confiarem em usar, eu acho que sim. Menos quando querem cancelar algum serviço. Aí você não quer falar com um *chatbot,* você quer falar com uma pessoa.

No Brasil, sei que tem, por exemplo, máquinas de sorvete em *shoppings.* Você interage com o robô e ele dá tchauzinho para você e as pessoas acham: "oh, que lindo! Que fofo!" As pessoas gostam. Agora, isso é uma tarefa muito objetiva, que eu tenho uma pergunta e uma resposta objetiva para quem está em frente a uma máquina que faz sorvete, por exemplo.

Agora, quando você está lidando com coisas que têm uma subjetividade ou então que estão fazendo um diagnóstico, você não espera que a máquina faça aquilo sozinha, você está esperando que seja a máquina, que é uma inteligência aumentada, como a gente chama, e não inteligência artificial. Inteligência aumentada é quando você está juntando o ser humano com a máquina e aquilo está dando uma resposta melhor para uma determinada tarefa.

Também tem a confiança até dos próprios algoritmos em relação à resposta. E as técnicas, hoje, não são totalmente interpretáveis. Na hora que você não sabe como aquela resposta aconteceu, trazendo para um outro ponto de transparência, perde a confiança. Então, tem um caminho longo pela frente. E as pessoas estão muito mais preocupadas com isso hoje. Como que eu deixo tudo mais transparente, confiável e auditável?

Imagem: AdobeStock.com

As pessoas estão muito predispostas realmente a utilizarem essas tecnologias. Eu trabalho bastante na área da saúde e eu nunca me deparei com uma situação de chegar para conversar com alguém e a pessoa falar bem assim: “ah, mas eu acho que a gente não deveria aplicar esse negócio porque não vai dar certo”. Ao contrário, a recepção é sempre muito boa. As pessoas já perceberam de fato que aquilo é uma necessidade.

Vamos falar agora sobre como a gente deveria enxergar essa questão do que tem sido proposto em relação à IA.

A IA é hoje uma tecnologia de propósito geral e vai se tornar cada vez mais presente. E uma tecnologia de propósito geral, fazendo um paralelo aqui, é como a gente tem hoje a eletricidade e o computador, que estão presentes em todos os lugares. Não perguntamos porque isso ocorre. Na verdade, é o contrário. Quando você chega num lugar e não tem energia, as pessoas ficam surpresas. A IA vai estar assim também, permeada em todos os lugares. E a gente vai ficar se perguntando: “não está aplicando IA aqui? Deveria!” Ela não vai resolver todos os problemas do mundo, esse não é o propósito, mas com certeza ela vai estar bem mais presente e a gente vai começar a achar estranho quando não estiver.

KC: **Mas você não acha que aí entra um lado que é mais complexo e traz outros problemas do ponto de vista social? Porque, com a eletricidade, você percebe a presença dela... Você não raciocina no seu dia a dia que você já tem, mas você a vê. Agora, quando você tem uma IA, você muitas vezes não faz ideia de que foi uma inteligência artificial por trás. De novo, a gente volta para a questão da transparência. Como é possível fazer para que as pessoas entendam? Faz parte de uma literacia, de uma educação, de um treinamento digital, mas como você consegue de fato explicar, traduzir uma coisa para que as pessoas a entendam, estejam mais abertas e saibam usá-la melhor?**

SA: Uma boa parte realmente vem da educação, para que as pessoas entendam que aquilo vai estar presente em todos os lugares e elas têm que se questionar. Tem uma parte também que é responsabilidade...

Cabe às pessoas que estão desenvolvendo ou aplicando uma solução deixá-la pelo menos de uma forma um pouco mais clara, porque você não está esperando que todo mundo tenha conhecimento sobre isso.

Tem uma outra coisa também em relação à questão da IA, que é em relação aos dados. As pessoas não sabem da importância dos dados, sobre seus respectivos dados, sobre como aquilo está sendo usado e como aquilo pode estar está sendo usado contra ela. As pessoas precisam realmente de uma educação, precisam saber que aquele dado está sendo usado para influenciar diversas tomadas de decisões na vida dela.

Eu não tenho resposta, realmente, pois é muito difícil dar essa resposta sobre o que a gente deveria fazer, porque há várias coisas que podem ser feitas, mas ainda são coisas muito pequenas.

KC: O programador e a programadora também têm vieses que são incorporados na hora de criarem modelos. Como é possível minimizar isso na hora de programarem?

SA: Primeiro, a gente tem que perguntar: qual é o problema que a gente está resolvendo e qual é o público-alvo? Geralmente, o que tem acontecido é que as pessoas estão propondo modelos e estão dizendo que aqueles modelos podem ser aplicados para qualquer coisa. Eu acho que os nossos modelos deveriam sair com uma bula de remédio: isso aqui é indicado para isso, isso é contraindicado para aquilo, não usa esse porque isso vai ter problemas ....

E isso começa com os dados. A questão é que esses modelos hoje precisam de muitos dados que, muitas vezes, você não sabe que estão sendo usados ali. Mas há algumas coisas simples que podem ser feitas e as pessoas não estão fazendo. Um exemplo: gerei meu modelo, agora vou aplicar testes aleatórios para avaliar se meu modelo está realmente funcionando, pensando em casos mais diversos possíveis, tendo uma equipe diversa que consegue fazer essas perguntas. Na hora que a gente faz uma prova dos 9, em relação ao nosso modelo, você vê: "opa, isso não está funcionando".

Imagem: AdobeStock.com

Vamos puxar o gancho do reconhecimento facial, que é muito problemático. Quantos modelos a gente tem de reconhecimento facial que não funcionam para pessoas de pele negra? Se você disponibiliza, tem que verificar se o negócio está funcionando. Não? Faça o seu trabalho! Vá lá e questione. E aí esse questionamento geralmente vem quando você tem uma equipe diversa, para quem é possível perguntar se acha que o que foi proposto é adequado e se funcionaria para todo mundo.

Vou pegar um exemplo bem bobo: filtros no Instagram que você muda a cor do cabelo. Vi uma pessoa que tinha cabelo liso e aquilo funcionou maravilhosamente bem para ela. Fui testar e ficou um caos. Não funcionava por causa do cabelo cacheado. Estou pegando aqui um exemplo realmente bobo.

Mas vamos dar outros exemplos, como a questão do câncer de pele. As imagens que a gente tem são essencialmente de pessoas brancas. Aquilo não vai funcionar como a gente espera para população brasileira. E eu não posso entregar esse modelo e achar que vai funcionar com o mesmo resultado de outros países. Não vai funcionar de jeito nenhum, porque o padrão é diferente do tipo de lesão. Vai dar uma resposta possivelmente errada. Mas acho que se questionar e ter equipe diversa já são grandes passos.

KC: O que você pode falar mais relação à questão do racismo algorítmico?

SA: O que eu acho que está acontecendo é que a gente está automatizando o racismo e, muitas vezes, quem está desenvolvendo isso são pessoas que não estão preocupadas (mesmo que de forma não intencional) em se questionarem sobre isso.

Então, novamente, precisamos de outras pessoas que estão questionando os modelos e vendo coisas que não deveriam ser aplicadas. Reconhecimento facial não deveria estar sendo usado! Sistemas de reconhecimento facial foram banidos e julgados no mundo. A gente não deveria estar fazendo reconhecimento facial, porque isso, na verdade, só arrebenta para o lado de quem já está sendo prejudicado e está só piorando uma situação que já existe.

Imagem: AdobeStock.com

KC: Pegando do ponto de vista de segurança, se você tem um sistema de reconhecimento facial que não reconhece direito a pele negra, mas no fundo há mais pessoas sendo presas em função disso, o que leva a esse resultado?

SA: Exatamente, ele está sendo vitimado duas vezes, pelo menos. Primeiro porque a pessoa só está sendo presa por causa da pele, isso já é uma agressividade enorme. E, segundo, porque aquela pessoa nem deveria estar sendo presa. Foi um erro realmente em relação ao sistema, de quem está usando aquilo, implantando aquilo [reconhecimento facial] que não deveria estar sendo implantado. Por isso que hoje há uma discussão muito grande em relação ao banimento do reconhecimento facial e não ser aplicado para tomar decisões para nada.

Tem uma outra questão que a gente está entendendo sobre o viés. Aí vem muito a parte computacional. Estamos tentando entender melhor as técnicas que aplicamos.

Há diversos tipos de vieses e isso é importante comentar. Tem um viés que é histórico. Se a gente voltar para o reconhecimento facial, que é bastante problemático, o viés histórico é o que a gente tem hoje na população carcerária do Brasil, que tem mais pessoas de pele negra do que de branca. Então, se você treinar o algoritmo com um conjunto de dados desse, você vai dizer que, provavelmente, ele indicaria uma pessoa de pele negra se eu tivesse que identificar alguém para prender ou não. Se a gente traz exatamente esse dado, o algoritmo aprendeu errado, porque a gente ensinou errado. É necessário balancear de alguma forma para esse aprendizado não acontecer desta forma. Tem outros vieses, como o que acontece quando extrai correlações espúrias do dado

Isso também aconteceu muito com a Covid agora. Há alguns artefatos na imagem que estavam sendo usados, em algumas técnicas, para dar certas respostas para pessoas que fizeram raio-X. Mas a técnica do modelo não estava prestando atenção na imagem do pulmão, e sim nos artefatos que estavam na imagem. Há vários problemas de vieses, em vários lugares, em relação a isso.

Há outros tipos de vieses ainda, como o da própria técnica e o de interpretação. É preciso ter cuidado na própria interpretação dos modelos. E, novamente, estamos estudando todas essas coisas, mas enquanto nós estivermos estudando, não podemos sair cometendo erros. Isso é importante. Se tem alguma coisa que não está funcionando, não dá para deixar o negócio operando, enquanto ele vai melhorando. Não! Tira esse negócio! Essa é a história do reconhecimento facial. Tem que parar com isso, porque não está funcionando. Tem que ser estudado antes de sair aplicando nas pessoas. Estuda, mas não no modelo implantado.

KC: Estamos entrando na questão da ética nas tecnologias.

SA: O que eu tenho falado recentemente é que a gente precisa falar mais de ética e menos de técnica.

E se nós falarmos um pouco mais sobre ética, começamos a refletir e colocá-la no processo. Eu vou pegar um exemplo de um trabalho que eu fiz com uns alunos de uma disciplina e que acabei discutindo uma questão de ética em relação ao processo e pedindo tarefas muito simples. Um grupo deveria definir o que é ética. Com o outro grupo, eu queria que eles pegassem ética em inteligência artificial e procurassem uma reportagem sobre como essa questão de ética (ou falta de ética na verdade) estava acontecendo no processo de IA. Foi realmente um trabalho muito simples. Mas eles foram procurar e se depararam com vários problemas, começaram a se questionar sobre os problemas que estavam resolvendo, sobre os dados que estavam usando e o que as pessoas estavam fazendo. Com isso, o projeto final, que tinha que começar de um jeito, terminou de outro, por causa desse questionamento.

Então, uma coisa que falta (e falta mesmo!) é a gente começar a falar, pois a gente não está discutindo sobre a ética.

Muitas coisas nesses modelos estão sendo gerados e somos todos responsáveis por ele. E a gente não está discutindo como aquele modelo está sendo gerado de fato, quais são os dados que estão sendo usados.

Hoje, existem as grandes conferências (falando do ponto de vista científico) que no processo de submissão dos artigos já estão fazendo questionamento em relação à ética do *paper* que você está propondo. Qual o problema que você está resolvendo? Quais são os seus dados? Como estão os seus dados? Onde ele foi testado? Essa discussão já está vindo para conferências, conferências grandes na parte de *machine learning,* que tem um público razoável.

Precisamos discutir e trazer isso para os cursos que são técnicos, como a matemática, estatística, computação, engenharias. Mas a gente não está discutindo a ética, a gente está falando muito das técnicas! Eu tenho certeza de que, em outros cursos, essa preocupação não é algo que está começando, é uma discussão permanente, mas, para muitas áreas, não é. Isso dá um problema... Estamos automatizando o problema e a gente tem que solucioná-lo.

KC: Como garantir transparência de fato e uma espécie de prestação de contas algorítmica? A gente sabe que os sistemas são tão complexos, com vários algoritmos e pessoas envolvidas, como dá para garantir, então, transparência no processo?

SA: É uma pergunta bem difícil. Essa discussão está acontecendo agora em vários setores, setores de governo, nas próprias empresas. Você tem que garantir essa transparência e informar como é aquele seu dado. Eu estou coletando alguma coisa? Onde aquele dado vai ser usado? Para que problema aquilo vai ser resolvido? Não é no sentido de impedir que aquele problema seja solucionado, mas se eu estou disposta a fornecer meu dado, eu quero saber onde aquele dado vai ser utilizado. Começando por aí, realmente existem várias perguntas que a gente poderia fazer.

Imagem: AdobeStock.com

Inclusive a questão ética e a transparência estão muito juntas para você poder auditar uma resposta. Eu entrei com um dado, saiu uma resposta e preciso entender aquele processo. Como funciona isso? As melhores técnicas não estão prontas para isso. Elas não fazem isso. Tem muita coisa que precisa ser feita.

KC: Algumas grandes empresas de tecnologia têm técnicas para detectar se tem viés no algoritmo. Esse tipo de técnica funciona?

SA: Funciona, mas só que sempre para um escopo. Tem um escopo de dado, um escopo de programa, tem sempre restrições. Não é uma técnica que funciona para tudo. E não funciona mesmo. A gente tem vários problemas que estão sendo resolvidos. Muitas vezes, a saída vai ser um número, que pode ser um número variando no espaço real (não é um número, 1, 2, 3, mas pode ser um 1.1, 1.2, 2.75) e isso já muda todo o processo, porque a gente está resolvendo problemas diferentes. Pode ser uma imagem, pode ser um vídeo. Então, como a gente dá essa resposta? É um conjunto imenso de técnicas e aquilo não funciona realmente para todas as coisas.

Mas eu vou dizer que tem muita gente preocupada, que sabe que, se isso não acontecer, algumas aplicações não poderão ser executadas, porque elas vão passar por uma regulação e não serão aprovadas. Então, a gente vai ter que resolver aquele problema. E é melhor que a gente comece a resolver, já desenvolvendo as técnicas, do que a gente ser cobrado depois. Porque seremos cobrados depois, pois somos todos responsáveis por isso e a gente precisa realmente estudar esse processo.

KC: Para finalizar, em relação ao aprendizado de máquina, o que está por vir no curto e no médio prazo, em termos de aplicação?

SA: Tem uma coisa que acho que vai ter bastante mudança (e já tem acontecido até), que é uma medicina mais precisa, voltada para cada pessoa. Hoje, já tem coisas desse tipo (um remédio pode funcionar para uma pessoa e de outro jeito para outra). Hoje, a gente usa o que dá para fazer no momento, mas poderia talvez ter resultados bem mais interessantes. Outras aplicações já existentes são relacionadas ao processo de produção de alimentos. Produzir alimento com menos desperdício e garantindo uma produção maior, por exemplo. São tarefas que, sendo automatizadas (e elas são bastante objetivas), têm um impacto muito forte para a população mundial.

Sandra Ávila

Sandra Avila é professora no Instituto de Computação (IC), da Universidade Estadual de Campinas (UNICAMP), desde Fevereiro de 2017. É doutora em Ciência da Computação, com duplo diploma, pela Universidade Federal de Minas Gerais (UFMG) e pela Sorbonne Université (UPMC Sorbonne, Paris 6, França), em 2013; mestre em Ciência da Computação pela UFMG, em 2008; e bacharel em Ciência da Computação pela Universidade Federal de Sergipe (UFS), em 2006. Foi pesquisadora científica em Pós-Doutorado na UNICAMP (2013 a 2016), na Faculdade de Engenharia Elétrica e Computação (FEEC), em convênio com a SAMSUNG e pelo PNPD/CAPES. Em 2018, 2019 e 2020, foi agraciada com o prêmio Google Latin America Research Awards. Suas pesquisas estão voltadas para Inteligência Artificial, mais especificamente Aprendizado de Máquina e Visão Computacional, com ênfase na Saúde, Análise de conteúdo sensível e Agricultura de precisão. Em 2020, Sandra Avila foi selecionada para representar o Brasil no BRICS Young Scientists Forum, na área de Inteligência Artificial. Sua paixão é incentivar meninas e mulheres a apostarem em carreiras nas áreas de STEM (Ciências, Tecnologia, Engenharias e Matemática).

Imagem: AdobeStock.com

doi.org/10.52959/2021535413

A MEDICINA ESTÁ CADA VEZ MAIS TECNOLÓGICA. MAS, AFINAL: QUANTO MAIS DIGITAL, MELHOR?

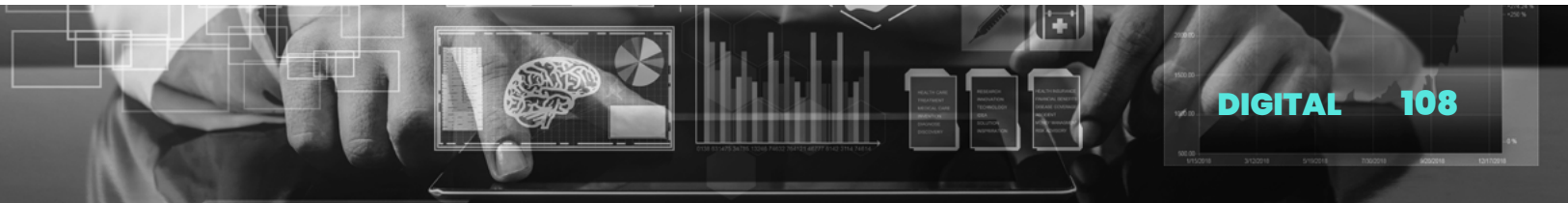
Rogério Pires

A medicina, na forma como conhecemos atualmente, só se tornou possível graças aos avanços da ciência e da tecnologia. Claro que a área médica já conta há algum tempo com ferramentas e dispositivos que facilitam a rotina dos profissionais e contribuem para a saúde dos pacientes, já que historicamente a tecnologia é uma constante aliada na linha de evolução e aperfeiçoamento da medicina. Porém, é inegável que, nas últimas décadas, a tecnologia passou a avançar com uma velocidade cada vez maior, e por isso já vemos máquinas substituindo inclusive funções humanas. Apesar de parecer natural para alguns, o excesso de tecnologia pode assustar outros. Mas afinal: é algo que devemos temer?

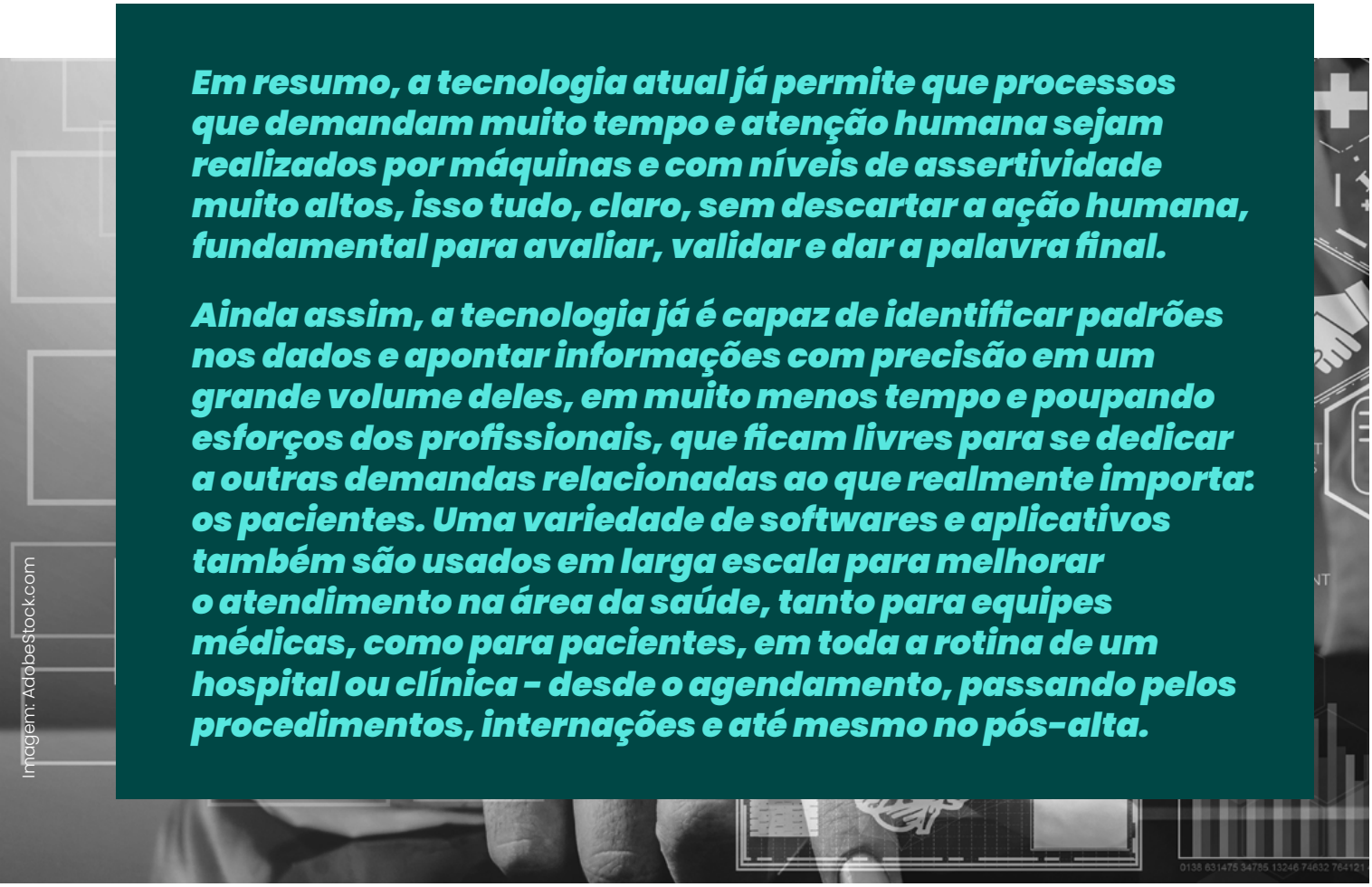
Os estudos em ciências como a anatomia, física, biologia e química se intensificaram no final do século XV, potencializando uma infinidade de descobertas científicas e tecnológicas que fizeram com que a medicina pudesse avançar ao longo dos tempos. Em grande exemplo foi o impacto causado pela revolucionária descoberta do Raio X, ainda no século XIX, pelo físico alemão Wilhelm Konrad Röentgen. Passamos então pelo desenvolvimento das vacinas, criadas por Edward Jenner no século XV para combater a varíola; dos antibióticos, com o descobrimento da penicilina por Alexander Fleming em 1928, além de muitos outros avanços. E todas essas descobertas foram promovidas baseadas nas mais recentes tecnologias de cada época.

Nos últimos tempos, essas inovações têm surgido com uma velocidade impressionante, promovendo profundas transformações no setor da saúde, com novas técnicas e métodos capazes de melhorar o diagnóstico e o tratamento de inúmeras doenças. Um exemplo é o uso da robótica, que passou a ajudar médicos a realizarem cirurgias cada vez menos invasivas e mais precisas, com o auxílio de braços mecânicos, promovendo menos riscos de infecção e sangramentos dos pacientes, por exemplo, além de uma maior precisão em áreas de difícil acesso.

Trazendo para o presente, recentemente fomos testemunhas oculares da corrida para o desenvolvimento de vacinas contra a COVID-19 em tempo recorde, vacinas que estão sendo a principal arma de combate aos impactos da maior pandemia de nossos tempos. O distanciamento social causado pela atual pandemia também ajudou a consolidar outros



avanços tecnológicos na área da saúde, como a telemedicina e diversos usos e aplicações da inteligência artificial (IA) em processos do setor, como no *compliance* das operadoras de planos de saúde na análise e aprovação de procedimentos, exames e cirurgias de forma automática, além da ajuda na automatização de processos de auditoria médica.



Em resumo, a tecnologia atual já permite que processos que demandam muito tempo e atenção humana sejam realizados por máquinas e com níveis de assertividade muito altos, isso tudo, claro, sem descartar a ação humana, fundamental para avaliar, validar e dar a palavra final.

Ainda assim, a tecnologia já é capaz de identificar padrões nos dados e apontar informações com precisão em um grande volume deles, em muito menos tempo e poupando esforços dos profissionais, que ficam livres para se dedicar a outras demandas relacionadas ao que realmente importa: os pacientes. Uma variedade de softwares e aplicativos também são usados em larga escala para melhorar o atendimento na área da saúde, tanto para equipes médicas, como para pacientes, em toda a rotina de um hospital ou clínica - desde o agendamento, passando pelos procedimentos, internações e até mesmo no pós-alta.

Imagem: AdobeStock.com

Conhecer melhor o paciente e ter todo seu histórico médico com facilidade também é outra grande revolução recente do setor. A partir da gestão de dados, o profissional de saúde consegue compreender a história do paciente e abordar o tratamento de uma maneira mais completa e eficaz. Deste modo, é possível evitar pedidos e encaminhamentos desnecessários e, portanto, realizar uma conduta mais adequada à necessidade do paciente. O resultado disso é o direcionamento do cuidado para a prevenção e a facilitação do acesso à saúde.

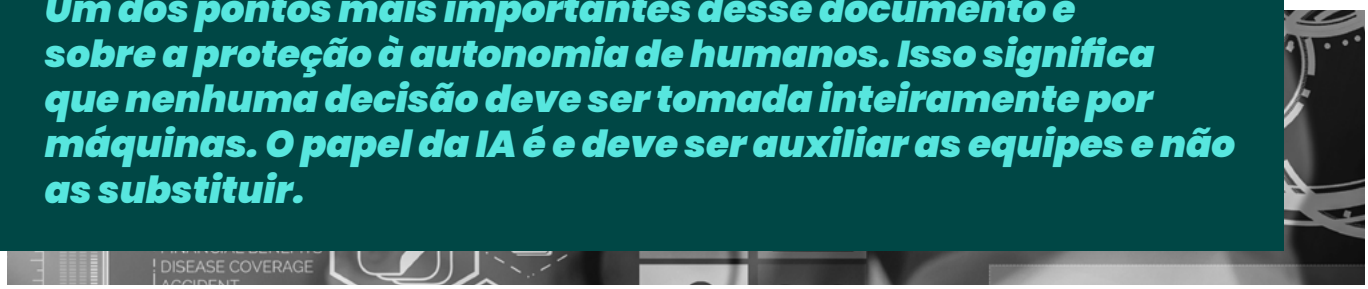
O big data é a principal ferramenta que permite otimizar o uso de dados em prol da medicina, permitindo o aprendizado sobre o comportamento de grupos, de consumo e de hábitos. A análise de uma grande quantidade de dados de maneira estratégica, por meio de *machine learning* e *data analytics*, possibilita a tomada de decisão mais assertiva.

INTELIGÊNCIA DE DADOS NA ÁREA DA SAÚDE: PARA ONDE VAMOS?

Ainda há um longo caminho a ser traçado no uso da inteligência de dados no setor de saúde, mas os avanços já são sensíveis. As principais instituições já apostam em sistemas para otimizar a gestão do negócio e apoiar os pesquisadores no desenvolvimento de novos produtos e tratamentos. Isso se torna possível porque reunir e destacar as informações mais importantes para determinado objetivo é um processo muito mais rápido com a IA.

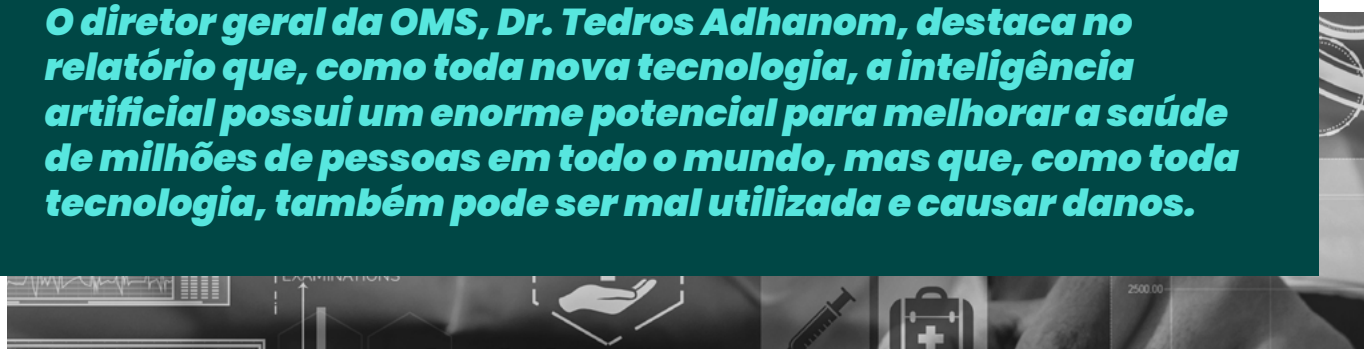
O assunto está tão em pauta que a Organização Mundial de Saúde (OMS)[1] divulgou em junho deste ano um guia sobre "Ética e governança da inteligência artificial para a saúde", que tem como objetivo principal indicar as diretrizes para o uso e análise corretos dos dados no setor, inclusive do ponto de vista de segurança das informações.

Um dos pontos mais importantes desse documento é sobre a proteção à autonomia de humanos. Isso significa que nenhuma decisão deve ser tomada inteiramente por máquinas. O papel da IA é e deve ser auxiliar as equipes e não as substituir.

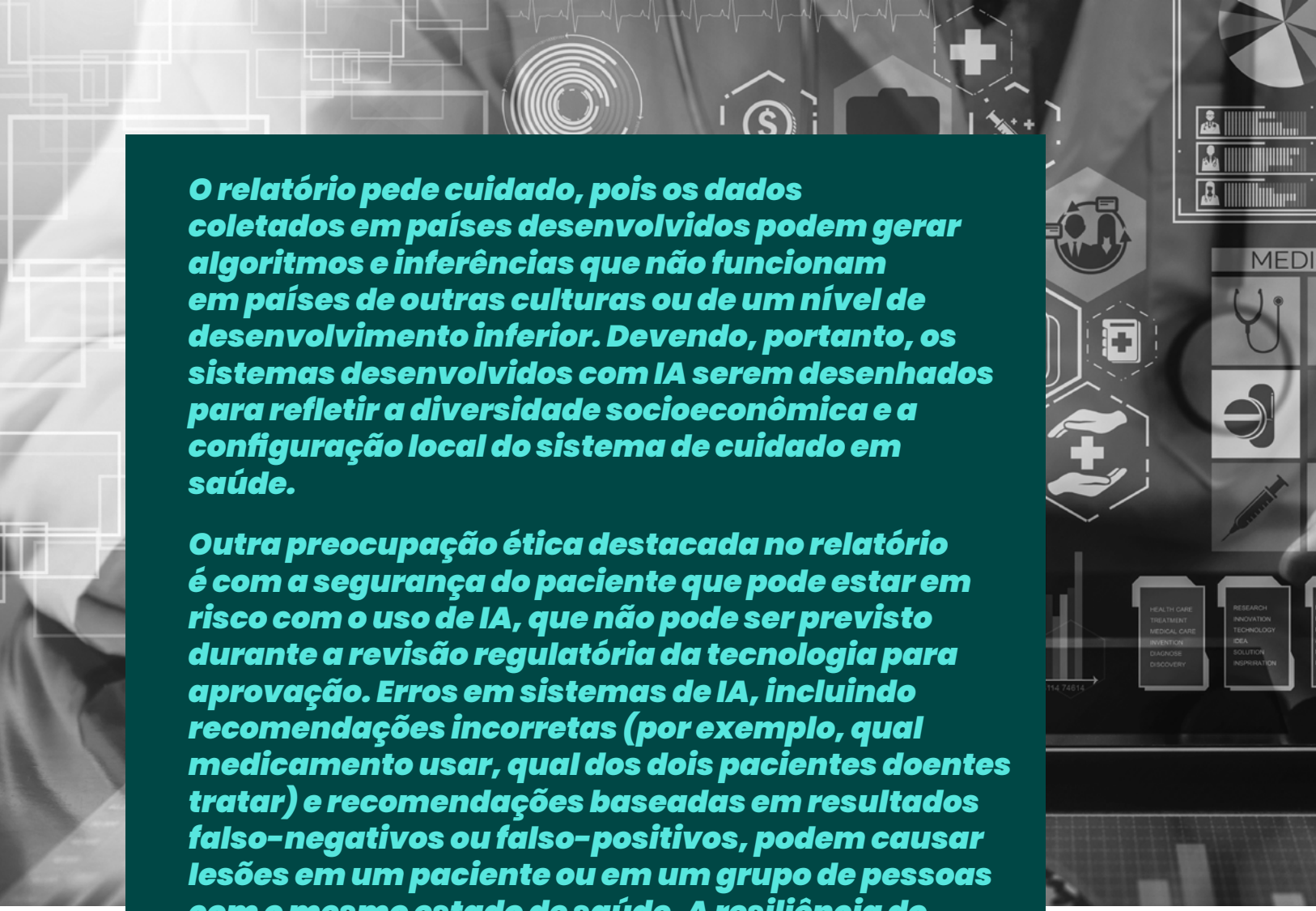


Talvez esse seja um dos principais desafios: educar os profissionais do setor sobre a importância de utilizar as soluções tecnológicas a favor da sua rotina de trabalho. Aos poucos, essa realidade está mudando, mas a falta de familiaridade com as ferramentas e entender a forma correta de analisar os dados ainda são pontos de aprendizagem a serem melhorados no setor.

O diretor geral da OMS, Dr. Tedros Adhanom, destaca no relatório que, como toda nova tecnologia, a inteligência artificial possui um enorme potencial para melhorar a saúde de milhões de pessoas em todo o mundo, mas que, como toda tecnologia, também pode ser mal utilizada e causar danos.



O alerta do Dr. Adhanom se refere aos desafios e riscos do uso desta tecnologia, incluindo coleta e uso antiético de dados de saúde; preconceitos codificados em algoritmos e riscos da inteligência artificial para a segurança do paciente, cibersegurança e meio ambiente.



O relatório pede cuidado, pois os dados coletados em países desenvolvidos podem gerar algoritmos e inferências que não funcionam em países de outras culturas ou de um nível de desenvolvimento inferior. Devendo, portanto, os sistemas desenvolvidos com IA serem desenhados para refletir a diversidade socioeconômica e a configuração local do sistema de cuidado em saúde.

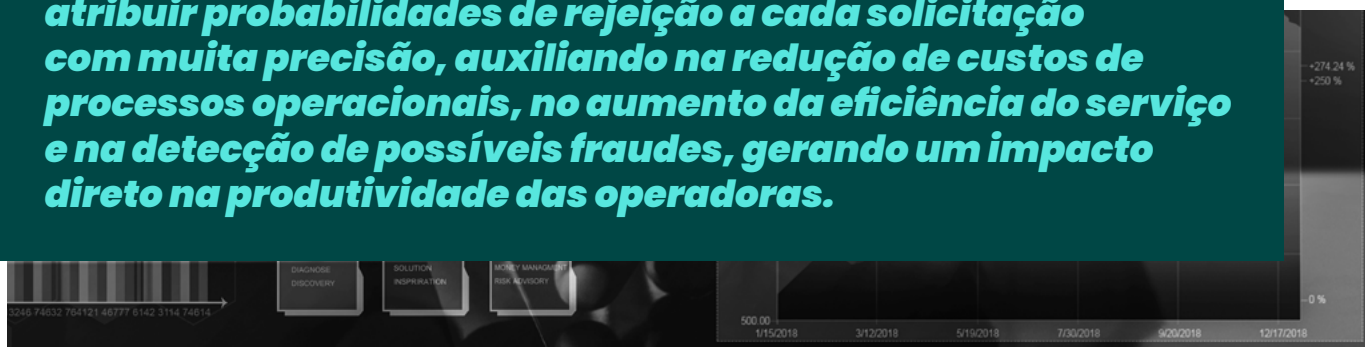
Outra preocupação ética destacada no relatório é com a segurança do paciente que pode estar em risco com o uso de IA, que não pode ser previsto durante a revisão regulatória da tecnologia para aprovação. Erros em sistemas de IA, incluindo recomendações incorretas (por exemplo, qual medicamento usar, qual dos dois pacientes doentes tratar) e recomendações baseadas em resultados falso-negativos ou falso-positivos, podem causar lesões em um paciente ou em um grupo de pessoas com o mesmo estado de saúde. A resiliência do modelo, ou o desempenho de uma tecnologia de IA ao longo do tempo, é um risco relacionado.

Os prestadores de cuidados de saúde também cometem erros de julgamento e outros erros humanos, mas o risco com a IA é que, tal erro, se corrigido em um algoritmo, pode causar danos irreparáveis a milhares de pessoas em um curto espaço de tempo se a tecnologia for amplamente utilizada (159). Além disso, a carga psicológica e o estresse de tais erros são suportados pelos fornecedores que operam essas tecnologias.

Por mais que estas preocupações sejam válidas, também é preciso se ressaltar que as novas legislações e investimentos em desenvolvimento e segurança garantem ótimos resultados da inteligência artificial na saúde em todo o mundo. Em alguns países desenvolvidos a inteligência artificial já é usada para melhorar a velocidade e a precisão do diagnóstico e da triagem de doenças; para a produtividade de todos os setores de atendimento; para auxiliar no atendimento clínico; fortalecer a pesquisa em saúde e o desenvolvimento de medicamentos e apoiar diversas intervenções de saúde pública, como vigilância de doenças, resposta a surtos e gestão de sistemas de saúde.

Mas aqui no Brasil, a IA aplicada no setor de saúde também é realidade. Hoje por exemplo ela já é usada para auxiliar o *compliance* das operadoras de planos de saúde na análise e aprovação de procedimentos médicos, exames e cirurgias de forma automática.

A partir do cruzamento de dados do paciente, é possível atribuir probabilidades de rejeição a cada solicitação com muita precisão, auxiliando na redução de custos de processos operacionais, no aumento da eficiência do serviço e na detecção de possíveis fraudes, gerando um impacto direto na produtividade das operadoras.



O paciente nem vai perceber, mas certamente será atendido mais rapidamente com este processo. Além do ganho em agilidade nas aprovações de procedimentos e exames, também podemos destacar a segurança em relação à eficiência da inteligência artificial – na TOTVS, a assertividade média alcançada pela nossa IA chega a 85%, ou seja, em 85% das análises, a decisão apontada pela máquina foi a mesma que a do médico auditor.

INTELIGÊNCIA DE DADOS NA ÁREA DA SAÚDE: NA PRÁTICA, O QUE MUDA?

Mas, na prática, o que muda nos processos de saúde de criação, estudo e tomadas de decisão com o uso da inteligência de dados? Certamente a velocidade e a qualidade com que os dados são pesquisados, reunidos e analisados. Em um tempo muito menor, as equipes têm acesso às informações que, com esforço apenas humano, talvez nem conseguissem descobrir. Desta forma, pesquisadores ou gestores têm mais e melhores informações para alcançar seus objetivos.

É fato, entretanto, que os benefícios da inteligência de dados para o segmento de saúde chegaram para ficar e são uma realidade. Desenvolver produtos, novos medicamentos e tratamentos por meio da IA já faz parte da rotina de pesquisadores ao redor do mundo, inclusive do Brasil.

Para as instituições de saúde as melhorias também são inúmeras. Analisar as informações compactadas por *machine learning* pode auxiliar na melhor gestão de recursos, humanos e de insumos médicos; na redução de custos operacionais; no melhor atendimento ao paciente e, consequentemente, no aumento do faturamento do negócio.

Em conclusão, acredito que não temos que temer a presença e o avanço do uso da tecnologia no campo da saúde. Temos recursos regulatórios seguros e que, até então, tem se mostrado eficientes para garantir seu melhor uso.

É preciso ponderar que a possibilidade de estarmos sempre conectados, de termos os prontuários dos pacientes sendo feitos de forma 100% eletrônica, a telemedicina, equipamentos de última geração, entre muitos outros, representam ganhos consideráveis para o setor - e tendem a avançar ainda mais ano a ano.

Olhando um pouco mais para o futuro da medicina, já se vislumbra uma tendência da quebra do paradigma de apenas ter foco em resolver as disfunções de saúde já existentes, passando a ter o foco muito maior na medicina preventiva. Com isso, o digital e a inteligência artificial ganham ainda mais importância na ajuda do monitoramento e uso massivo de dados para prever acontecimentos em grupo ou, principalmente, individualizados.

Quanto mais tecnológica for a medicina, melhor será nossa qualidade e expectativa de vida.

Rogério Pires

Rogério Pires assumiu o cargo de diretor de Healthcare na TOTVS em 2017. Com vasta experiência no segmento de saúde, atua no gerenciamento de equipes de desenvolvimento de sistemas e está à frente das operações do segmento.

Sua trajetória e conhecimento estão pautados nos mais de 20 anos atuando no segmento de tecnologia e Health, passando por grandes empresas como GE, Pixeon e UOL.

Formado em Ciência da Computação pela Pontifícia Universidade Católica de Minas Gerais, possui MBA e é mestre em Engenharia da Computação.

NOTAS E REFERÊNCIAS

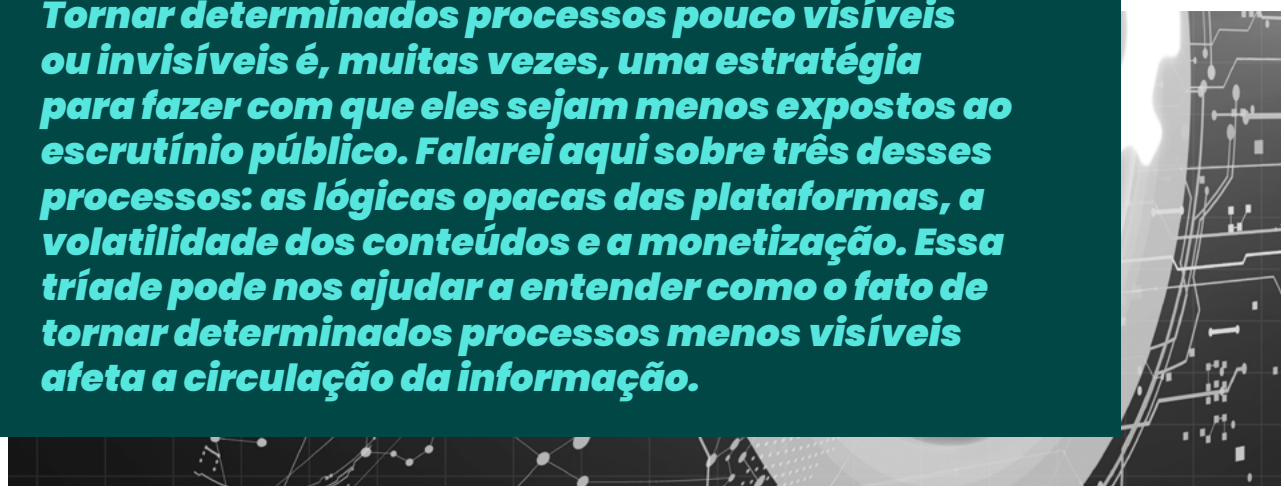
1 https://www.who.int/publications/i/item/9789240029200

doi.org/10.52959/2021535414

INVISIBILIZAÇÃO COMO ESTRATÉGIA: COMO A DESINFORMAÇÃO PODE SE ESCONDER NOS CAMINHOS TECNOLÓGICOS?

Nina Santos

Tornar determinados processos pouco visíveis ou invisíveis é, muitas vezes, uma estratégia para fazer com que eles sejam menos expostos ao escrutínio público. Falarei aqui sobre três desses processos: as lógicas opacas das plataformas, a volatilidade dos conteúdos e a monetização. Essa tríade pode nos ajudar a entender como o fato de tornar determinados processos menos visíveis afeta a circulação da informação.

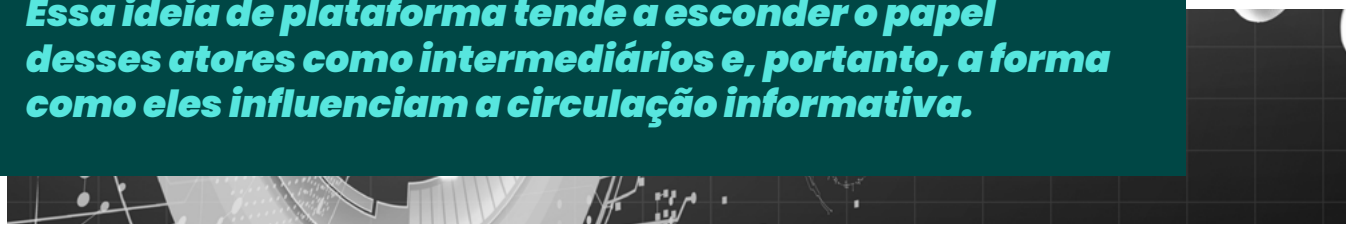


Comecemos por uma discussão sobre a ideia de plataforma. Ela e suas variações, como plataformizado, plataformização, de-plataformização, são alguns dos termos que frequentemente ouvimos nos debates sobre comunicação digital.

A palavra plataforma vem do Francês, 'plate-forme', forma plana. Esse é o imaginário que as plataformas desejam construir sobre si próprias, como espaços "abertos, neutros e com arranjos igualitários, que prometem suporte para quem fica sobre elas", como diz Gillespie (Gillespie, 2010, p. 350). Pois é exatamente questionando o que se esconde por trás dessa ideia que precisamos começar.

Imagem: AdobeStock.com

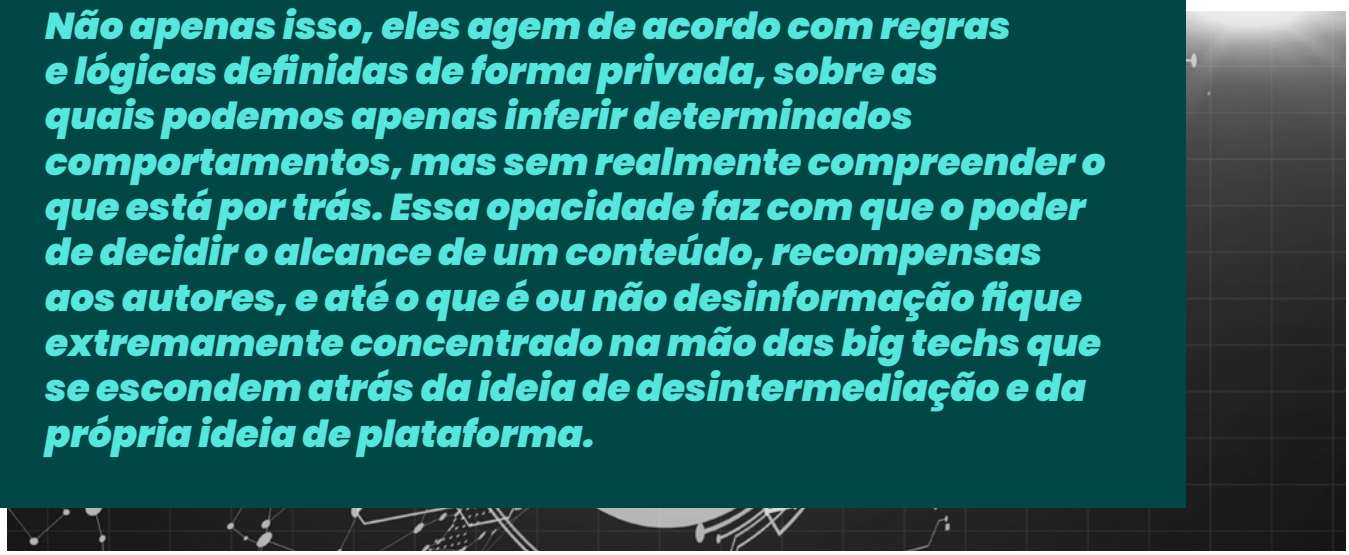
Essa ideia de plataforma tende a esconder o papel desses atores como intermediários e, portanto, a forma como eles influenciam a circulação informativa.



Daí os discursos sobre uma suposta desintermediação proporcionada pela internet, em que haveria uma comunicação mais direta do que antes. Mas não seriam essas plataformas, suas lógicas de organização e funcionamento, seus interesses comerciais e sociais também intermediadores?

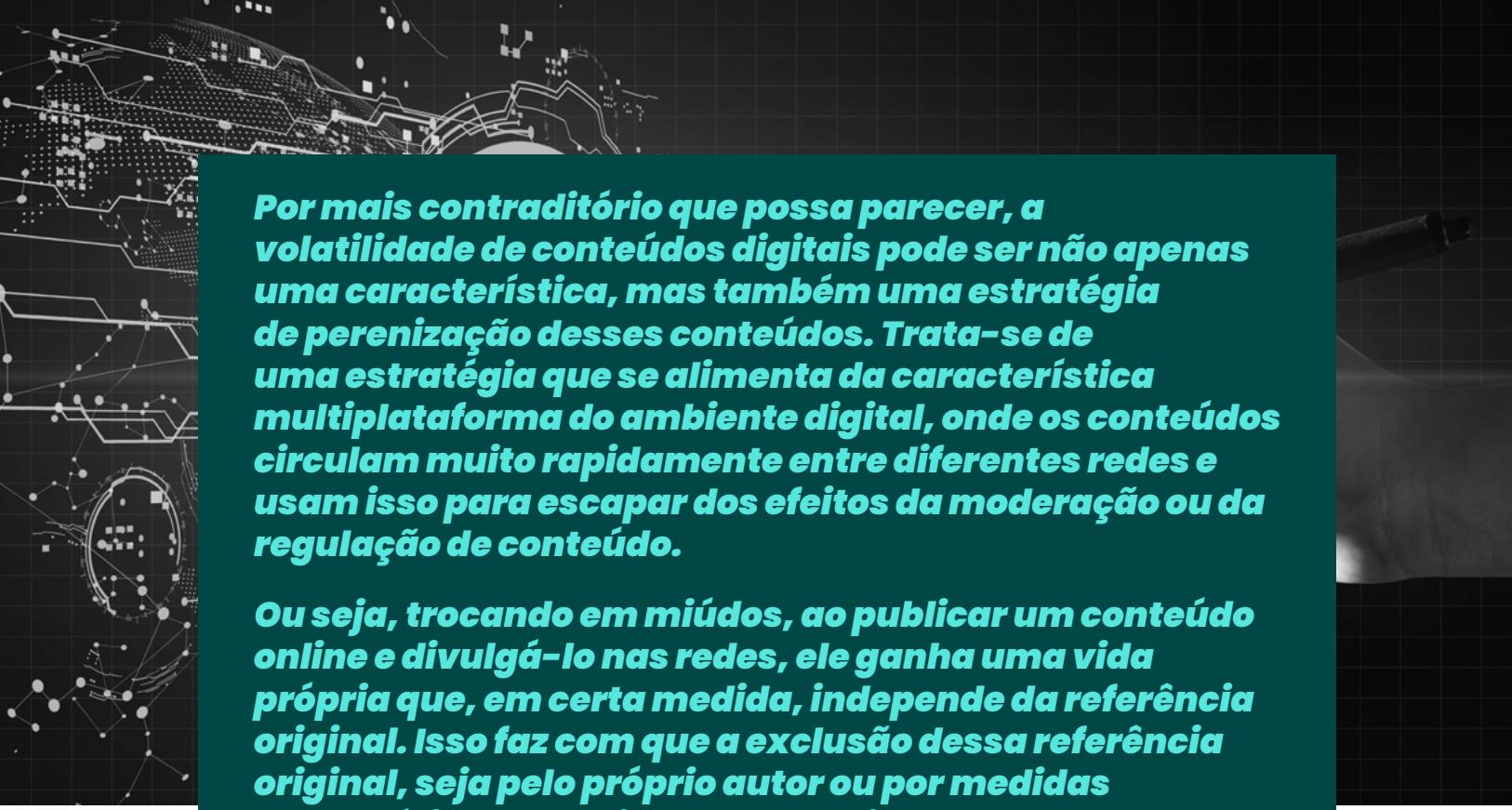
Portanto, o que temos, na verdade, é uma cadeia de mediações mais ampla, mais complexa e menos visível do que tínhamos antes. Se antes tínhamos o jornalista como mediador, visível, criticável, agora temos mais níveis e as plataformas têm um papel central nisso. Esses novos mediadores produzem uma fragmentação informativa que tem consequências de vários tipos para o que Hannah Arendt (1958) chama de mundo comum, aquele conhecido e partilhado pelos membros de uma comunidade.

Não apenas isso, eles agem de acordo com regras e lógicas definidas de forma privada, sobre as quais podemos apenas inferir determinados comportamentos, mas sem realmente compreender o que está por trás. Essa opacidade faz com que o poder de decidir o alcance de um conteúdo, recompensas aos autores, e até o que é ou não desinformação fique extremamente concentrado na mão das big techs que se escondem atrás da ideia de desintermediação e da própria ideia de plataforma.



Bom, passamos então para o nosso segundo ponto, que tem a ver com temporalidade.

O argumento de que o ambiente digital torna os processos sociais mais voláteis funciona para explicar muitos fenômenos, da emergência de mobilizações sociais à eleição de governantes incidentais, como defende Sérgio Abranches (2020). Existe um elemento volátil que é mesmo inerente à velocidade da própria rede, mas precisamos analisar também possíveis usos dessa característica.



Por mais contraditório que possa parecer, a volatilidade de conteúdos digitais pode ser não apenas uma característica, mas também uma estratégia de perenização desses conteúdos. Trata-se de uma estratégia que se alimenta da característica multiplataforma do ambiente digital, onde os conteúdos circulam muito rapidamente entre diferentes redes e usam isso para escapar dos efeitos da moderação ou da regulação de conteúdo.

Ou seja, trocando em miúdos, ao publicar um conteúdo online e divulgá-lo nas redes, ele ganha uma vida própria que, em certa medida, independe da referência original. Isso faz com que a exclusão dessa referência original, seja pelo próprio autor ou por medidas regulatórias, tenha impacto restrito.

Uma pesquisa feita por Marco Toledo Bastos e Dan Mercea (2019), na Universidade de Londres, mostrou que 29% dos *links* usados em *tweets* durante a campanha do Brexit desapareceram depois do referendo. Segundo eles, os *links* levavam a contas do Twitter que tinham sido removidas, bloqueadas ou apagadas ou a sites que não existiam mais.

Com base nesse e em outros estudos, Bastos e colegas (2021) vão propor um modelo de mensuração de informações de baixa qualidade. Um dos elementos desse modelo é justamente a sua duração, tendo em vista que, segundo eles, informações de baixa qualidade circulando em ambientes digitais são marcadas por uma pequena vida útil.

Aqui, no Brasil, em uma pesquisa ainda em desenvolvimento da qual participo junto com Viktor Chagas e Juliana Marinho, identificamos que 42% dos *links* compartilhados em grupos bolsonaristas no WhatsApp sumiram em um ano. Todos esses conteúdos, no entanto, estão longe de ter desaparecido das redes.

Uma parte da pesquisa consistiu em demonstrar a relação entre a data de publicação de vídeos do Youtube e a data em que eles passam a circular em grupos do WhatsApp bolsonarista. O que encontramos é que a grande maioria destes conteúdos já nasce multiplataforma, ou seja, assim que publicados em uma rede, já estão circulando em outra. É o pesquisador Viktor Chagas vem chamando de 'conteúdo real-time'.

Em se tratando de conteúdos bolsonaristas, não apenas eles são prontamente compartilhados, como tendem a ser compartilhados durante mais tempo do que em outros públicos. Um relatório recente, feito por pesquisadores do DAPP (Piaia et al., 2021), mostrou que *links* que circulam no *cluster* bolsonaristas no Twitter podem durar até 250 horas, enquanto em outros grupos essa medida se restringe a 100 horas.

Ou seja, conteúdos de baixa qualidade tendem a ser publicados e compartilhados rápida e longamente, o que faz com que a existência do conteúdo original seja muito menos relevante. Uma das consequências disso é que todas as medidas de moderação que digam respeito a apenas uma plataforma – como o Youtube tirar esses vídeos do ar – tenham um efeito importante, porém limitado dada a dimensão do fenômeno.

Chegamos então ao último ponto que gostaria de destacar. Ele diz respeito aos processos de monetização do conteúdo digital. Esse é um tema do qual se fala muito no mundo da publicidade, dos *influencers*, da construção de negócios e projetos digitais, mas que me parece bastante subexplorado no debate público.

O debate sobre desinformação é muito centrado na circulação orgânica do conteúdo, e isso é mesmo muito importante. Ou seja, falamos muito sobre as pessoas que repassam fake news ou do presidente que fala fake news em rede nacional. Mas o papel da monetização das redes é absolutamente central nesse processo.

Existe um impacto econômico da desinformação que ainda temos dificuldade de medir, mas que alimenta operações organizadas e estruturadas de desinformação. Um desses impactos vem de uma lógica criada pelas próprias plataformas, que é a de pagar produtores de conteúdo pela sua produção a partir da audiência alcançada.

No Youtube, por exemplo, estima-se que, em média, o produtor de conteúdo receba um centavo por visualização. Quando pensamos na casa dos milhões de *views* que frequentemente vídeos com informações falsas atingem, essa receita deixa de ser desprezível.

Ou seja, há um sistema das plataformas que remunera conteúdos que conseguem atrair a atenção das pessoas e, portanto, fazer com que elas fiquem mais tempo nas redes. E a desinformação tem conseguido se beneficiar bastante desse mecanismo.

Inclusive, recentemente, vimos o que acredito que seja a primeira decisão judicial no Brasil sobre desmonetização de conteúdos. O TSE decidiu que as mídias sociais deveriam suspender a monetização e os mecanismos de recomendação de conteúdos de contas que estão propagando informações falsas sobre eleições.

Ações de desmonetização já estavam sendo feitas, mas por decisões internas das plataformas ou por pressão da sociedade civil. No Brasil, esse processo ganhou muita atenção com as atividades do Sleeping Giants, por exemplo. A recente decisão do TSE mostra a importância de que essa lógica de funcionamento interna das plataformas seja compreendida por instâncias-chave no regime democrático, como aquelas do Judiciário.

Bom, certamente, esses três pontos não são exaustivos, mas espero que eles nos ajudem a entender como se criam caminhos dentro dessas estruturas tecnológicas e como eles podem servir para que a desinformação seja um problema do tamanho que é hoje.

O debate sobre estratégias tecnológicas da desinformação tem uma tarefa inicial, que é a de olhar por trás das cortinas, dos tapetes, das portas fechadas e entender o que realmente constrói esse espaço que, muitas vezes, tendemos a naturalizar.

Nina Santos

Nina Santos é pós-doutoranda no Instituto Nacional de Ciência e Tecnologia em Democracia Digital e pesquisadora associada do Centre d'Analyse et de Recherche Interdisciplinaires sur les Médias (Université Paris II). Foi pesquisadora visitante no Center of Advanced Internet Research (CAIS - Alemanha, 2020) e no grupo Social Movements in the Global Age, na Université de Louvain-la-Neuve (SMAG - Bélgica, 2018). Sua tese de doutorado, defendida na Université Paris II, foi premiada com o Prix de thèse da instituição e indicada ao Prix de la Chancellerie des Universités de Paris.

Imagem: AdobeStock.com

NOTAS E REFERÊNCIAS

Abranches, S. (2020). O tempo dos governantes incidentais. São Paulo: Companhia das Letras.

Arendt, H. (1958). The Human Condition. Chicago & London: The University of Chicago Press.

Bastos, M. T., & Mercea, D. (2019). The Brexit botnet and user-generated hyperpartisan news. Social Science Computer Review, 37(1), 38-54. https://doi.org/10.1177/0894439317734157

Bastos, M., Walker, S., & Simeone, M. (2021). The IMPED Model: Detecting Low-Quality Information in Social Media. American Behavioral Scientist. https://doi.org/10.1177/0002764221989776

Gillespie, T. (2010). The politics of "platforms". New Media and Society, 12(3), 347–364. https://doi.org/10.1177/1461444809342738

Piaia, V. et al. (2021). (Pseudo)Ciência e esfera pública. São Paulo.

doi.org/10.52959/2021535415

COMO AS *FAKE NEWS* AFETAM A CONFIANÇA NA ECONOMIA DIGITAL? COMO EVITÁ-LAS?

Nilson de Oliveira

"Conhecerás a mentira, e a mentira te aprisionará." A frase é do presidente do Tribunal Superior Eleitoral (TSE) e ministro do Supremo Tribunal Federal (STF), Luiz Roberto Barroso, em pronunciamento no dia 9 de setembro de 2021. Barroso respondia ao presidente da República, Jair Bolsonaro, que, dois dias antes, tinha ocupado palanque na Avenida Paulista, em São Paulo, para, entre ataques ao STF, reafirmar acusações nunca comprovadas de que o sistema eleitoral com o uso de urnas eletrônicas é fraudulento.

Desde que foi eleito, em 2018, Bolsonaro e parte expressiva de sua base política insistem na narrativa de que o modelo informatizado de coleta de votos, em vigor nos últimos 25 anos, é facilmente adulterado. Por mais que se mostre que o sistema tem várias camadas de segurança, que não é possível o *hackeamento* das urnas, que todo o processo de coleta de informações e contabilização dos votos é auditável pelos partidos políticos e representantes da sociedade civil, o presidente continua a afirmar que a forma mais segura de garantir lisura na disputa eleitoral é o uso de voto impresso e sua contagem manual.

Os bolsonaristas tentaram, por meio de projeto de emenda constitucional, mudar a legislação eleitoral para promover o evidente retrocesso. Na Câmara dos Deputados, precisavam obter o apoio de 308 dos 513 parlamentares para saírem vitoriosos. Em 10 de agosto, o placar do plenário registrou 229 favoráveis e 218 contrários. A proposta foi arquivada. Vários deputados alinhados com o presidente se opuseram à volta ao passado maculado por inúmeros casos de irregularidades que deturpavam o caráter democrático do voto.

Mesmo neste contexto, de ampla rejeição às suas teses, no palanque da Paulista, Bolsonaro afirmou: "A alma da democracia é o voto, não podemos admitir um sistema eleitoral que não oferece qualquer segurança por ocasião das eleições. E não é uma pessoa do TSE que vai nos dizer que este processo é seguro, porque não é. Um ministro do TSE, usando sua caneta, usar sua caneta e desmonetizar páginas que criticam esse tipo de votação. Queremos voto auditável e contagem pública dos votos".

E diante dos cerca de 125 mil simpatizantes que o ouviam atentamente, muitos deles com cartazes em defesa do voto impresso, o presidente asseverou: "Não posso participar de uma farsa como essa, patrocinada pelo presidente do Tribunal Superior Eleitoral".

A observação desses fatos remete a uma parábola judaica. Certo dia, a Mentira e a Verdade se encontraram. A Mentira disse para a Verdade: "Bom dia, dona Verdade!". E a Verdade foi conferir se realmente era um bom dia. Olhou para o alto, não viu nuvens de chuva, vários pássaros cantavam e, vendo que realmente era um bom dia, respondeu para a Mentira: "Bom dia, dona Mentira!". "Está muito calor hoje...", comentou a Mentira. E a Verdade, vendo que a Mentira falava a verdade, relaxou. A Mentira, então, convidou a Verdade para se banhar no rio. Despiu-se de suas vestes, pulou na água e falou: "Venha, dona Verdade. A água está uma delícia". E, assim que a Verdade, sem duvidar da Mentira, tirou suas vestes e mergulhou, a Mentira saiu da água, vestiu-se com as roupas da Verdade e foi embora. A Verdade, por sua vez, recusou-se a vestir-se com as roupas da Mentira e, por não ter do que se envergonhar, saiu nua a caminhar na rua. Aos olhos das pessoas, porém, era mais fácil aceitar a mentira vestida de verdade, do que a verdade nua e crua.

A Mentira travestida de Verdade aprisiona aquele que fixa seu olhar nela, como bem disse o ministro Barroso. Aprisiona porque cria um vínculo de confiança com o emissor da mensagem que deliberadamente utiliza argumentos falaciosos e ficcionais para o exercício do poder. Poder, aqui, entenda-se, não é apenas uma referência à política, mas ao centro gravitacional de um relacionamento.

Um parêntese importante. Observe, caro leitor, que este artigo não usará a tão propalada expressão *fake news* para designar informações falsas, desinformação ou mentira. A única licença é o título, para localizar o texto no debate do assunto. E isso porque, como afirma a jornalista Cristina Tardáguila, fundadora da Agência Lupa, primeira agência de notícias especializada em *fact-checking* no Brasil, "se algo é *fake* (falso), não é *news* (notícia). O paradoxo contido na expressão reluz à distância"[1].

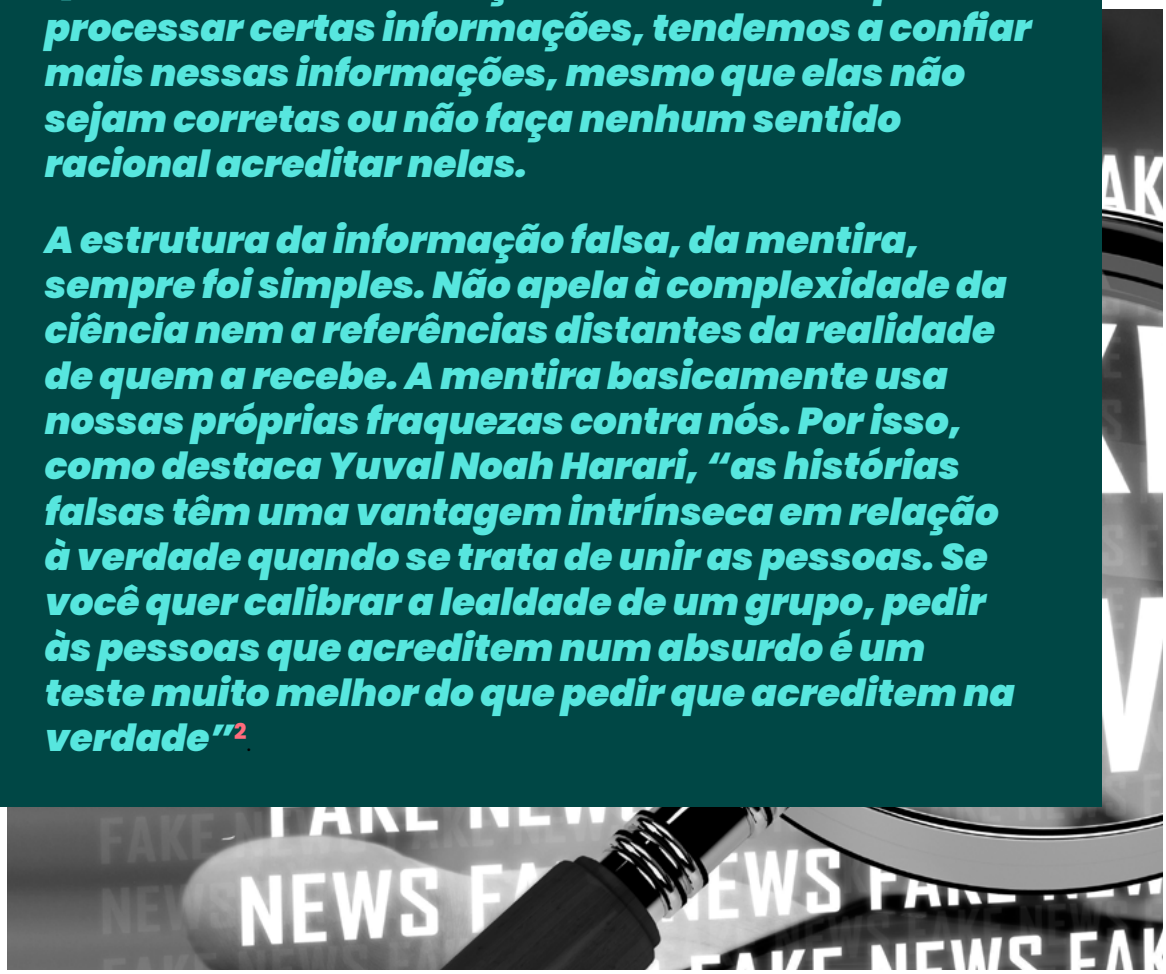
A psicologia cognitiva conceitua como "fluência de processamento" a sensação de facilidade (ou dificuldade) que temos quando estamos processando algum tipo de informação. Várias pesquisas têm mostrado que a fluência de processamento está diretamente relacionada com julgamentos que fazemos das coisas ao nosso redor.

O professor e pesquisador no Departamento de Psicologia da Universidade do Alabama (EUA), André L. Souza, do blog Cognando, dá um bom exemplo para entender melhor o conceito: "muitas pessoas dizem que odeiam a língua alemã pelo simples fato de que as palavras germânicas são muito grandes (*erfrischungsgetränk*, refrigerante em português, por exemplo). Para um falante acostumado com o tamanho médio das palavras portuguesas, termos grandes podem ser assustadores (e difíceis de processar). A simples sensação de que o idioma alemão é difícil de ser processado faz com que pessoas tenham a sensação de que não gostam da língua".

Com o sentimento de confiança acontece a mesma coisa.

Quando temos a sensação de "facilidade" para processar certas informações, tendemos a confiar mais nessas informações, mesmo que elas não sejam corretas ou não faça nenhum sentido racional acreditar nelas.

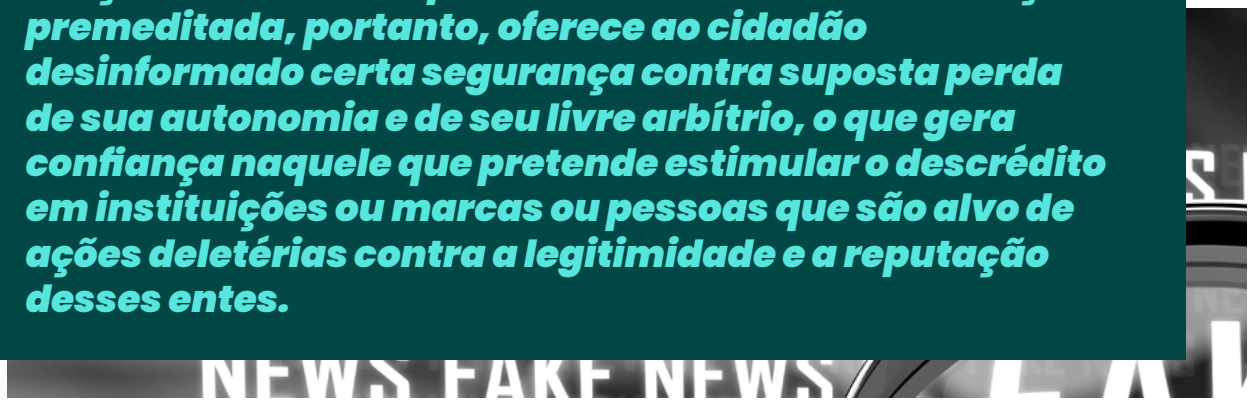
A estrutura da informação falsa, da mentira, sempre foi simples. Não apela à complexidade da ciência nem a referências distantes da realidade de quem a recebe. A mentira basicamente usa nossas próprias fraquezas contra nós. Por isso, como destaca Yuval Noah Harari, "as histórias falsas têm uma vantagem intrínseca em relação à verdade quando se trata de unir as pessoas. Se você quer calibrar a lealdade de um grupo, pedir às pessoas que acreditem num absurdo é um teste muito melhor do que pedir que acreditem na verdade"[2].



Voltemos ao caso da urna eletrônica x voto impresso. Todo e qualquer sistema que envolva algoritmos é tido como instransponível para a grande maioria das pessoas. A não ser os especialistas e os desenvolvedores, poucos conseguem relatar como as informações são processadas, ainda mais quando envolve um volume astronômico de dados.

Assim, quando alguém apela à fórmula papel + caneta + contagem manual = eleição sem fraude, a fluência do processamento da mensagem é mais fácil, mais tangível, o que estimula a percepção de não manipulação. Em uma sociedade, como a contemporânea, cuja base tecnológica intensificou a circulação de informações, cria-se a partir da equação citada, por exemplo, o solo fértil para uma narrativa que sustenta as teorias da conspiração.

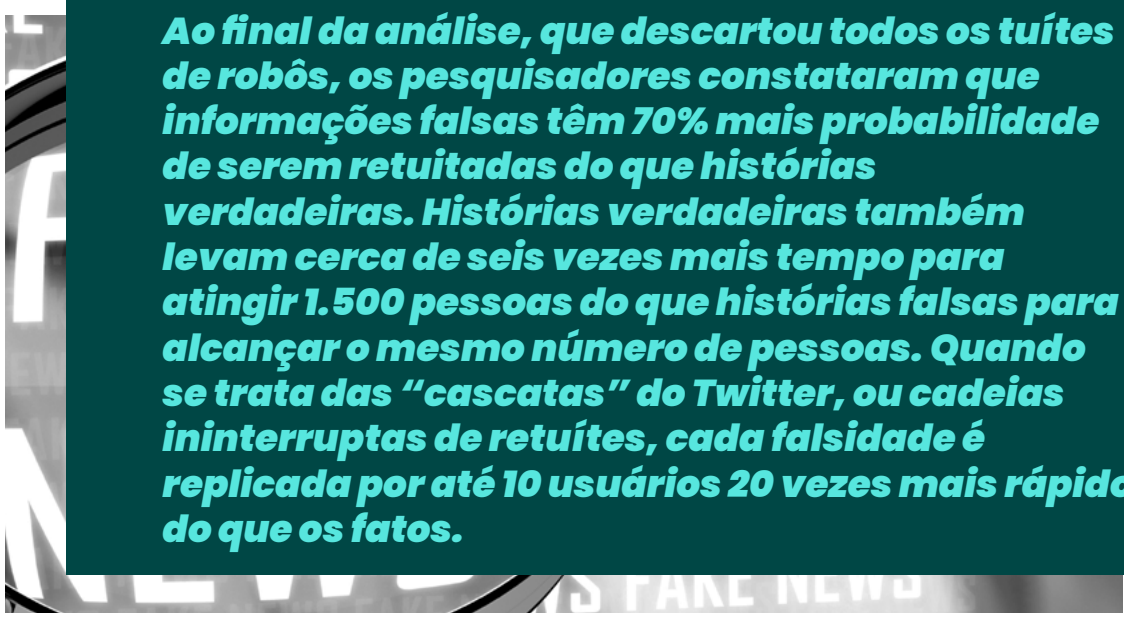
Graças à fluência do processamento, a desinformação premeditada, portanto, oferece ao cidadão desinformado certa segurança contra suposta perda de sua autonomia e de seu livre arbítrio, o que gera confiança naquele que pretende estimular o descrédito em instituições ou marcas ou pessoas que são alvo de ações deletérias contra a legitimidade e a reputação desses entes.



Em "Como as Democracias Morrem"[3], os cientistas políticos norte-americanos Steven Levitsky e Daniel Ziblatt descrevem o lento processo de corrosão das instituições democráticas, promovido por um governante legitimado pelo voto. O êxito para o candidato a autocrata se impor é a quebra total da confiança do eleitorado na democracia. E, para isso, ele precisa alimentar sistematicamente a coletânea de histórias falsas, entre outras desconstruções políticas, como enfraquecimento do Judiciário e a contenção da imprensa independente.

Em 2018, a revista *Science* publicou o artigo "The Spread of True and False News Online"[4], de autoria de Soroush Vosoughi, Sinan Aral e Deb Roy, professores e pesquisadores do Massachusetts Institute of Technology (MIT). Com a ajuda do Twitter, o trio rastreou cerca de 126.000 histórias que se espalharam na rede social, postagens que foram tuitadas cumulativamente mais de 4,5 milhões de vezes por cerca de 3 milhões de pessoas, entre os anos de 2006 e 2017.

Ao final da análise, que descartou todos os tuítes de robôs, os pesquisadores constataram que informações falsas têm 70% mais probabilidade de serem retuitadas do que histórias verdadeiras. Histórias verdadeiras também levam cerca de seis vezes mais tempo para atingir 1.500 pessoas do que histórias falsas para alcançar o mesmo número de pessoas. Quando se trata das "cascatas" do Twitter, ou cadeias ininterruptas de retuítes, cada falsidade é replicada por até 10 usuários 20 vezes mais rápido do que os fatos.



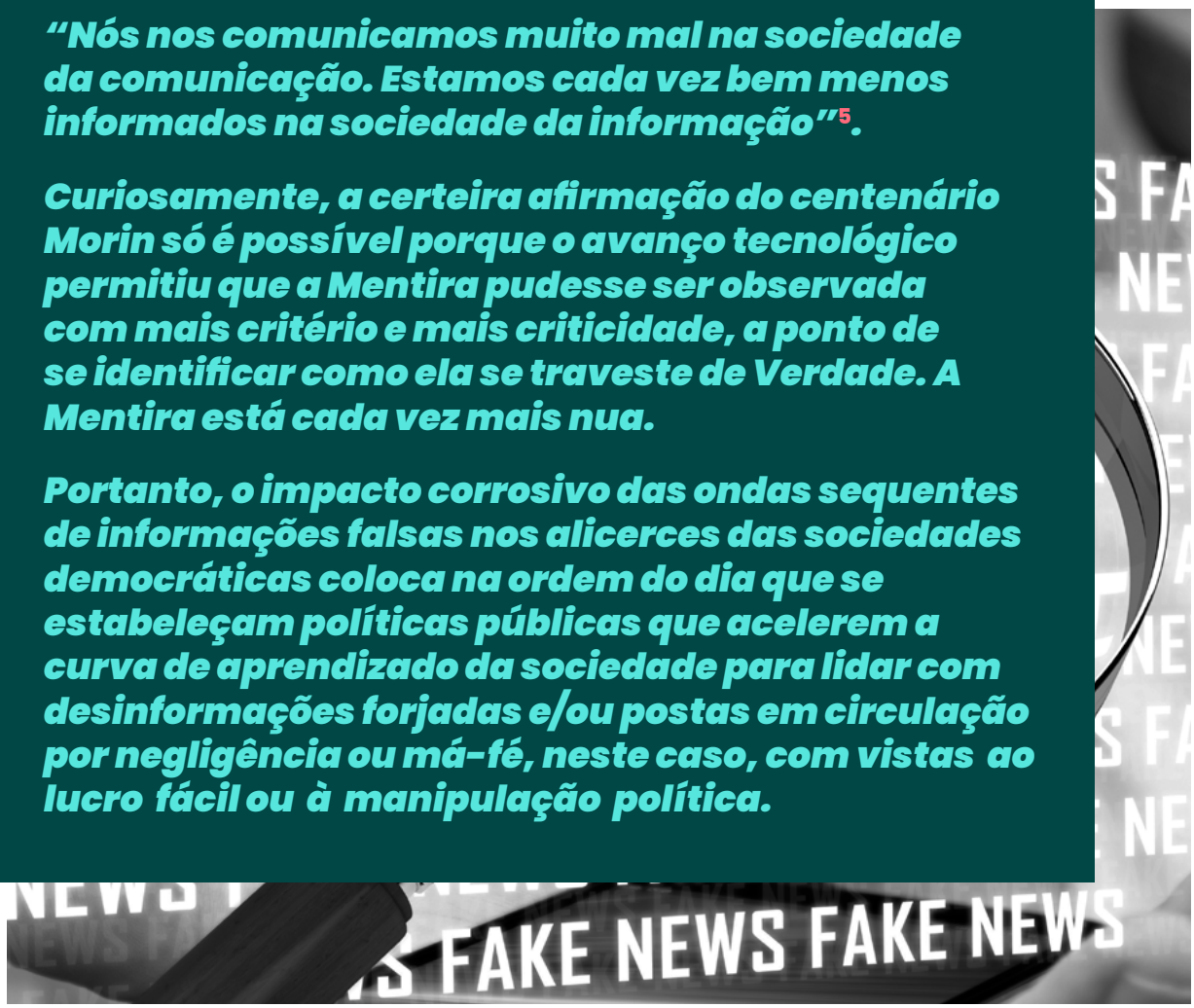
Das 126.000 histórias, a política compreendeu a maior categoria de postagens, com cerca de 45.000, seguida por lendas urbanas, negócios, terrorismo, ciência, entretenimento e desastres naturais. A disseminação de histórias falsas foi mais pronunciada para referências à política do que verificada em outras categorias.

Todo este cenário, que parece um tanto desolador, remete à recente constatação feita pelo filósofo Edgar Morin, em sua conta no Twitter:

"Nós nos comunicamos muito mal na sociedade da comunicação. Estamos cada vez bem menos informados na sociedade da informação"[5].

Curiosamente, a certeira afirmação do centenário Morin só é possível porque o avanço tecnológico permitiu que a Mentira pudesse ser observada com mais critério e mais criticidade, a ponto de se identificar como ela se traveste de Verdade. A Mentira está cada vez mais nua.

Portanto, o impacto corrosivo das ondas sequentes de informações falsas nos alicerces das sociedades democráticas coloca na ordem do dia que se estabeleçam políticas públicas que acelerem a curva de aprendizado da sociedade para lidar com desinformações forjadas e/ou postas em circulação por negligência ou má-fé, neste caso, com vistas ao lucro fácil ou à manipulação política.



O mais eficiente anteparo contra a desinformação e a mentira e a melhor proteção da veracidade passa necessariamente pelas escolas. A educação básica de qualidade continua a ser o processo mais virtuoso "para estimular o discernimento na escolha das leituras e um saudável ceticismo na forma de absorvê-las"[6].

No Brasil, por incrível que pareça, desde 2017, as condições já estão oferecidas pela Base Nacional Comum Curricular (BNCC), que prevê o desenvolvimento do pensamento crítico de mensagens da mídia em escolas.

Não é preciso nenhum édito para que a educação midiática esteja nas salas de aulas das escolas e das universidades. Para ficar mais claro, a BNCC estabelece que entre as competências a serem desenvolvidas nos alunos está a capacidade de "argumentar com base em fatos, dados e informações confiáveis, para formular, negociar e defender ideias, pontos de vista e decisões comuns que respeitem e promovam os direitos humanos, a consciência socioambiental e o consumo responsável"[7].

Se isso for levado a sério pelas autoridades educacionais federais, estaduais e municipais, o ciclo virtuoso fará com que cursos universitários ofereçam a seus alunos aulas de *media literacy* ou alfabetização midiática, com ampla contribuição das plataformas e empresas de tecnologia.

Se a sociedade brasileira e suas elites estiverem realmente desejosas de colocar o país numa rota de avanço civilizatório, as cartas estão na mesa.

Nilson de Oliveira

Sócio da Torabit, uma das principais plataformas brasileiras de monitoramento digital, é sociólogo formado pela Faculdade de Filosofia, Letras e Ciências Humanas da Universidade de São Paulo (USP), com MBA em Gestão de Negócios Socioambientais (Ceats-USP/Ipe). Neste ano, ingressou no MBA em Data Science e Analytics, da USP Esalq. Chegou a cursar três anos de engenharia eletrônica na Faculdade de Engenharia Industrial (FEI) e abandonou o bacharelado em Física, na USP, no penúltimo semestre. Por 18 anos, foi jornalista da Folha de S.Paulo, onde atuou como editor e coordenador. Após deixar a Redação do jornal, tornou-se consultor na área de comunicação corporativa para auxiliar as empresas e outras organizações a cuidarem de suas reputações, lidarem com situações críticas que podem ameaçar seus negócios ou desgastar relacionamentos com públicos estratégicos e a se adequarem à agenda da sustentabilidade. Integrou em 2010 e 2014 a coordenação da comunicação das campanhas da ex-senadora Marina Silva à Presidência da República. A experiência de 2010 propiciou impulsionar uma candidatura, pela primeira vez na política brasileira, com a eficiente sinergia entre as mídias tradicionais e os meios digitais. A disputa eleitoral seguinte foi marcada pelo enfrentamento inédito, até então, de adversários que empregaram suas redes sociais para espalhar fake news. Nas duas oportunidades, contou com a valiosa e prestigiosa parceria de Caio Túlio Costa, uma das principais referências da internet no Brasil.

NOTAS E REFERÊNCIAS

1 Tardáguila, Cristina, "Desinformação/Fact-Checking", in Tempestade Perfeita – Sete Visões da Crise do Jornalismo Profissional, Editora Intrínseca, 2021

2 Harari, Yuval Noah, 21 Lições para o Século 21, Companhia das Letras, 2018

3 Levistisky, Steven & Ziblatt, Daniel, Como as Democracias Morrem, Zahar, 2018

4 Vosoughi, Soroush; Aral, Sinan & Roy, Deb, "The Spread of True and False News Online", in Science, Vol. 359, 2018. Disponível em https://www.science.org/doi/abs/10.1126/science.aap9559, 2018

5 Morin, Edgar, https://twitter.com/edgarmorinparis/status/1431679136146378753?s=21

6 Frias Filho, Otavio, "O que é falso sobre fake news", in "Dossiê Pós-Verdade e Jornalismo", Revista da USP, número 116, Editora da Universidade de São Paulo, 2018. Disponível em https://www.revistas.usp.br/revusp/article/view/146576/140222

7 Base Nacional Comum Curricular (BNCC) - http://basenacionalcomum.mec.gov.br/images/BNCC_EI_EF_110518_versaofinal_site.pdf

doi.org/10.52959/2021535416

QUAL É A ESTRUTURA DE INTERVENÇÃO IDEAL PARA CONTER AS *FAKE NEWS* E REFORÇAR A DEMOCRACIA?

Sascha Meinrath, Steven Mansour, Humza Jilani

Este artigo visa ajudar a forjar um caminho unificado no esforço criticamente importante para conter a informação falsa e reforçar a democracia. Primeiro, são discutidas as ações regulatórias necessárias para lidar com os danos das plataformas de mídia digital. Em seguida, são descritos tais danos, bem como os potenciais espaços para a ação regulatória e legislativa. O capítulo conclui com uma proposta de estrutura de intervenção em cinco níveis, exigindo divulgação e transparência, auditorias algorítmicas, multas por não cumprimento intencional , diminuição da proteção de responsabilidade e processo criminal.

AÇÕES REGULATÓRIAS NECESSÁRIAS PARA LIDAR COM OS DANOS DAS PLATAFORMAS DE MÍDIA DIGITAL

Os reguladores da União Europeia já começaram a averiguar como estabelecer um regime para examinar, auditar e fazer cumprir as violações da privacidade das plataformas de mídia digital[1]. Poderes semelhantes também foram instituídos para permitir a supervisão de outros danos relacionados a essas plataformas. Da mesma forma, as capacidades tecnológicas necessárias para identificar, documentar, rastrear e analisar desinformações estão amplamente disponíveis. As empresas de mídia digital têm usado tais ferramentas para rastrear materiais protegidos por direitos autorais e identificar trabalhos deles derivados por décadas.

Em essência, a funcionalidade necessária para impedir a desinformação já está incorporada aos principais modelos de negócios de muitas empresas de mídia.

Portanto, os esforços regulatórios para conter a desinformação e a informação errada nas mídias sociais deveriam se concentrar em determinar o nível de acesso aos dados e à tecnologia – e o empoderamento legal – necessário para avaliar e informar sobre a natureza, a amplitude e o escopo dos danos observados em todo o cenário das mídias sociais e das plataformas digitais.

Para cumprir esse papel essencial, os reguladores precisarão exercer quatro poderes básicos:

1. Acesso: Acesso abrangente e sem restrições aos dados e metadados (timestamps, algoritmos de conteúdo ativo, originando e disseminando usuários etc.) específicos à informação falsa que está sendo auditada.

2. Auditoria: O estabelecimento de autoridades de auditoria permitindo o estabelecimento de um "limiar de dano" (uma medida quantitativa e qualitativa de exposição de um grupo de usuários ou demografia a conteúdo nocivo que constitui uma violação da lei).

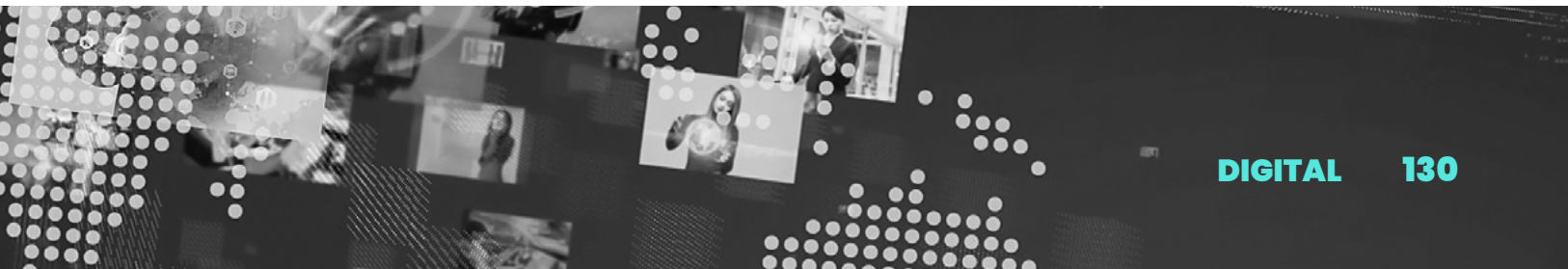
3. Mandatos de implementação: A criação de medidas que as empresas devem implementar – sejam elas de concepção, entrega ou mudanças nos termos de uso – a fim de mitigar os danos reais e potenciais.

4. Intervenção: Intervenções significativas que desincentivam as plataformas de continuar a permitir a propagação de informações errôneas e outros conteúdos prejudiciais.

O primeiro poder é direto – assim como durante uma Avaliação de Impacto na Privacidade (PIA), todos os dados relevantes em torno do conteúdo em questão precisarão ser disponibilizados para auditoria. As auditorias de plataformas de mídia digital são necessárias para ajudar a lidar com a perigosa propagação de desinformação e informação errada. O segundo e o terceiro poderes estão relacionados com a natureza e os objetivos dessas auditorias: De que devem ser compostas e a que devem conduzir? Após o exercício dos três primeiros poderes, o poder final será necessário para garantir a conformidade e a responsabilização das empresas pelas falhas contínuas.

ACESSO E AUDITORIA

A primeira área proposta de foco regulatório requer acesso não apenas ao conteúdo, mas também aos conjuntos de algoritmos, processos decisórios e estruturas pelas quais o conteúdo da plataforma é promovido, rebaixado, censurado, removido e compartilhado (assim como quais partes interessadas internas e externas têm acesso para visualizar, modificar ou manipular esses dados). Ao equipar os reguladores com as informações necessárias para entender como a informação falsa tem se espalhado por uma determinada rede, eles estarão mais bem munidos para enfrentar os episódios atuais e futuros.



A próxima faceta de um regime de auditoria abrangente para plataformas de mídia digital é a investigação dos métodos usados para difundir conteúdos problemáticos (e os concomitantes resultados prejudiciais e deletérios engendrados por sua propagação). Os impactos da disseminação também devem ser examinados – identificando as consequências negativas e os públicos-alvo mais vulneráveis, determinando se a propagação direcionada é intencional ou o subproduto do foco "acidental", avaliando quais são os círculos mais propensos a contribuir para a disseminação de informações errôneas específicas, e examinar se existem "nós" identificáveis que tendem a agir como "multiplicadores de força" para a disseminação de informações falsas. Relacionado a este fim, a Aliança Global para Mídia Responsável (GARM) é uma iniciativa da indústria para coordenar esforços entre plataformas, agências de mídia e marqueteiros para desenvolver entendimentos comuns de conteúdo "prejudicial e sensível", criar transparência para os participantes da indústria sobre onde o conteúdo sensível pode estar presente e discutir opções para aplicar políticas de monetização consistentes com a estrutura da GARM[2]. No entanto, embora a criação da GARM seja um começo positivo, confiar na auto-regulamentação pelas partes interessadas no negócio não será suficiente para amenizar adequadamente o problema. Dada a centralidade da otimização da atenção para o modelo de negócios principal do setor, deve haver um papel para que os reguladores intervenham e influenciem os incentivos para remover o conteúdo problemático.

Os reguladores também precisarão ter acesso a todas as informações necessárias para identificar a composição, natureza e amplitude das redes de difusão de informações falsas, bem como informações sobre a sua própria difusão. Da mesma forma, os efeitos do mundo real da informação falsa atingindo seu alvo demográfico, influenciando seu público e substituindo a informação especializada, tudo isso precisa ser estudado e avaliado para que os reguladores compreendam a extensão total dos danos causados por qualquer algoritmo particular ou nexo de informação falsa.

IMPLEMENTAÇÃO E INTERVENÇÃO

Quando violações, o não cumprimento ou a não observância de mandatos destinados a conter informações falsas forem documentados, os reguladores precisarão impor multas impactantes e outros desincentivos, bem como ter o poder de intimar plataformas de mídia digital a fim de obter o nível necessário de acesso e permissões para conduzir uma investigação e auditoria completas. Em todo o mundo, já existem precedentes relevantes para esses tipos de poderes dentro dos setores de privacidade, financeiro/bancário, de segurança alimentar e farmacêutico, e precisariam simplesmente ser transferidos para o domínio de dados e informações (ver box ao final do artigo) . Nos Estados Unidos, o leque de atividades da Food and Drug Administration contra violações da segurança alimentar inclui a emissão de notificações para a empresa infratora de delitos, solicitando injunções judiciais contra uma ação e até mesmo abrindo processos criminais por determinadas violações sob a Seção 301 da Lei de Cosméticos (que diz respeito principalmente à adulteração de marcas e produtos).[3]

Da mesma forma, a Comissão de Títulos e Câmbio pode impor punições civis e administrativas contra os infratores, incluindo ordens judiciais que obriguem os indivíduos a se envolverem em certas ações, restituição de dinheiro recebido por atividade de conduta ilegal e penalidades civis.[4] Nesta mesma linha, a Agência de Proteção Ambiental, recentemente, flexibilizou sua força reguladora para processar a Volkswagen por violação das normas de emissão de poluentes, resultando em multas de vários bilhões de dólares. [5]

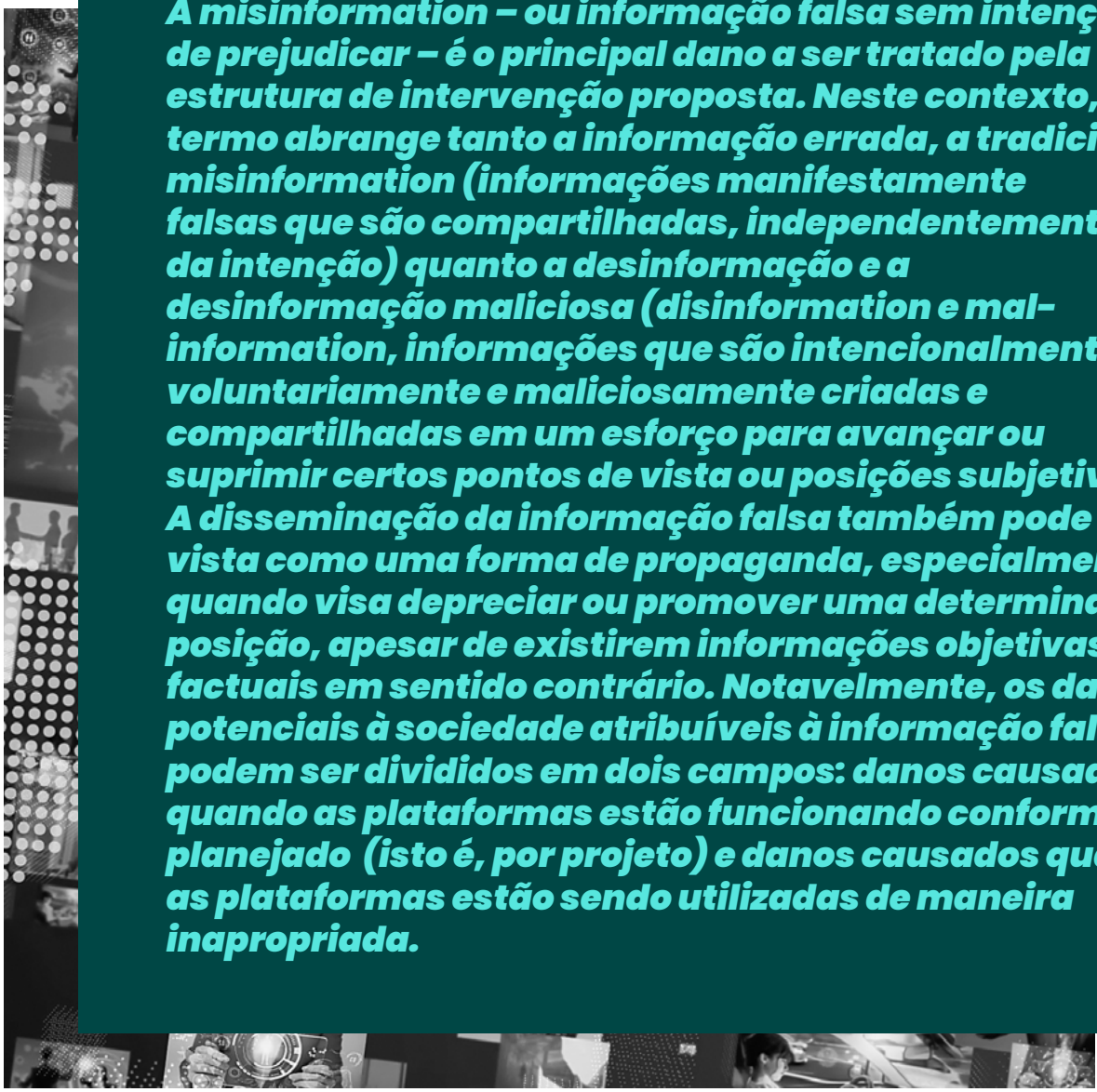
Os reguladores também devem assegurar que a divulgação de conteúdos relevantes e a alfabetização digital sejam incorporadas ao funcionamento das plataformas de mídia digital. O cumprimento das medidas propostas exigiria que essas fornecessem as informações e treinamento necessários para que os usuários tomassem decisões esclarecidas sobre a propagação da informação. Da mesma forma, assim é possível que os usuários possam ser responsabilizados pela participação voluntária na distribuição de informação falsa.

Em essência, as plataformas de mídia digital seriam obrigadas a ajudar a informar e educar os usuários e visitantes sobre o conteúdo que poderia ser enganoso antes de se espalhar, ajudando tanto a educar os cidadãos sobre técnicas úteis para identificar a informação falsa quanto a limitar o ciclo de vida da publicação problemática.

Vários países, incluindo o Reino Unido, Finlândia e Holanda, já ordenaram campanhas de alfabetização sobre a mídia com o objetivo de conter a informação falsa e orientar os cidadãos sobre como verificar as fontes e estar vigilantes antes de compartilhar ou repassar um conteúdo potencialmente enganoso. Embora tais medidas sejam um bem-vindo passo adiante, deve-se tomar cuidado para evitar censurar os esforços jornalísticos e a liberdade de expressão – apesar de a maioria das informações falsas (ao contrário da opinião pessoal) ser facilmente identificada como tal, mesmo na revisão mais superficial.

No Brasil, o artigo 12 do Marco Civil da Internet estabelece uma estrutura legal abrangente para crescentes intervenções por violações de proteção à privacidade. No entanto, embora seja pioneira no campo da privacidade e proteção ao consumidor, esta lei de 2014 permanece em grande parte omissa quanto aos direitos dos usuários da Internet de serem livres de propaganda e quanto às responsabilidades das plataformas de mídia digital em impedir sua disseminação.

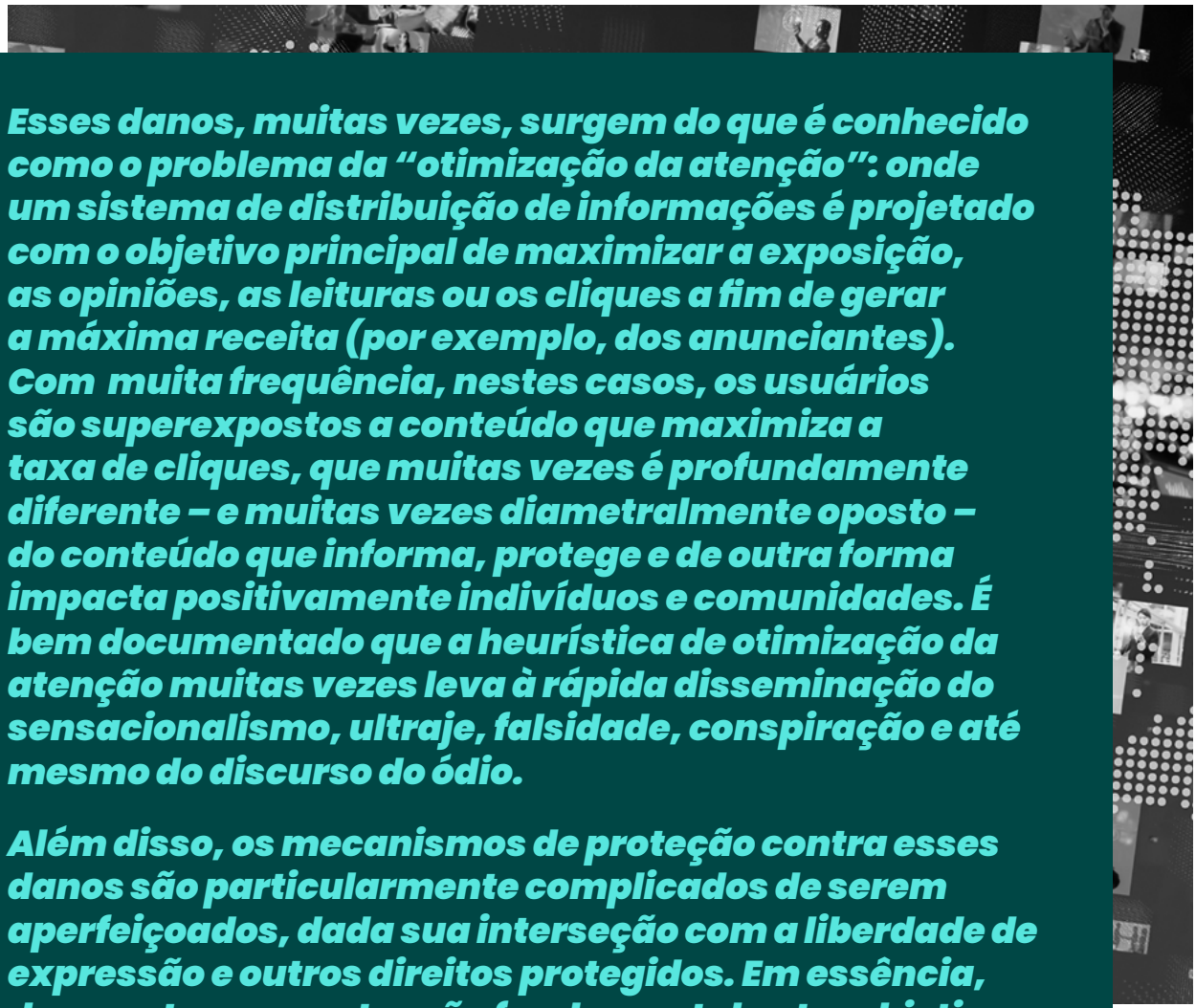
DANOS A SEREM TRATADOS



A misinformation – ou informação falsa sem intenção de prejudicar – é o principal dano a ser tratado pela estrutura de intervenção proposta. Neste contexto, o termo abrange tanto a informação errada, a tradicional misinformation (informações manifestamente falsas que são compartilhadas, independentemente da intenção) quanto a desinformação e a desinformação maliciosa (disinformation e mal-information, informações que são intencionalmente, voluntariamente e maliciosamente criadas e compartilhadas em um esforço para avançar ou suprimir certos pontos de vista ou posições subjetivas). A disseminação da informação falsa também pode ser vista como uma forma de propaganda, especialmente quando visa depreciar ou promover uma determinada posição, apesar de existirem informações objetivas/ factuais em sentido contrário. Notavelmente, os danos potenciais à sociedade atribuíveis à informação falsa podem ser divididos em dois campos: danos causados quando as plataformas estão funcionando conforme planejado (isto é, por projeto) e danos causados quando as plataformas estão sendo utilizadas de maneira inapropriada.

DANOS CAUSADOS POR PLATAFORMAS QUE FUNCIONAM CONFORME O ESPERADO POR PROJETO

Os danos decorrentes de plataformas que funcionam conforme o esperado são os problemas que a sociedade experimenta não por causa de conteúdo ilegal ou exploração enganosa de tais plataformas, mas sim devido à disseminação viral de informações falsas através de uma plataforma quando esse produto está sendo utilizado como pretendido. Ou seja, danos causados pelas plataformas que estão sendo utilizadas para disseminar mídia e propaganda legal – mas factualmente imprecisa.



Esses danos, muitas vezes, surgem do que é conhecido como o problema da "otimização da atenção": onde um sistema de distribuição de informações é projetado com o objetivo principal de maximizar a exposição, as opiniões, as leituras ou os cliques a fim de gerar a máxima receita (por exemplo, dos anunciantes). Com muita frequência, nestes casos, os usuários são superexpostos a conteúdo que maximiza a taxa de cliques, que muitas vezes é profundamente diferente – e muitas vezes diametralmente oposto – do conteúdo que informa, protege e de outra forma impacta positivamente indivíduos e comunidades. É bem documentado que a heurística de otimização da atenção muitas vezes leva à rápida disseminação do sensacionalismo, ultraje, falsidade, conspiração e até mesmo do discurso do ódio.

Além disso, os mecanismos de proteção contra esses danos são particularmente complicados de serem aperfeiçoados, dada sua interseção com a liberdade de expressão e outros direitos protegidos. Em essência, demonstram uma tensão fundamental entre objetivos conflitantes de liberdade individual e danos à sociedade.

DANOS DE PLATAFORMAS QUE ESTÃO SENDO UTILIZADAS INAPROPRIADAMENTE

Os danos resultantes do uso inadequado das plataformas são causados pela sua manipulação ou exploração por agentes malignos. Esta forma de dano muitas vezes se sobrepõe e/ou alavanca os danos das plataformas que trabalham adequadamente. Por exemplo, a criação de redes de contas falsas e/ou híbridas reais/falsas com o propósito de ampliar artificialmente o conteúdo explora a lógica dos algoritmos de otimização da atenção. Normalmente, são utilizados "hacks" projetados para fazer com que os algoritmos de curadoria das plataformas de mídia digital priorizem a mídia para beneficiar um conjunto de usuários ou pontos de vista em relação a outro. Os maus agentes procuram conduzir uma conversa para fins comerciais ou políticos em detrimento do grupo-alvo.

A exploração dos danos pode incluir: Comportamento Inautêntico Coordenado perpetrado por atores estatais ou não estatais, influenciadores pay-for-play que promovem produtos ou ideias sem revelar pagamento, publicidade discriminatória ou enganosa, click-bait para ganhos comerciais e a organização de atividades ilegais e/ou grupos de ódio.

FOCOS DE INTERVENÇÃO

Existem dois objetos principais de intervenção para alterar a propagação de mídia nociva e informação falsa: agências reguladoras e órgãos legislativos.

Em muitas jurisdições, os órgãos reguladores já estão autorizados a instituir a estrutura de intervenção proposta abaixo. Em alguns países e estados, entretanto, novas leis precisariam ser criadas para instituir uma supervisão significativa das plataformas de mídia digital.

Os locais regulatórios em potencial incluem agências de supervisão transnacionais, como as autoridades da Comissão Europeia (estabelecidas pela Digital Services Act's E-Commerce Directive), bem como entidades de nível nacional, como a Federal Trade Commission e a Federal Communications Commission dos Estados Unidos. No nível estadual ou regional, as comissões de serviços públicos e outras agências semelhantes têm capacidades de supervisão dos serviços de telecomunicações e serviços online que se integrem na estrutura atual. Em países específicos, as leis nacionais de proteção ao consumidor em relação às condições de trabalho, fabricação e segurança de produtos, controles de poluição e supervisão da autoridade tributária fornecem esquemas úteis de como o comportamento corporativo pode ser efetivamente investigado - e desincentivos significativos criados - para conter a disseminação de desinformação.

Em uma escala mais global, a legislação transnacional poderia tomar emprestado do domínio dos direitos autorais e da propriedade intelectual elementos que poderiam ser utilizados para defender que plataformas de mídia digital prestem contas além das fronteiras nacionais. Da mesma forma, nos setores financeiro/bancário e de investimento, vários tratados internacionais trabalham para garantir que o mau comportamento corporativo possa ser reprimido através das fronteiras internacionais.

ESTRUTURA DE INTERVENÇÃO PROPOSTA

As empresas que administram plataformas de mídia digital precisam de uma estrutura de supervisão transparente, com um conjunto claro de expectativas e um sistema de responsabilização padronizado. Para garantir que as empresas não sejam pegas desprevenidas por novos mandatos regulatórios, a criação de uma estrutura de escalonamento multiníveis concederá às empresas múltiplas oportunidades de cumprimento da lei antes que as medidas mais sérias sejam instituídas. Assim, operando de boa-fé, as empresas serão capazes de resolver rapidamente as questões para eliminar o risco de responsabilização financeira e legal bem antes que se torne necessária uma intervenção mais relevante.

A estrutura de intervenção de cinco níveis proposta abaixo oferece um caminho claro para o futuro, equilibrando as práticas e prioridades empresariais com a responsabilidade corporativa para com a sociedade em geral. Cada um dos cinco níveis contém tanto uma oportunidade de melhorar as questões de propagação de informação falsa e vieses, como uma série ascendente de medidas sobre as empresas, caso fracassem na resolução de problemas recorrentes. Os exemplos apresentados, retirados de plataformas de mídia digital e outras indústrias, oferecem precedentes relevantes para as intervenções que estão sendo propostas.

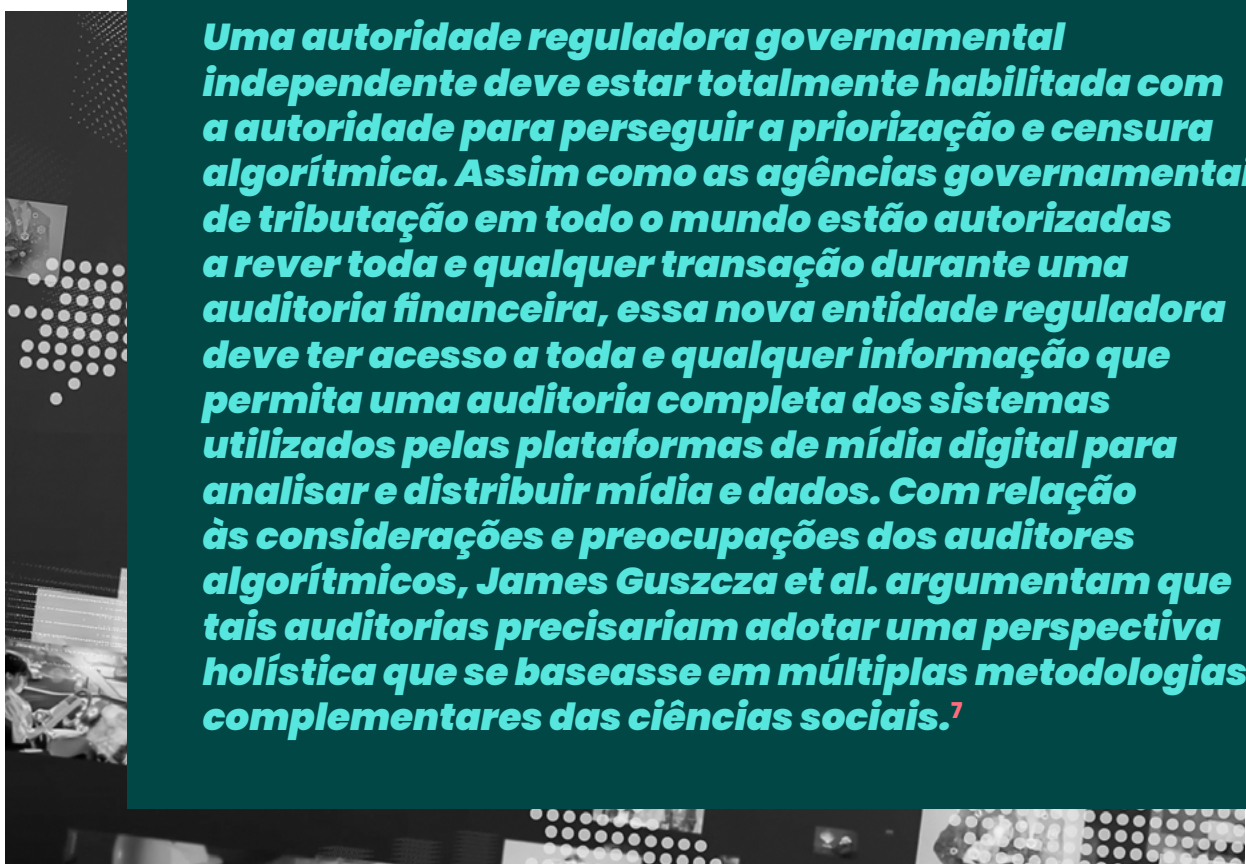
DIVULGAÇÃO E TRANSPARÊNCIA

Em geral, as empresas já têm indivíduos em cargos com obrigações legais que as tornam pessoalmente responsáveis pela conduta de sua empresa, caso se verifique que a organização tenha infringido a lei. Um diretor financeiro, por exemplo, pode ser responsabilizado pessoalmente se supervisionar uma violação de certas leis contábeis e de relatórios fiscais. No mesmo espírito, um indivíduo ou equipe de indivíduos deve ter a responsabilidade legal primária de administrar o tratamento de informações falsas, desinformações e seus perigos e danos

associados. Exigir que um indivíduo (ou grupo de indivíduos) exerça ativamente a diligência em assuntos de informação falsa permitirá que as plataformas de mídia digital designem e capacitem as partes interessadas, estabeleçam protocolos de tomada de decisão e garantam a conformidade com essa estrutura regulatória proposta. Tal pessoa, ou equipe de pessoas, seria responsável por assinar o desempenho, impacto e resultados dos vários algoritmos usados pela plataforma de mídia para publicar, exibir, compartilhar e difundir conteúdo.

O professor de Direito de Harvard, Jonathan Zittrain, e o professor de Direito de Yale, Jack Balkin, propõem que esses requisitos de divulgação e transparência poderiam se enquadrar em uma categoria mais ampla de "fiduciários de informação". As empresas concordariam com um conjunto de práticas de informação justa e prometeriam vender esses dados somente a outros atores que obedecessem a regras semelhantes.[6]

AUDITORIAS ALGORÍTMICAS



Uma autoridade reguladora governamental independente deve estar totalmente habilitada com a autoridade para perseguir a priorização e censura algorítmica. Assim como as agências governamentais de tributação em todo o mundo estão autorizadas a rever toda e qualquer transação durante uma auditoria financeira, essa nova entidade reguladora deve ter acesso a toda e qualquer informação que permita uma auditoria completa dos sistemas utilizados pelas plataformas de mídia digital para analisar e distribuir mídia e dados. Com relação às considerações e preocupações dos auditores algorítmicos, James Guszcza et al. argumentam que tais auditorias precisariam adotar uma perspectiva holística que se baseasse em múltiplas metodologias complementares das ciências sociais.[7]

Além disso, um plano de melhoria da auditoria algorítmica deve ser desenvolvido pelo auditor para assegurar tanto a divulgação completa dos resultados dos fatos, como também que as empresas tenham total clareza quanto ao que precisa ser feito para cumprir a lei atual. Os resultados e os entregáveis deste plano também serão da competência da(s) posição(ões) interna(s) descrita(s) acima, no Nível I de intervenção.

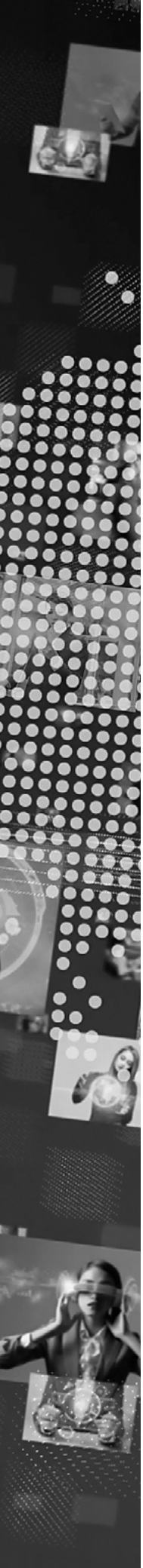
O indivíduo ou indivíduos nesta posição precisarão assinar os resultados da auditoria, bem como as mudanças necessárias para que a empresa esteja em conformidade com as exigências legais.

MULTAS SIGNIFICATIVAS E IMPACTANTES PELO NÃO CUMPRIMENTO INTENCIONAL

O General Data Protection Regulation da União Europeia,, sob o artigo 83, tem um sistema de multas de dois níveis que prevê multas de 2% ou 4% (especificamente relacionadas a violações de privacidade) da receita global da empresa. Da mesma forma, quando se trata de divulgação e contenção de informações falsas, os valores das multas podem variar, dependendo do tipo de infração, da vontade das partes interessadas e dos impactos ou potenciais impactos da não conformidade.

A fim de desenvolver um incentivo multicanal à conformidade, as penalidades financeiras também devem ser combinadas com restrições às operações comerciais.

Investigações sobre a forma como as plataformas lidam com a disseminação de informações errôneas em suas redes serão seguidas por medidas para mitigar os danos atribuíveis a falhas no cumprimento. As empresas que lucram com a disseminação de informações falsas terão que tomar medidas concretas e imediatas para demonstrar seu compromisso de interromper a disseminação. A Lei de Aplicação da Rede Alemã poderia fornecer um modelo potencial para tais multas. De acordo com essa legislação, as empresas de tecnologia poderiam enfrentar multas de até 50 milhões de euros, por incidência, caso não removam o discurso do ódio das suas plataformas.[8]



DIMINUIÇÃO DA PROTEÇÃO DE RESPONSABILIDADE (DIMINUIÇÃO DA "NEUTRALIDADE" DA DOUTRINA DA TERCEIRA PARTE)

As plataformas neutras que fornecem conteúdo gerado pelo usuário sem qualquer ponderação ou curadoria são fundamentalmente diferentes dos serviços e aplicações que priorizam e adaptam ativamente a mídia para seus usuários. Da mesma forma, as proteções de responsabilização destinam-se a garantir que plataformas neutras não sejam responsabilizadas pelo conteúdo em que não tiveram participação na criação ou disseminação. Isto, entretanto, é bem diferente do papel desempenhado por uma plataforma de mídia digital que, tendo falhado sistematicamente, em melhorar uma conhecida propagação de informação falsa ou violação da informação, e seguindo a implementação de um plano de melhoria e/ou multas, não se qualifica mais como uma plataforma neutra – mas sim como o curador ativo de mídia problemática. Assim, uma menor proteção de responsabilidade deveria se aplicar à plataforma de mídia digital como um intermediário – o que não infringiria nenhum direito relevante de liberdade de expressão concedido aos transmissores de ideias e informações.

Exemplos de proteções de responsabilização que podem ser retiradas das plataformas de mídia digital que continuam a propagar informações nocivas/militares incluem as concedidas através da Seção 230 da Lei de Decência das Comunicações de 1996 e/ou Seção 512 da Lei de Direitos Autorais do Milênio Digital nos Estados Unidos, ou a Diretiva de Comércio Eletrônico de 2000 na União Europeia. Alguns comentaristas propuseram que a Seção 230 deveria ser usada como alavanca para induzir que as plataformas fossem mais transparentes – forçando-as a ganhar imunidade ao revelar como seus algoritmos ordenam as notícias e quanta informação falsa está sendo divulgada.[9] Nesta linha, Danielle Citron e Benjamin Wittes sugerem que a reforma da Seção 230 pode envolver a adição de linguagem sobre "medidas razoáveis para prevenir ou abordar usos ilegais" de serviços como um pré-requisito para proteções de responsabilidade.[10]

AÇÃO PENAL

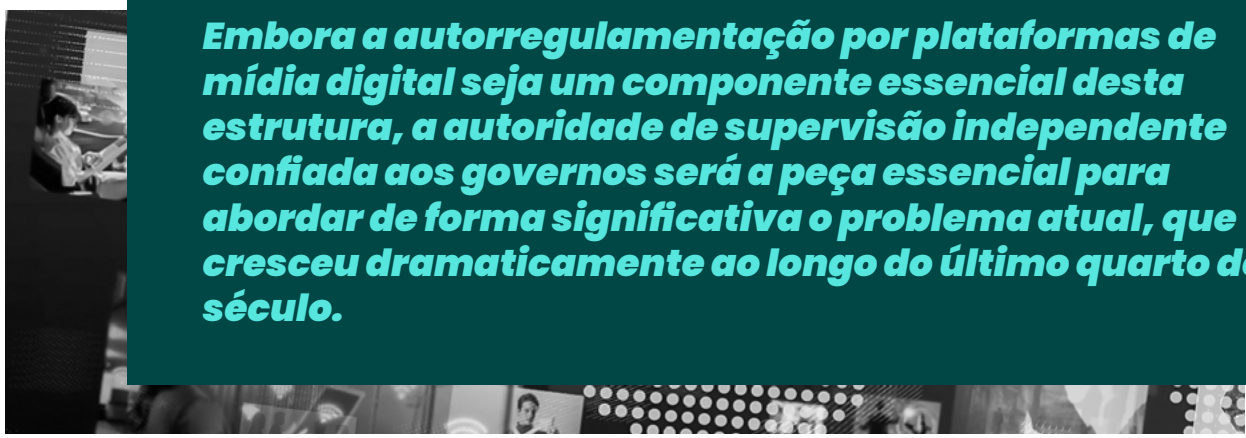
Por mais que existam estruturas de processo penal dentro dos domínios financeiro e de produção/extração de recursos nacionais, são necessárias vias claramente delineadas para o processo penal no setor de divulgação de dados/informações para garantir que as corporações e os indivíduos envolvidos em atividades sistemáticas de violação da lei sejam responsabilizados.

Para plataformas de mídia digital reincidentes/intransigentes que continuam a propagar informação falsa e conteúdo nocivo/abusivo, apesar das vias anteriores de intervenção, a última camada desta estrutura de intervenção envolve um processo criminal em duas etapas:

1. Ação penal corporativa visando a empresa/organização infratora; e,

2. Ação penal contra o(s) indivíduo(s) designado(s) para supervisionar a conformidade da plataforma de mídia digital com a lei.

Embora a intenção e a esperança desta estrutura regulatória proposta seja que cada nível proporcione um desestímulo adequado e crescente para fomentar a cessação imediata da mídia prejudicial e/ou a informação falsa, os reguladores não devem se coibir de instituir regras claras e/ou prazos que desencadeiem novas intervenções.



Embora a autorregulamentação por plataformas de mídia digital seja um componente essencial desta estrutura, a autoridade de supervisão independente confiada aos governos será a peça essencial para abordar de forma significativa o problema atual, que cresceu dramaticamente ao longo do último quarto de século.

BOX

EXEMPLOS DOS CINCO NÍVEIS DA ESTRUTURA DE INTERVENÇÃO

Cada um dos cinco níveis da estrutura de intervenção proposta contém tanto uma oportunidade de melhorar as questões de propagação de informação falsa e vieses, como uma série crescente de repercussões para um fracasso contínuo na resolução de problemas recorrentes. Os exemplos a seguir, retirados de plataformas de mídia digital e outras indústrias, fornecem precedentes relevantes para as intervenções que estão sendo propostas:

I. Divulgação e Transparência – A carta da Aliança Global para Mídia Responsável estabelece os primeiros passos para a divulgação e transparência, criando um mecanismo aprovado pela indústria para regras de divulgação padrão e exigindo a necessidade de uma autoridade de auditoria independente: https://wfanet.org/garm

II. Auditorias algorítmicas – Exemplos de agências governamentais que obrigam as organizações a divulgar informações são inúmeras, sendo a Receita Federal dos Estados Unidos apenas uma das muitas instituições com poder de auditoria para obrigar a divulgação de todo e qualquer documento relevante para uma auditoria financeira:https://www.irs.gov/businesses/small-businesses-self-employed/irs-audits

III. Multas Significativas e impactantes pelo não cumprimento intencional – Em 2020, a Amazon enfrentou multas antitruste propostas de 10% de sua receita mundial, ou cerca de US$ 30 bilhões, por possíveis violações das regras antitruste da União Europeia: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077

IV. Diminuição da Proteção de Responsabilização – No outono de 2020, a Federal Communication Comission dos Estados Unidos abriu um processo para investigar a reformulação da Seção 230 da Lei de Decência das Comunicações para aumentar a responsabilidade por plataformas de mídia que censuram informações: https://www.fcc.gov/ecfs/search/filings?proceedings_name=RM-11862. Embora esse esforço particular pareça estar em desacordo com os padrões internacionais de apoio à liberdade de expressão, a noção de que as empresas de mídia não têm direito à responsabilidade ilimitada está consagrada em inúmeros instantes da lei de difamação ao redor do mundo .

V. Processo Penal – A Volkswagen (IAV GmbH) foi acusada de conspiração para fraudar os Estados Unidos, e vários funcionários receberam penas de prisão por suas atividades criminosas:https://www.justice.gov/usao-edmi/us-v-volkswagen-16-cr-20394

Sascha Meinrath

Sascha Meinrath is the Palmer Chair in Telecommunications at Penn State and director of X-Lab, an innovative think tank focusing on the intersection of vanguard technologies and public policy. Professor Meinrath is a renowned technology policy expert and is internationally recognized for his work over the past two decades as a community internet pioneer, social entrepreneur, and angel investor.

Prior to founding X-Lab, Meinrath was vice president of the New America Foundation, where he founded the Open Technology Institute in 2008 and built it into one of the largest public interest tech policy organizations in Washington, D.C. He also founded the Commotion Wireless Project, which works around the globe to strengthen communities by providing tools to build their own local communications infrastructures, and co-founded Measurement Lab, a global online platform for researchers to deploy Internet measurement tools that empower the public and key decision-makers with useful information about broadband connectivity.

Professor Meinrath was elected as an Ashoka Fellow for Social Entrepreneurship in 2012, and has been named to the Time Magazine "Tech 40" as one of the most influential figures in technology, to the "Top 100" in Newsweek's Digital Power Index, and is a recipient of the Public Knowledge IP3 Award for excellence in public interest advocacy. He is widely published in both academic and media outlets, including Critical Studies in Media Communications, International Journal of Communications, Journal of Communications Law and Policy, Journal of Internet Law, Journal for Community Informatics, IEEE Internet Computing Magazine, IEEE Spectrum, Foreign Policy, The Hill, Time Magazine, Politico, Slate, The Guardian and many others.

Mr. Meinrath has been a vocal public intellectual and a leading voice calling for accountability over the governmental spying programs, and is at the forefront of D.C. policy debates over how Congress and the White House should rein in the cybersecurity-industrial complex. He serves as a board member for the American Indian Policy Institute, Brave New Software Foundation; Defending Rights and Dissent Foundation; Acorn Active Media Foundation; and Fourth Amendment Advisory Committee. He is also a member of the advisory councils for the Calyx Institute, FreedomBox Foundation, Loomio, and Whistleblower Aid.

Meinrath's research focuses on broadband connectivity, distributed communications, Digital Feudalism, Digital Craftsmanship, telecommunications and spectrum policy, cybersecurity and privacy, and the impacts of disruptive technology, and is a testament to his lifelong commitment to promoting social and economic justice -- values he embraced while attending a rough inner-city school in New Haven, Connecticut.

Imagem: AdobeStock.com

Steven Mansour

Steven Mansour provides training and support to scientists, non-profits and community groups throughout Latin America since 2004. He has given Linux & Open Source Software workshops in Cuba, and works closely with the Fundación Canguro in Colombia, developing knowledge transfer strategies for doctors and researchers working with premature & low birth weight (LBW) infants. He was Director of Technology & Partnerships at the World Association of Young Scientists, a UNESCO project to support young scientists and early-career researchers. Steven worked closely with the McGill University Health Center, the Centre Hospitalier Universitaire Sainte-Justine and the Alberta Children's Hospital to develop social research and e-learning tools for professors and students in Mother-Child research. His work on Internet privacy and security has been featured in international media.

Humza Jilani

Humza Jilani studies digital public policy and national security at the University of Oxford, where he reads for a Master of Philosophy in International Relations as a Marshall Scholar. His research explores the role of historical media networks, both online and offline, in fomenting political violence. Born and raised in Houston, Humza has researched terrorists' use of emerging technologies for Tech Against Terrorism, worked in business development in Karachi, Pakistan at rural development startup UpTrade and as an economic analyst at the Foreign, Commonwealth and Development Office in London, U.K., and spent a summer reporting on technology and defense for Foreign Policy magazine. Jilani graduated magna cum laude with highest honors in Social Studies from Harvard University.

NOTAS E REFERÊNCIAS

1 See, e.g., the European Commission's Consultation on the Digital Services Act: https://ec.europa.eu/digital-single-market/en/news/consultation-digital-services-act-package.

2 "GARM: Brand Safety Floor + Suitability Framework." Global Alliance for Responsible Media. https://wfanet.org/l/library/download/urn:uuid:7d484745-41cd-4cce-a1b9-a1b4e30928ea/garm+brand+safety+floor+suitability+framework+23+sept.pdf.

3 "FD&C Act Chapter III: Prohibited Acts and Penalties." U.S. Food & Drug Administration. https://www.fda.gov/regulatory-information/federal-food-drug-and-cosmetic-act-fdc-act/fdc-act-chapter-iii-prohibited-acts-and-penalties. Also see, "Types of FDA Enforcement Actions." U.S. Food & Drug Administration. https://www.fda.gov/animal-veterinary/resources-you/types-fda-enforcement-actions.

4 "About the Division of Enforcement." U.S. Securities and Exchange Commission. https://www.sec.gov/enforce/Article/enforce-about.html.

5 "Learn About Volkswagen Violations." United States Environmental and Protection Agency. https://www.epa.gov/vw/learn-about-volkswagen-violations.

6 Zittrain, Jonathan and Jack M. Balkin. "A Grand Bargain to Make Tech Companies Trustworthy." The Atlantic, October 3, 2016. https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/; Balkin, Jack M. "Information Fiduciaries and the First Amendment." U.C. Davis Law Review 49, no. 4 (2016): 1183-1283.

7 Guszcza, James, Iyad Rahwan, Will Bible, Manuel Cebrian, & Vic Katyal. "Why We Need to Audit Algorithms." Harvard Business Review, November 28, 2018. https://hbr.org/2018/11/why-we-need-to-audit-algorithms.

8 Toor, Amar. "Germany Passes Controversial Law to Fine Facebook over Hate Speech." The Verge, June 30, 2017. https://www.theverge.com/2017/6/30/15898386/germany-facebook-hate-speech-law-passed.

9 Stigler Committee on Digital Platforms, Final Report, September 2019. https://www.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf.

10 Citron, Danielle, and Benjamin Wittes. "The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity." Fordham Law Review 86, no. 2 (2017): 401–23.

doi.org/10.52959/2021535417

QUAL A FUNÇÃO SOCIAL DA NOVA ECONOMIA?

O LADO POSITIVO DA "GIG ECONOMY"

Diego Barreto

Desde que o mundo é mundo, a tecnologia tem o poder de provocar profundas transformações na sociedade. Do tacape às máquinas a vapor, da agricultura ao processamento de código binário, as inovações são ao mesmo tempo conquista e desafio, excitação e medo. Elas alimentam a nossa imaginação, mas têm o poder de mexer com o *status quo* e desfazer as zonas de conforto, às quais, sabemos, as pessoas adoram se apegar. Com isso, não quero dizer que o impacto da nova economia na vida das pessoas deva ser ignorado em nome do "progresso" ou outra ideia abstrata parecida. Isso não é diferente para o que observamos na Nova Economia, em especial para as novas relações de trabalho. Do ponto de vista social, a insegurança em relação ao futuro é mais que justa, especialmente entre as camadas mais vulneráveis, sobretudo considerando as incertezas e dificuldades do Brasil nos últimos anos. Entretanto, é importante pontuar alguns aspectos da questão com, mais que serenidade, profundidade. A reflexão sobre fatos e dados no tema pode nos trazer boas notícias.

A explosão das plataformas baseadas em tecnologia proprietária, que estão na base da Nova Economia, ao intermediar a prestação de serviços, veio acompanhada da discussão sobre "precarização" do trabalho. Aqui, é importante um olhar pragmático sobre o tema.

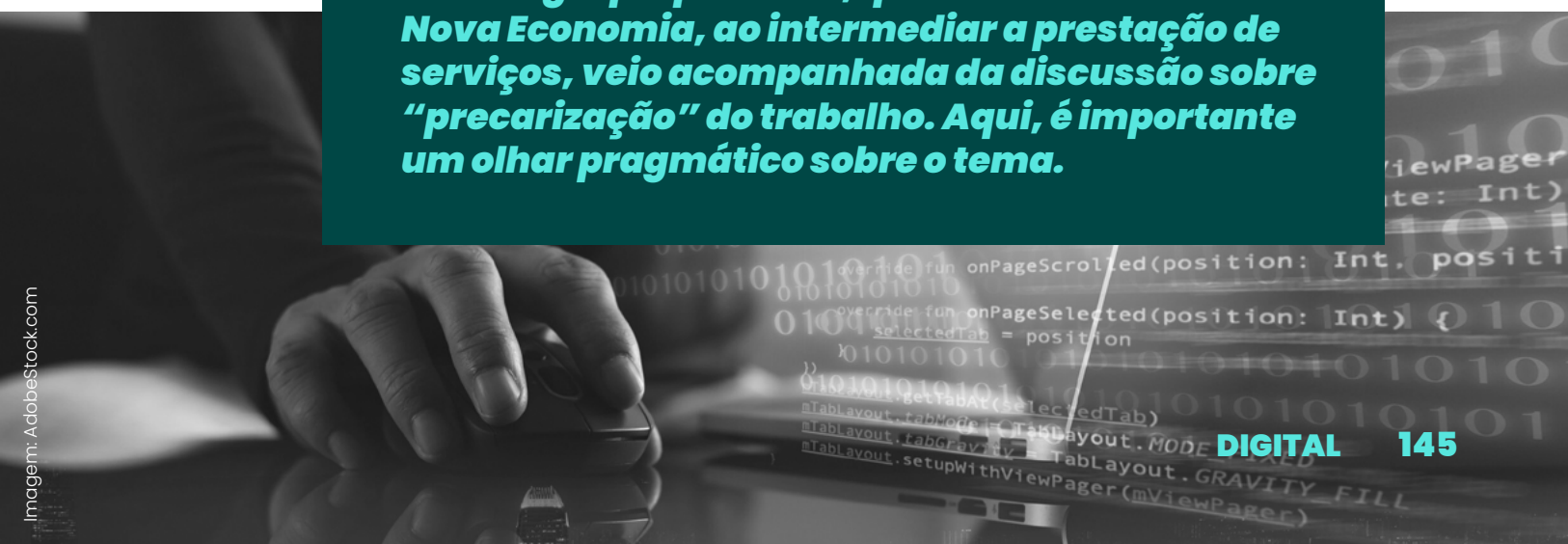


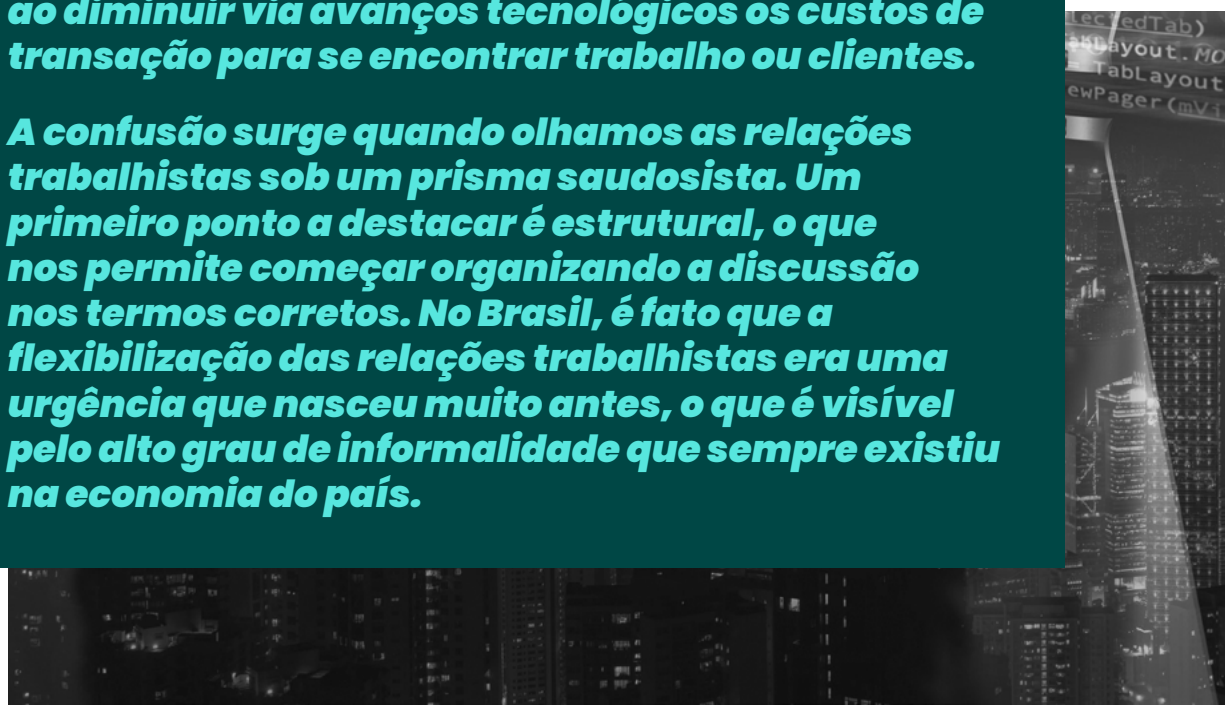
Imagem: AdobeStock.com

O sentido acabou colando em especial nas plataformas que conectam os usuários a fornecedores de bens e serviços – como é o caso, por exemplo, dos aplicativos de transporte e de *delivery*. O que nos leva ao conceito de *gig economy*, definido por relações flexíveis de trabalho, sem vínculo empregatício, que garantem novas oportunidades e autonomia para os trabalhadores. Ao mesmo tempo, esses modelos de negócio vêm sendo apontados como responsáveis pela retirada de direitos e benefícios.

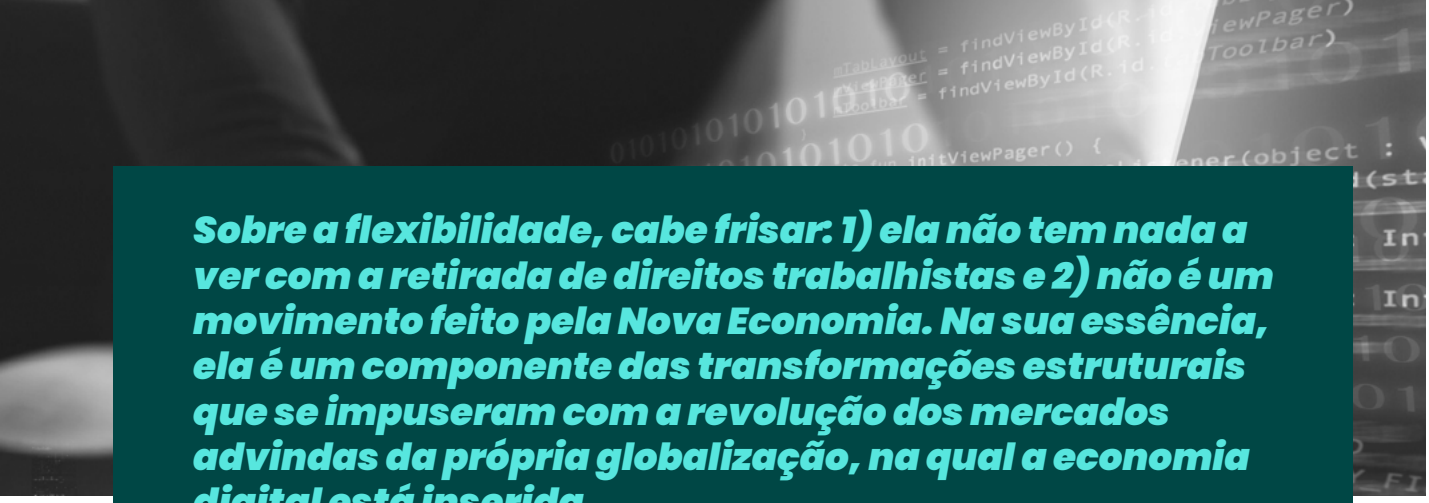
A *gig economy* só se tornou realidade a partir do avanço tecnológico, mas sua base conceitual existe desde 1937, quando o economista e, mais tarde, prêmio Nobel Ronald Coase teorizou sobre a natureza das firmas[1]. Coase conceitua que os custos de transação são fundamentais para a organização das empresas e isso tem impacto direto na quantidade de pessoas envolvidas em sua atividade.

A Nova Economia atua diretamente neste ponto, ao diminuir via avanços tecnológicos os custos de transação para se encontrar trabalho ou clientes.

A confusão surge quando olhamos as relações trabalhistas sob um prisma saudosista. Um primeiro ponto a destacar é estrutural, o que nos permite começar organizando a discussão nos termos corretos. No Brasil, é fato que a flexibilização das relações trabalhistas era uma urgência que nasceu muito antes, o que é visível pelo alto grau de informalidade que sempre existiu na economia do país.



Nas últimas décadas do século 20, a revolução global cobrou a fatura de uma economia então pouco competitiva, acostumada aos favores do Estado e às barreiras de entrada. No campo trabalhista, uma saída (bastante discutível) adotada por muitas empresas foi a terceirização da mão de obra, uma forma de driblar o alto custo dos contratos celebrados por meio da agora quase octogenária Consolidação das Leis do Trabalho.



Sobre a flexibilidade, cabe frisar: 1) ela não tem nada a ver com a retirada de direitos trabalhistas e 2) não é um movimento feito pela Nova Economia. Na sua essência, ela é um componente das transformações estruturais que se impuseram com a revolução dos mercados advindas da própria globalização, na qual a economia digital está inserida.

Essa é uma confusão tão comum quanto a de pensar que a discussão dos trabalhos sob demanda são de agora. O encanador e o eletricista que arrumaram suas casas por décadas são trabalhadores sob demanda. O entregador de comida e manicures que vão até sua casa por décadas são trabalhadores sob demanda.

A partir daí podemos pensar o sentido que vai se construindo em torno do conceito "flexibilizar". Sim, precisamos encarar a realidade de que o emprego nos moldes antigos, supostamente seguro e estável, mas para poucos, não faz mais sentido nesse novo cenário. Não porque o financeiro da empresa precisa de um alívio, mas porque a sociedade conectada e em rede demanda uma transformação de toda a lógica do trabalho. Saem os processos engessados e hierarquias rígidas, entram a agilidade e a colaboração, que permitem montar equipes com todos os tipos de potencialidade. Mesmo a terceirização, hoje regulamentada, é um expediente importante. Nessa outra dimensão, flexibilização é um valor não só positivo, mas fundamental. O consumidor quer. Uma grande quantidade de trabalhadores quer. No fim, o importante é conectar os diferentes estilos de vida aos mais variados modelos de negócio de forma a gerar o maior ganho social e econômico possível.

É essa lógica que tem o potencial de transformar o Brasil, porque já está modificando a vida de muita gente.

As plataformas digitais de serviços reduzem dramaticamente as barreiras de entrada ao emprego, dispensando não apenas o controle centralizado dos métodos e horários de trabalho, mas também os de seleção e desempenho de funcionários. Essa flexibilização tem duas consequências centrais: resulta em mais autonomia para o trabalhador e cria oportunidades que de outra forma não existiriam.

Tomemos os casos dos motoristas de aplicativo e dos entregadores de comida. Qualquer pessoa, munida apenas de um meio de transporte e de um celular, pode garantir renda de maneira quase instantânea, sem nenhum acordo de exclusividade. O que, por sua vez, permite ao trabalhador prestar serviço para mais de uma plataforma e para mais de um setor, de acordo com a sua disponibilidade e necessidade, sem as barreiras e as interdições contratuais antigas.

Uma pesquisa do Instituto Locomotiva, encomendada pelo iFood, no começo de 2021[2], mostrou que, de cada dez trabalhadores do setor de delivery, quatro tinham a sua única fonte de renda nas plataformas de delivery. Para 56% dos entrevistados, elas são a principal fonte de rendimentos. O estudo aponta ainda que 94% enxergam mais flexibilidade para compor seus horários ao trabalhar com entregas por aplicativos.

Ainda no cenário pré-pandemia de COVID-19, a economia compartilhada reunia um exército de quase 4 milhões de autônomos. Em contraste com o passado, esse novo cenário significa uma abertura muito maior, também, para jovens atrás do primeiro emprego, que se tornou particularmente difícil após os meses de pandemia, além da velha exigência de experiência. Para muitos, é também uma forma de complementar renda e um colchão para amortecer as oscilações do mercado de trabalho.

Esse cenário foi bem muito representado em escala mundial em um relatório recente da Organização Internacional do Trabalho (OIT)[3]. Baseado em pesquisas e entrevistas de 12 mil trabalhadores de 100 países, 70 empresas, 16 empresas de plataforma e 14 associações de trabalhadores desse setor, o levantamento mostra o potencial de oportunidades de renda para trabalhadores em geral, em especial mulheres, pessoas com deficiência, jovens, imigrantes e refugiados, bem como os que precisam complementar seus ganhos.

Segundo o relatório, o número de plataformas de trabalho quintuplicou no espaço de uma década, criando uma força de trabalho que já tem rosto. Motoristas e entregadores de aplicativo, personagens centrais na discussão da chamada "precarização", tendem a ser mais jovens (36 e 29 anos, respectivamente) do que os que trabalham em ambientes tradicionais desses setores (44 e 31 anos). A disparidade de gênero segue flagrante, mas ainda assim menor que na totalidade do mercado: nas duas atividades, a presença feminina é de menos de 10% da força total, mas esse número é quase o dobro do verificado nos serviços de transporte e entrega fora das plataformas digitais.

Imigrantes e refugiados, por seu turno, representam cerca de 15% da força de trabalho no setor de entrega baseada em aplicativos. Mas há variações reveladoras. Na Argentina e no Chile, por exemplo, esse número chega a 70% entre os trabalhadores que atuam no *delivery* – consequência do grande fluxo de imigrantes refugiados venezuelanos aos nossos vizinhos nos últimos anos. Chama a atenção, aqui, o fato de 43% (Argentina) a 47% (Chile) desses trabalhadores possuírem formação universitária – um dado, dramático, que diz muito mais das conjunturas econômicas e políticas do que propriamente da *gig economy,* que se mostra uma alternativa para quem, por qualquer razão, faltam oportunidades nas suas áreas de formação. Outra revelação preocupante é a jornada de trabalho estendida. Em média, os motoristas e entregadores do universo pesquisado trabalham, respectivamente, 65 e 59 horas por semana – muito tempo, claro, mas equivalente ou menor (70 e 57 horas) ao verificado nos serviços prestados por empresas tradicionais nessas áreas. Sem uma visão centralizada, eles vão de um app para o outro durante o dia, estendendo suas cargas de trabalho.

Em parte, o estudo capta também a devastação econômica provocada pela pandemia de COVID-19. Em que pese o crescimento da demanda global dos serviços de *delivery* no período, o tempo de trabalho aumentou e a renda diminuiu – o que foi resultado de um aumento da competição, com mais entregadores nas ruas: sete entre dez disseram ter seus rendimentos reduzidos. O quadro é coerente com o apurado no Brasil.

A excepcionalidade da pandemia mostra que, sim, existem questões importantes a serem equacionadas por todo o ecossistema da gig economy. Entretanto, e novamente, é preciso estabelecer os termos corretos nesse debate. De maneira geral, o estudo da OIT identifica que os ganhos nas plataformas digitais tendem a ser maiores que nos seus equivalentes analógicos e demonstram como a paisagem institucional e as especificidades locais – demanda, contexto cultural e presença de concorrência – são decisivas.

Esse é mais um ponto importante: o desafio de aprimorar o modelo, garantindo uma renda mínima por hora aos trabalhadores, além de mais segurança social e amparo, não é meramente gerencial. É sobretudo uma demanda por políticas públicas.

O seu eventual sucesso vai depender, em primeiro lugar, da efetividade dos agentes econômicos e políticos e dos atores sociais na construção de um novo arranjo e na resolução de dilemas que são históricos. No Brasil, pesam em toda a cadeia a desigualdade gritante, os vícios de nossas elites, a recessão e o desemprego dos últimos anos, entre outros fatores estruturais ou mesmo circunstanciais, como, por exemplo, a desastrosa gestão da pandemia.

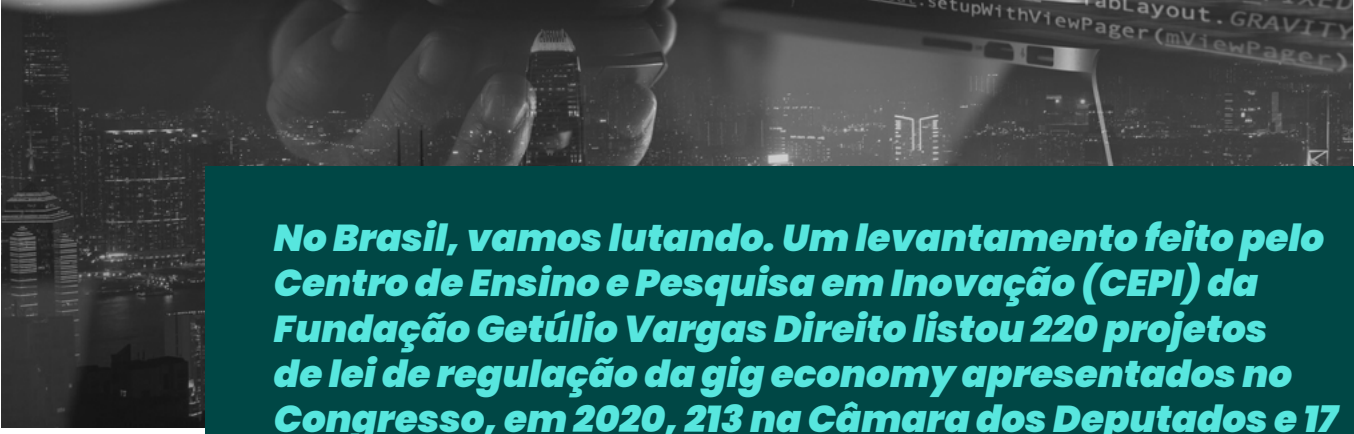
Pactuada, essa transformação passa, necessariamente, por uma regulação adequada do setor.

Um marco regulatório específico para as plataformas deve ser um objetivo de todos os envolvidos no debate, uma vez que elas estão promovendo uma transformação profunda na própria concepção do trabalho – que é global, mas segue sendo variável, dependendo do contexto econômico em que está inserido.

Em 2018, a cidade de Nova York, por exemplo, aprovou a adoção de uma renda mínima por hora para os motoristas de aplicativo.

A principal preocupação do setor era que a medida resultasse em um aumento de tarifas – já que as empresas teriam de cobrir a diferença se o trabalhador não atingisse esse patamar –, afastando os clientes. Iniciado em fevereiro de 2019, o sistema se mostrou factível e até vantajoso para os envolvidos. Sobre essa experiência, um estudo publicado em dezembro de 2020 identificou, a partir da análise de meio bilhão de viagens realizadas entre agosto de 2017 e dezembro 2019, um aumento de cerca de 9% nas rendas diárias dos motoristas nesse regime[4].A adoção do mecanismo implicou na limitação de entrada de novos motoristas e em um aumento médio de 6% nas viagens, bem absorvido pelos passageiros.

A demanda, as distâncias médias percorridas e até o contexto cultural de uma cidade com hábitos de mobilidade específicos foram a chave para esse exemplo, até agora, de sucesso. A limitação do número de motoristas, por exemplo, pode se revelar contraproducente em cidades de perfis distintos, criando uma barreira para aqueles que teriam essa alternativa de rendimento. Do mesmo modo, as variações do preço final pago pelo passageiro poderiam inviabilizar todo o modelo. Preço dos combustíveis, trânsito e gastos de manutenção, por exemplo, são fatores externos que fazem toda a diferença na conta final. Não há uma receita universal, nem panaceia capaz de sugerir que a solução está logo ali na esquina. É necessário diálogo franco e baseado em dados para avançar no assunto.



No Brasil, vamos lutando. Um levantamento feito pelo Centro de Ensino e Pesquisa em Inovação (CEPI) da Fundação Getúlio Vargas Direito listou 220 projetos de lei de regulação da gig economy apresentados no Congresso, em 2020, 213 na Câmara dos Deputados e 17 no Senado Federal[5].

Grande número deles se limitava a propor soluções de enfrentamento à COVID-19 e, para a análise amostral, foram considerados 40 desse universo – 39 projetos de lei ordinária e um de lei complementar. Entre os mais abrangentes, o relatório destaca três deles: PL 3748/2020, da deputada Tabata Amaral; PL 3754/2020 (senador Alessandro Vieira); e PL 4172/2020 (deputado Henrique Fontana). Em boa parte, as propostas procuram incorporar, de maneira modulada, dispositivos legais da CLT e benefícios como salário-mínimo, seguro-desemprego, licença-maternidade, segurança e afastamento remunerado do trabalho por necessidade médica.

Os três projetos estão em fase de tramitação, e seu mérito, nesse momento, está em pavimentar o caminho para uma eventual criação de um Marco Regulatório das Plataformas, que precisa ser o resultado de um amplo debate entre os setores envolvidos, os trabalhadores e o poder público.

De tal modo que se contornem as armadilhas ideológicas, o tiroteio dos *lobbies* e populismo arcaico. Que levem em consideração as especificidades locais, desviando-se de medidas que acabem sendo contraproducentes.

A revolução propagada pelas novas tecnologias impõe desafios, mas não deixa de ser uma grande oportunidade para o desenvolvimento. Que o Marco Regulatório das Plataformas seja um passo para o estabelecimento de uma nova lógica econômica, para construirmos um Brasil diferente. Menos tutelada pelo Estado, sim, e mais flexível, integrada ao ambiente colaborativo e de inclusão que são indissociáveis das empresas da Nova Economia .

Diego Barreto

Diego Barreto é Vice-Presidente de Finanças e Estratégia do iFood e autor do best seller “Nova Economia”. Também é mentor na Endeavor e na 500 Startups, além de atuar a favor de startups em diferentes países e como conselheiro de empresas da Velha e da Nova Economia. Formado em Direito na PUC/SP, possui um MBA pelo IMD Business School, na Suíça, foi executivo sênior da Movile e da Suzano Papel e Celulose. Atualmente é Colunista MIT Technology Review.

NOTAS E REFERÊNCIAS

1 COASE, Ronald Harry. The nature of the firm. Economica, v. 4, n. 16, p. 386-405, 1937.

2 A pesquisa quantitativa, feita por telefone com questionário estruturado, reuniu relatos de 1.241 entregadores, entre homens e mulheres, coletados entre 23 e 26 de abril. A margem de erro é de 2,8 pontos percentuais.

3 World Employment and Social Outlook 2021: The role of digital labour platforms in transforming the world of work. International Labour Office – Geneva: ILO, 2021.

4 KOUSTAS, Dmitri; PARROT, James; REICH, Michael. New York City's Gig Driver Pay Standard: Effects on Drivers, Passengers, and the Companies. The New School Center for New York City Affairs.

5 Centro de Ensino http://bibliotecadigital.fgv.br/dspace/handle/10438/29938 e Pesquisa em Inovação da FGV Direito SP. Briefing temático #1: Projetos de lei de 2020 sobre gig economy - uma sistematização de definições e normas sobre condições de trabalho, benefícios e remuneração. Versão São Paulo: FGV Direito SP, 1º dez. 2020.

doi.org/10.52959/2021535418

COMO LIDAR COM O IMPACTO DA ECONOMIA DIGITAL NO MUNDO DO TRABALHO?

Wilson Engelmann

Se vive, de acordo com Luciano Floridi, em uma "era hiperconectada", o que gera um cenário *OnLife*, que corresponde "[...] à nova experiência de uma realidade hiperconectada dentro da qual não faz mais sentido perguntar se se pode estar *online* ou *offline*"[1]. Se tem, portanto, cada vez mais, uma vida projetada em redes e dependente delas para o desenvolvimento do ser humano em um espaço híbrido e multimodal. A condição humana é afetada pelo desenvolvimento constante e crescente das tecnologias de informação e comunicação, provocando o seguinte quadro de transformações:

"I. indefinição da distinção entre realidade e virtualidade;

II. o obscurecimento das distinções entre humano, máquina e natureza;

III. a reversão da escassez de informações para a abundância de informações; e

IV. a mudança da primazia das entidades para a primazia das interações."[2]

Essas modificações já são realidade, impactando a vida das pessoas na sociedade, com destaque para as novas relações de trabalho, estruturando a denominada *Gig Economy*, que se nutre justamente da crescente dificuldade de se separar a relação entre o humano e a máquina.

A *Gig Economy* se insere nesse cenário fluído, inovador, revolucionário e desconhecido, que se nutre pela grande disponibilidade de informações que circulam em redes virtuais locais, nacionais e globais, gerando novos riscos, inclusive para o mundo do trabalho, que sempre foi estruturado a partir de um contrato de trabalho fortemente definido pela lei. Esses movimentos decorrem na convergência das tecnologias que se inserem no panorama da Quarta Revolução Industrial[3], como a inteligência artificial, nanotecnologias, internet das coisas, dentre outras tecnologias.

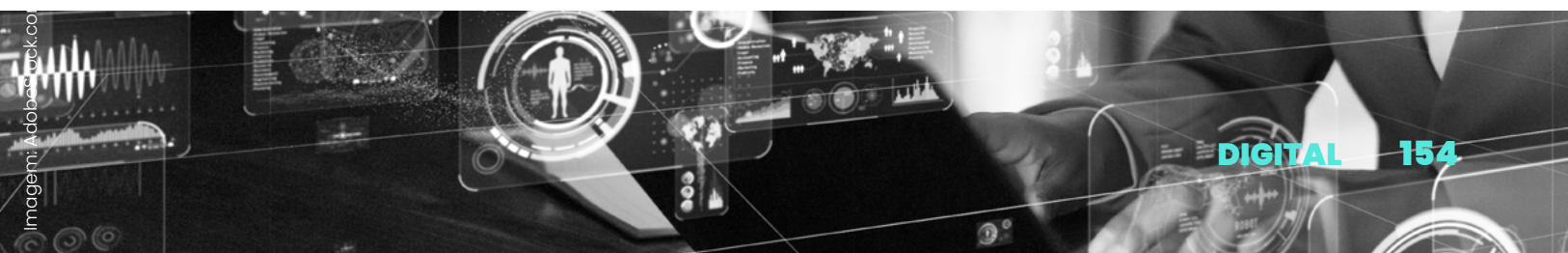
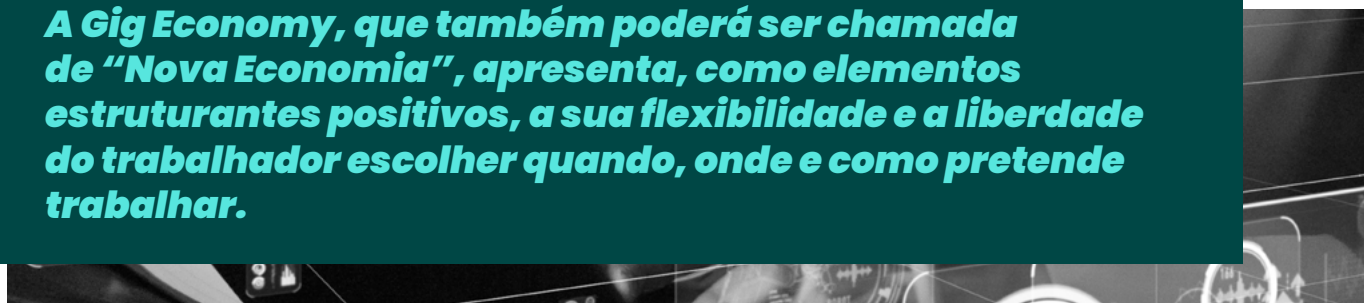


Imagem: Adobe Stock.com

A Gig Economy, que também poderá ser chamada de "Nova Economia", apresenta, como elementos estruturantes positivos, a sua flexibilidade e a liberdade do trabalhador escolher quando, onde e como pretende trabalhar.

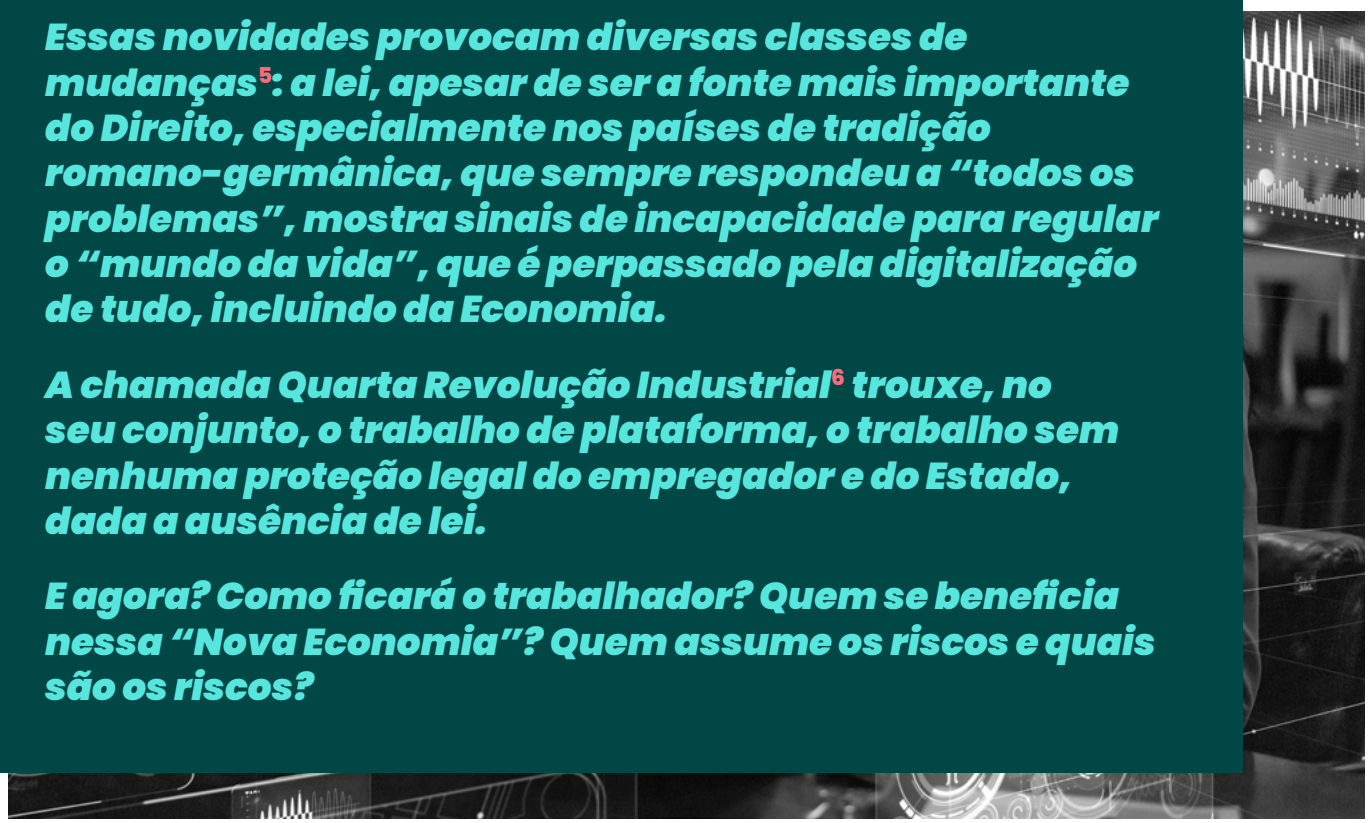


Essa Economia se utiliza fortemente das tecnologias digitais, gerando redes que conectam os chamados *freelances* com os clientes para fornecer serviços de curto prazo ou compartilhamento de ativos. É um segmento em crescimento, trazendo benefícios econômicos de produtividade e a geração de empregos informais, postos sem conexão com a legislação trabalhista e previdenciária.[4]

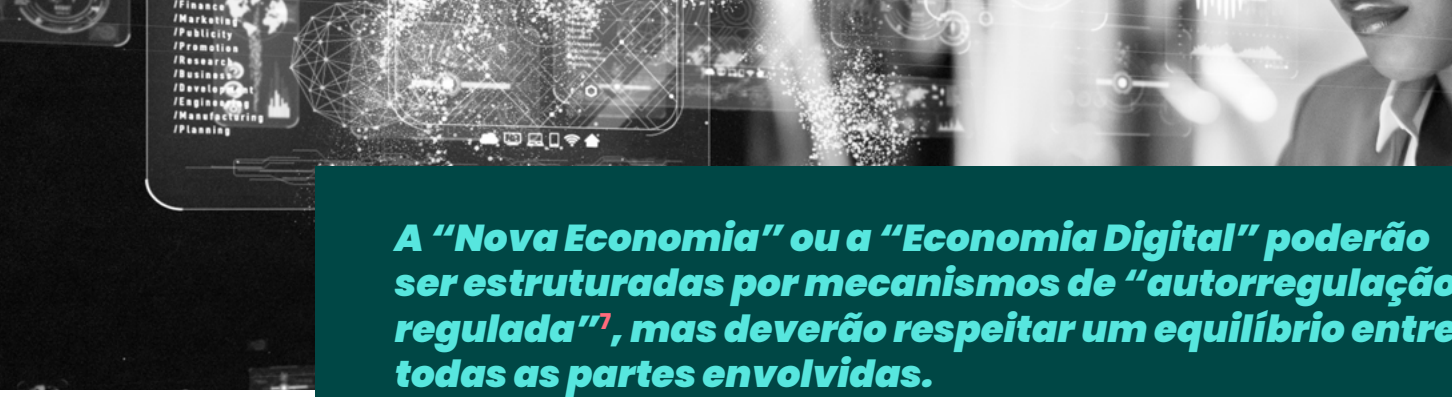
Essas novidades provocam diversas classes de mudanças[5]: a lei, apesar de ser a fonte mais importante do Direito, especialmente nos países de tradição romano-germânica, que sempre respondeu a "todos os problemas", mostra sinais de incapacidade para regular o "mundo da vida", que é perpassado pela digitalização de tudo, incluindo da Economia.

A chamada Quarta Revolução Industrial[6] trouxe, no seu conjunto, o trabalho de plataforma, o trabalho sem nenhuma proteção legal do empregador e do Estado, dada a ausência de lei.

E agora? Como ficará o trabalhador? Quem se beneficia nessa "Nova Economia"? Quem assume os riscos e quais são os riscos?



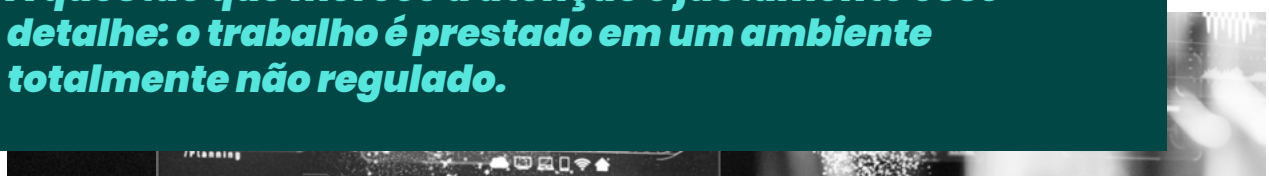
Se sabe que as relações sócio-humanas precisam acompanhar as transformações geradas pelos próprios humanos. Entretanto, apesar dos avanços que se anunciam, se deverá cuidar para não vulnerabilizar ainda mais as pessoas que já se encontram em níveis "quase" inaceitáveis. Por isso, será importante observar e enfrentar os efeitos das anunciadas "novidades" – e que são chamadas de "inovação". Nem tudo é humanamente aceitável.



A "Nova Economia" ou a "Economia Digital" poderão ser estruturadas por mecanismos de "autorregulação regulada"[7], mas deverão respeitar um equilíbrio entre todas as partes envolvidas.

Segundo Robert Edward Freeman, em seu livro "Strategic Management: a stakeholder approach"[8], se deverá praticar uma nova narrativa para os negócios: "nela, os empreendedores não precisariam ter vergonha de ganhar dinheiro, desde que seus negócios fossem acompanhados por um senso de propósito e de moralidade".[9] Portanto, aqui se tem um primeiro princípio que deverá orientar a resposta à pergunta título deste artigo: se a Economia digital conseguir respeitar e se orientar por tal constatação de Freeman, estará em condições de prosseguir. Caso contrário, deverá entrar em *stand by*, a fim de se ressignificar.

A questão que merece a atenção é justamente esse detalhe: o trabalho é prestado em um ambiente totalmente não regulado.

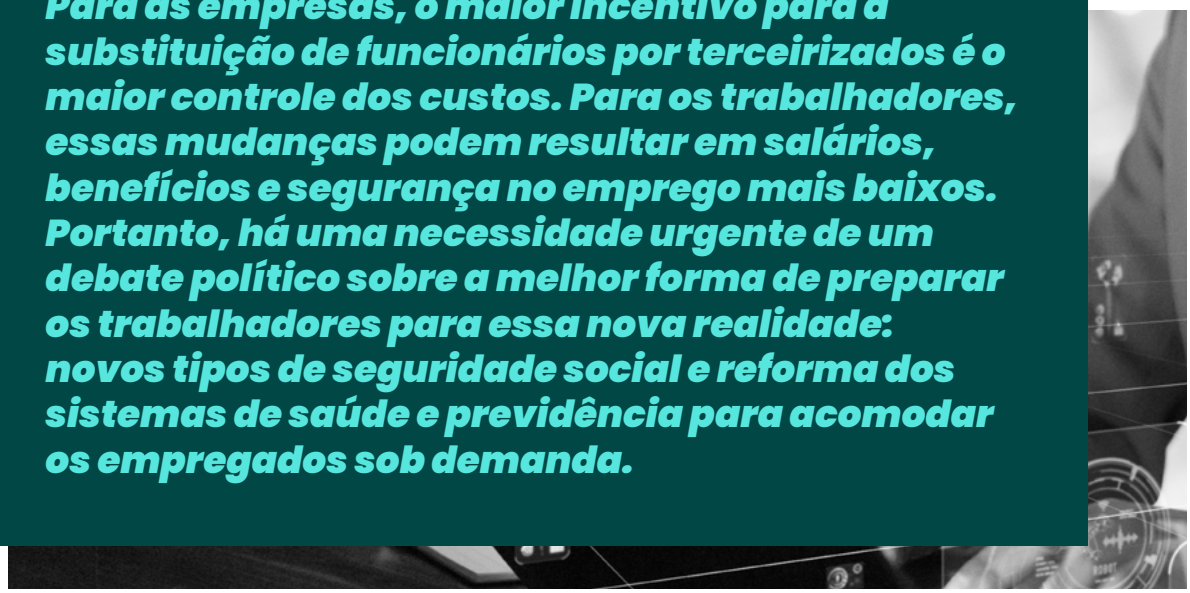


Se observa um debate global sobre esses "novos trabalhos" e as inéditas categorias de "trabalhadores independentes".[10] Na linha de um documento elaborado e publicado pelo Governo do Reino Unido: a *Gig Economy* envolve a "troca de trabalho por dinheiro entre indivíduos ou empresas por meio de plataformas digitais que facilitam ativamente a correspondência entre provedores e clientes, em uma base de curto prazo e pagamento por tarefa".[11] Aqui se tem os efeitos que essa "Nova Economia" trará para os trabalhadores e o meio ambiente do trabalho como se conhece até este momento.

Klaus Schwab descreve diversos impactos no meio ambiente do trabalho, que serão gerados pelos avanços das tecnologias convergentes da Quarta Revolução Industrial, afetando também o trabalhador, como a extinção de muitos postos de trabalho e diversas profissões; surgirão novos trabalhos e postos de trabalhos; aumentará o número de desempregados; a emergência de novas modalidades de segregação entre segmentos de baixa competência/baixo salário e alta competência/alto salário; a ampliação da economia sob demanda; a organização de "nuvem humana" onde as atividades são estruturadas em atribuições e projetos distintos, ou seja, essas atividades profissionais são lançadas em nuvens virtuais de potenciais trabalhadores, que serão localizados pelos empregadores, em qualquer lugar do mundo. Essas características evidenciam uma efetiva revolução no trabalho, que estará vinculado à conexão a uma rede virtual mundial.[12]

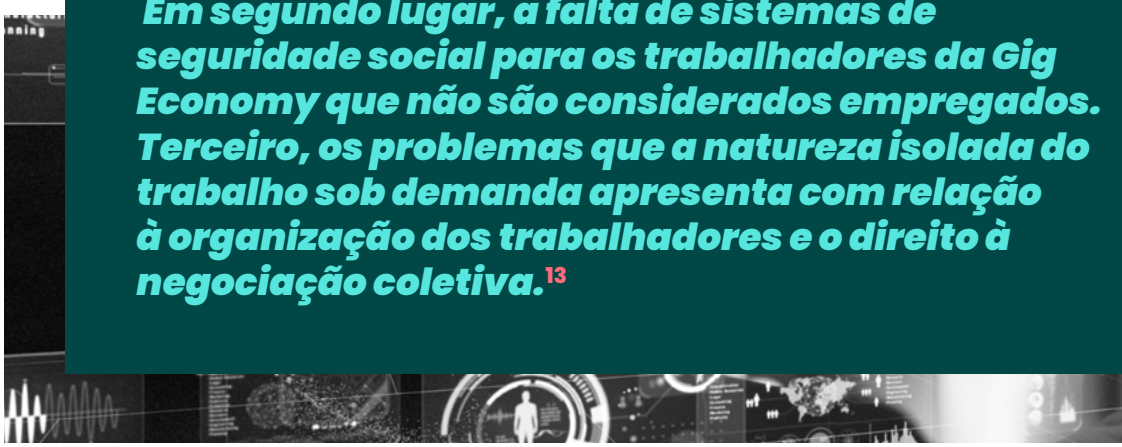
As plataformas de trabalho digitais permitem ganhos de eficiência ao facilitar a correspondência entre a oferta e a demanda de setores de serviços. Ao mesmo tempo, causam desafios significativos no mercado de trabalho devido ao tipo de empregos que criam e às implicações que esses arranjos de trabalho têm para um segmento crescente da população que deles participa.

Para as empresas, o maior incentivo para a substituição de funcionários por terceirizados é o maior controle dos custos. Para os trabalhadores, essas mudanças podem resultar em salários, benefícios e segurança no emprego mais baixos. Portanto, há uma necessidade urgente de um debate político sobre a melhor forma de preparar os trabalhadores para essa nova realidade: novos tipos de seguridade social e reforma dos sistemas de saúde e previdência para acomodar os empregados sob demanda.



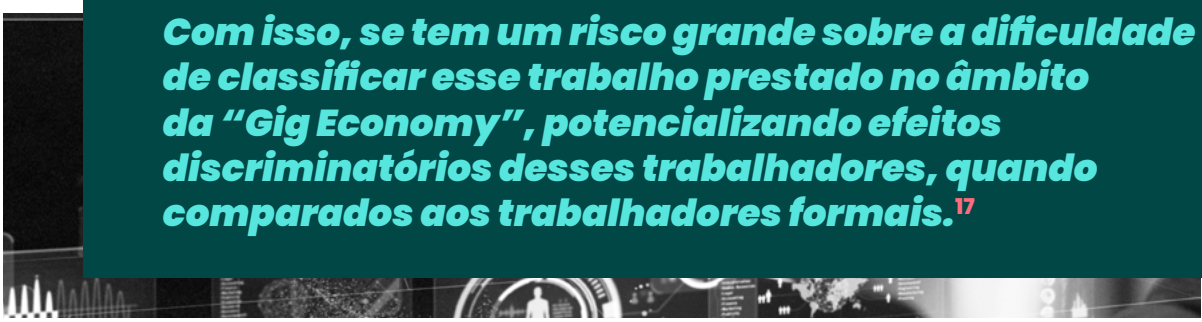
Outros desafios que essas novidades trazem: a probabilidade de se caracterizar erros de classificação do trabalhador em plataformas de trabalho digital. Isso é relevante porque os benefícios e proteções dos trabalhadores se estabelecem de acordo com uma classificação realizada pelo próprio algoritmo e definem a base jurídica sobre a qual as disputas entre diversos colaboradores podem ser resolvidas.

Em segundo lugar, a falta de sistemas de seguridade social para os trabalhadores da Gig Economy que não são considerados empregados. Terceiro, os problemas que a natureza isolada do trabalho sob demanda apresenta com relação à organização dos trabalhadores e o direito à negociação coletiva.[13]



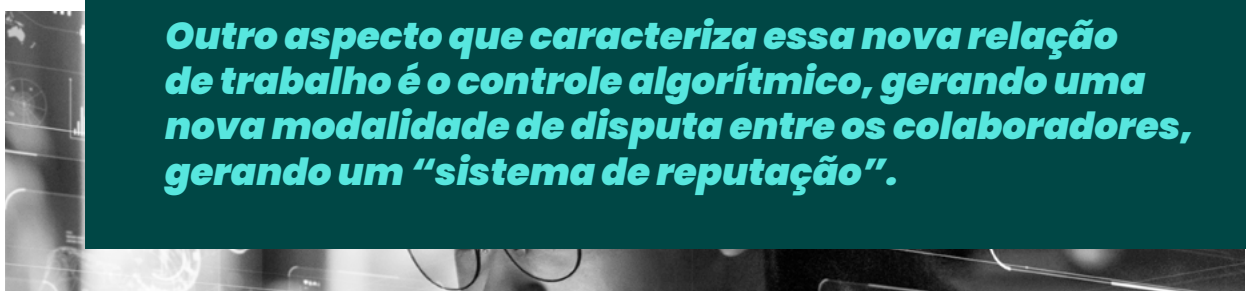
Do ponto de vista do mercado de trabalho, a "economia de compartilhamento digital", que é outra denominação da *Gig Economy*, não faz parte da economia formal, que se caracteriza por ser "baseada no emprego de mão de obra assalariada dentro de um quadro de regras e regulamentos, usualmente concebidos e implementados pelo Estado, sobre o trabalho horas, salários mínimos, saúde e segurança no trabalho ou obrigações de seguridade social de empregadores e empregados".[14] Os empregos na economia formal, ao contrário dos empregos na economia compartilhada, são protegidos até certo ponto, com salários regulares e com a contribuição (formal) dos trabalhadores para os serviços públicos por meio do pagamento de impostos sobre sua renda.[15]

Em contraste, a economia informal – onde está a *Gig Economy* – é definida como "composta por todas as formas de 'emprego informal' – isto é, emprego sem contratos formais (ou seja, coberto pela legislação trabalhista), benefícios trabalhistas ou proteção social [e o] trabalho assalariado em empregos informais". Considerando-se essas diferenças, a denominada "Nova Economia", sustentada, em grande medida pela "economia do compartilhamento", traz um variado cardápio de benefícios para os "proprietários" dos novos modelos de trabalho, dentre os quais se destacam os fiscais e a desnecessidade de cumprir a legislação trabalhista e previdenciária em relação aos seus "colaboradores". Esses aspectos acabam gerando uma modalidade de concorrência desleal com as atividades formalizadas, que ficam obrigadas a todas as obrigações fiscais e tributárias.[16]



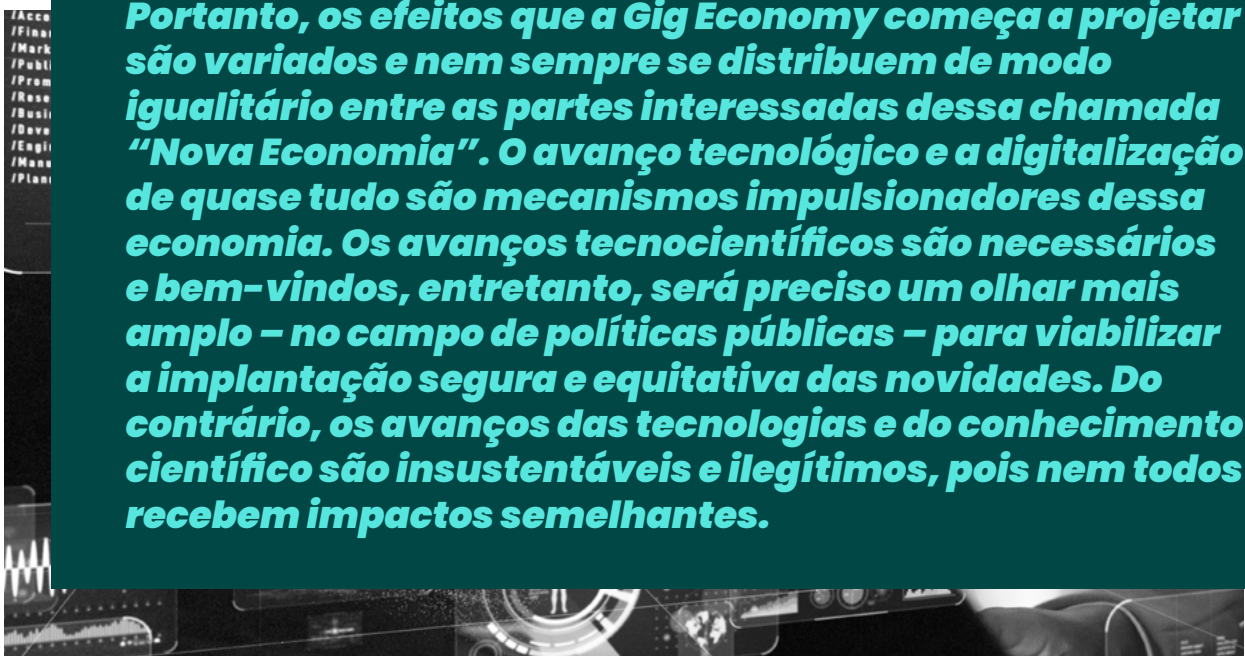
Com isso, se tem um risco grande sobre a dificuldade de classificar esse trabalho prestado no âmbito da "Gig Economy", potencializando efeitos discriminatórios desses trabalhadores, quando comparados aos trabalhadores formais.[17]

Nessa "Nova Economia", os ditos "empregadores" trabalham com um baixo nível de responsabilidade pelos seus colaboradores, podendo encerrar unilateralmente a relação com o "empregado", sem o pagamento de verbas rescisórias.[18]



Outro aspecto que caracteriza essa nova relação de trabalho é o controle algorítmico, gerando uma nova modalidade de disputa entre os colaboradores, gerando um "sistema de reputação".

Nesse espaço virtual se tem uma constante vigilância de todos sobre todos, abrindo problemas com relação à privacidade e o compartilhamento, muitas vezes não compreendido ou não autorizado, de dados pessoais. Esses "novos trabalhos" operam por tarefas, muitas vezes sustentadas em arranjos casuais, sazonais e baseados em contratos temporários. Aqui se abre uma frente para questões éticas de variadas dimensões, expondo uma nova faceta do cruzamento da flexibilidade e precariedade das "relações laborais" que se estabelecem entre os trabalhadores e os "proprietários dos novos trabalhos".



Portanto, os efeitos que a Gig Economy começa a projetar são variados e nem sempre se distribuem de modo igualitário entre as partes interessadas dessa chamada "Nova Economia". O avanço tecnológico e a digitalização de quase tudo são mecanismos impulsionadores dessa economia. Os avanços tecnocientíficos são necessários e bem-vindos, entretanto, será preciso um olhar mais amplo – no campo de políticas públicas – para viabilizar a implantação segura e equitativa das novidades. Do contrário, os avanços das tecnologias e do conhecimento científico são insustentáveis e ilegítimos, pois nem todos recebem impactos semelhantes.

Wilson Engelmann

Pós-Doutor em Direito Público-Direitos Humanos, Universidade de Santiago de Compostela, Espanha; Doutor e Mestre em Direito Público, Programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos – UNISINOS, RS, Brasil; Professor e Pesquisador do Mestrado Profissional em Direito da Empresa e dos Negócios e do Programa de Pós-Graduação em Direito - Mestrado e Doutorado ambos da UNISINOS; Bolsista de Produtividade em Pesquisa do CNPq; e-mail: wengelmann@unisinos.br; ORCID: https://orcid.org/0000-0002-0012-3559

NOTAS E REFERÊNCIAS

1 FLORIDI, Luciano (editor) e outros. The Onlife Manifesto: being human in a Hyper-connected Era. Londres: Springer Open, 2015, edição digital. p. 1.

2 Ibidem, p. 7.

3 SCHWAB, Klaus. A quarta revolução industrial. Tradução Daniel Moreira Miranda. São Paulo: EDIPRO, 2016 e SCHWAB, Klaus; DAVIS, Nicholas. Aplicando a quarta revolução industrial. Tradução Daniel Moreira Miranda. São Paulo: EDIPRO, 2018.

4 CHARLTON, Emma. What is the gig economy and what's the deal for gig workers? Fórum Econômico Mundial. 26 May 2021. Disponível em: https://www.weforum.org/agenda/2021/05/what-gig-economy-workers/. Acesso em 13 set. 2021.

5 Para ampliar, sugere-se a consulta: CENTRO DE GESTÃO E ESTUDOS ESTRATÉGICOS – CGEE. Desenvolvimento tecnológico e mercado de trabalho – Digitalização e relação homem-máquina: mudanças e tendências na legislação em nível global. Brasília: Centro de Gestão e Estudos Estratégicos, 2021; CENTRO DE GESTÃO E ESTUDOS ESTRATÉGICOS - CGEE. Desenvolvimento tecnológico e mercado de trabalho – Subsídios para políticas públicas. Brasília: Centro de Gestão e Estudos Estratégicos, 2021; CENTRO DE GESTÃO E ESTUDOS ESTRATÉGICOS – CGEE. Desenvolvimento tecnológico e mercado de trabalho – Estudo sobre relações de trabalho no setor financeiro. Brasília: Centro de Gestão e Estudos Estratégicos, 2021.

6 SCHWAB, Klaus; DAVIS, Nicholas. Aplicando a quarta revolução industrial. Tradução Daniel Moreira Miranda. São Paulo: EDIPRO, 2018.

7 Para aprofundar: ENGELMANN, Wilson. Nanotecnologia e direitos humanos. In: Cadernos de Dereito Actual, Santiago de Compostela, Espanha, n. 9. Núm. Ordinário, 2018, p. 441-487. Disponível em http://www.cadernosdedereitoactual.es/ojs/index.php/cadernos/article/view/325/201. Acesso em 13 set. 2021.

8 FREEMAN, Robert Edward. Strategic Management: a stakeholder approach. Cambridge: Cambridge University Press, 2010.

9 BOCCIA, Sandra. Por uma nova narrativa para os negócios. Revista Época Negócios, n. 141, novembro de 2018, p. 96.

10 CHARLTON, Emma. What is the gig economy and what's the deal for gig workers? Fórum Econômico Mundial. 26 May 2021. Disponível em: https://www.weforum.org/agenda/2021/05/what-gig-economy-workers/. Acesso em 13 set. 2021.

11 Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/687553/The_characteristics_of_those_in_the_gig_economy.pdf. Acesso em 08 set. 2021.

12 SCHWAB, Klaus. A quarta revolução industrial. Tradução Daniel Moreira Miranda. São Paulo: EDIPRO, 2016; CASTELLS, Manuel. A galáxia da internet: reflexões sobre a

internet, os negócios e a sociedade. Tradução Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2003, p. 77-82; O'CONNOR, Sarah. The human cloud: a new world of work. In: The Financial Times, de 08 outubro 2015. Disponível em: https://www.ft.com/content/a4b6e13e-675e-11e5-97d0-1456a776a4f5. Acesso em 08 set. 2021.

13 ARTECONA, Raquel; CHAU, Terence. Labour issues in the digital economy. ECLAC - Studies and Perspectives n. 17 – Washington, D.C. Agosto de 2017. Disponível em: https://repositorio.cepal.org/bitstream/handle/11362/42046/1/S1700563_en.pdf. Acesso em 08 set. 2021.

14 Daniels, P.W., 2004. Urban challenges: the formal and informal economies in mega-cities. In Cities, v. 21, 501–511. Essa citação se encontra na p. 504.

15 Daniels, P.W., 2004. Urban challenges: the formal and informal economies in mega-cities. In: Cities, v. 21, 501–511.

16 POURI, Maria J.; HILTY, Lorenz M. The digital sharing economy: A confluence of technical and social sharing. Environmental Innovation and Societal Transitions, v. 38, 2021, p. 127-139.

17 MING TAN, Zhi; AGGARWAL, Nikita; COWLS, Josh; MORLEY, Jessica; TADDEO, Mariarosaria; FLORIDI, Luciano. The ethical debate about the gig economy: a review and critical analysis. Technology in Society, v. 65, 2021. Disponível em: http://www.elsevier.com/locate/techsoc. Acesso em 13 set. 2021.

18 GOSWANI, Manisha. Revolutionizing employee employer relationship via gig economy. Materials Today: proceedings. Esse artigo ainda não está publicado de modo online, foi aceito para publicação em 17 de setembro de 2020. Por isso, se encontra em pré-visualização no seguinte endereço: www.elsevier.com/locate/matpr. Acesso em 13 set. 2021.

doi.org/10.52959/2021535419

COMO O ATIVISMO DIGITAL PODE SER USADO PARA ENFRENTAR DESIGUALDADES SOCIOECONÔMICAS E DIVISÕES DIGITAIS?

Clovis Freire

A pandemia da COVID-19 nos mostrou o papel crítico das tecnologias digitais para mitigar o impacto da crise em tantas áreas, utilizando soluções digitais como *e-learning*, *e-health*, teletrabalho, *e-commerce* e *e-government*. Ao mesmo tempo, a pandemia também expôs vários *gaps* digitais. A falta de acesso à internet, a baixa velocidade da rede, as disparidades nas habilidades de uso das tecnologias e fatores sociais têm afetado o acesso e a participação das pessoas na economia e na sociedade por meios digitais. Muitas empresas não estavam prontas para usar tecnologias digitais para mitigar a crise porque não tinham implantado soluções digitais em suas funções principais.

Essas divisões digitais expuseram o fato de que as desigualdades digitais e socioeconômicas se tornaram interligadas. Com o mundo digital e o mundo físico se tornando mais integrados, para fechar a brecha digital temos que também enfrentar as desigualdades socioeconômicas. Não é possível enfrentar um sem atacar o outro.

Nesse sentido, qual é o papel do ativismo civil na redução das desigualdades socioeconômicas e digitais?

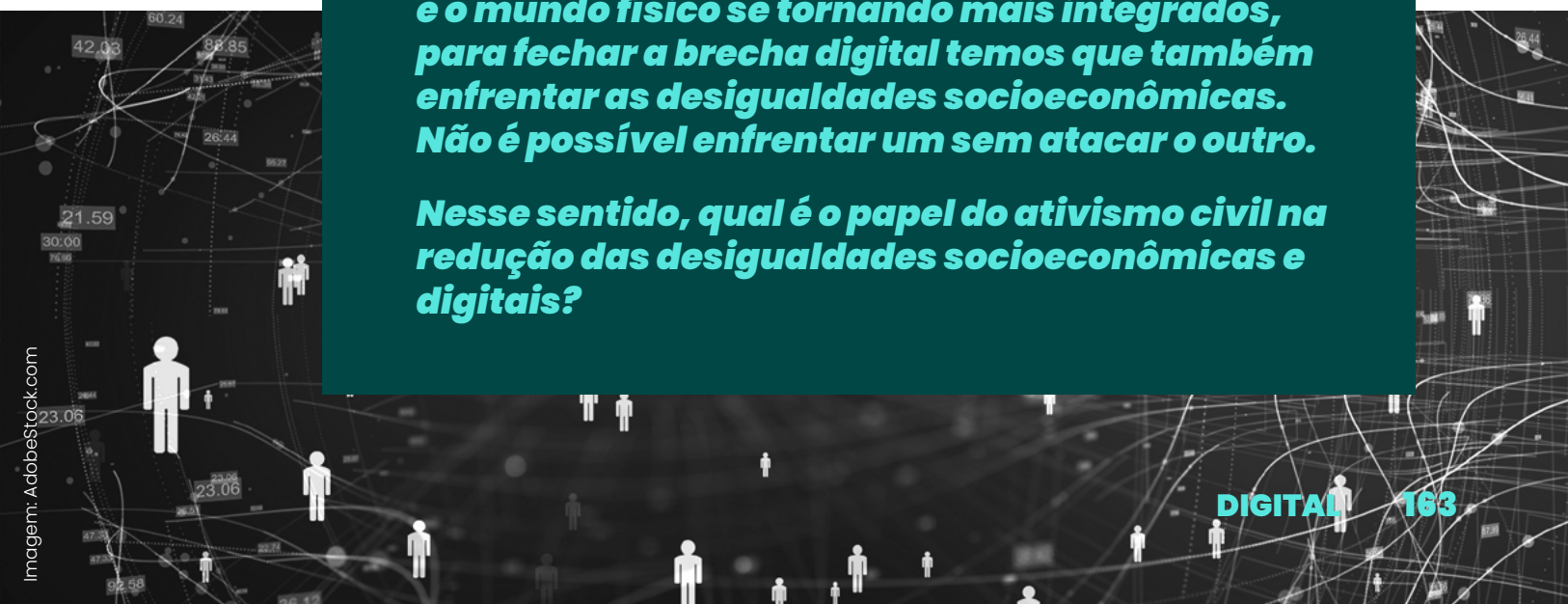


Imagem: AdobeStock.com

DESIGUALDADES SOCIOECONÔMICAS E DIGITAIS

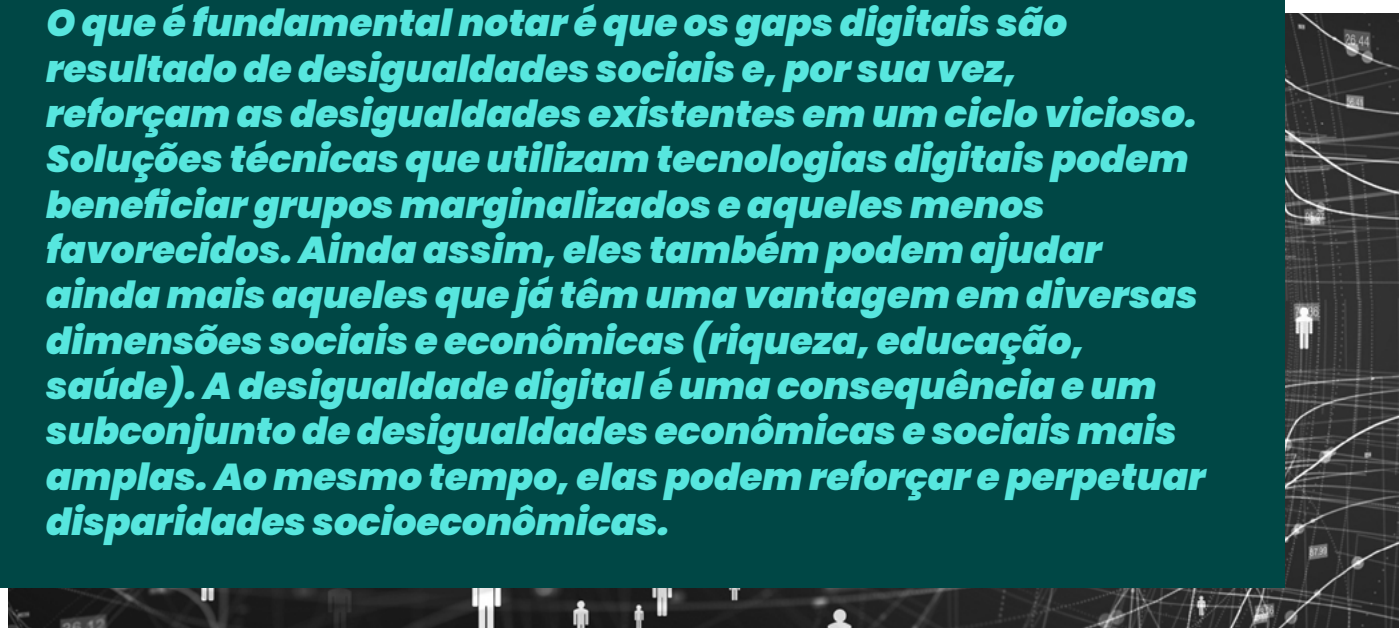
Para responder a essa pergunta, temos primeiro que entender melhor o *status* e a relação entre as desigualdades socioeconômicas e a divisão digital.

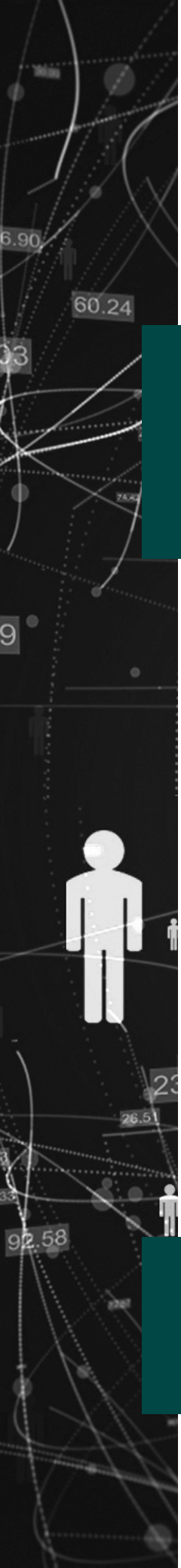
Vivemos em um tempo de crescente prosperidade. As pessoas, em média, estão vivendo uma vida mais longa e saudável, obtendo mais anos de educação e tendo melhor acesso à água limpa, saneamento e eletricidade. Uma classe média global emergiu, alimentada pelo rápido crescimento das economias emergentes. Também tivemos grandes ganhos na implantação e acesso a tecnologias digitais. Os sinais de celular agora atingem mais de 95% da população global, e estima-se que mais de 50% usem a internet[1].

Ao mesmo tempo, há desigualdades crescentes. A pobreza extrema persiste, com mais da metade de todas as pessoas do mundo nessa condição vivendo na África subsaariana[2]. A riqueza é muito concentrada, com o 1% dos mais ricos do mundo possuindo mais riqueza do que 90% da população global[3]. As disparidades de oportunidades em educação, saúde e renda ainda são diretamente afetadas pelas questões de gênero, localização urbana/rural e país de nascimento. Recentemente, o mundo também se concentrou no desafio urgente da justiça racial. Em muitas cidades, as pessoas têm participado de protestos generalizados contra o racismo sistêmico e as divisões que ele perpetua.

Em relação às tecnologias digitais, há grandes divisões digitais dentro e entre os países, particularmente no que diz respeito ao acesso à internet e aos equipamentos digitais. Por exemplo, a proporção de pessoas que usam a rede mundial de computadores em países desenvolvidos é mais de quatro vezes maior que nos países menos desenvolvidos. Em média, as mulheres têm 17% menos chances do que os homens de usar a internet – o *gap* varia de 3% nos países desenvolvidos a 43% nos países menos desenvolvidos[4].

O que é fundamental notar é que os gaps digitais são resultado de desigualdades sociais e, por sua vez, reforçam as desigualdades existentes em um ciclo vicioso. Soluções técnicas que utilizam tecnologias digitais podem beneficiar grupos marginalizados e aqueles menos favorecidos. Ainda assim, eles também podem ajudar ainda mais aqueles que já têm uma vantagem em diversas dimensões sociais e econômicas (riqueza, educação, saúde). A desigualdade digital é uma consequência e um subconjunto de desigualdades econômicas e sociais mais amplas. Ao mesmo tempo, elas podem reforçar e perpetuar disparidades socioeconômicas.





ENFRENTANDO AS DIVISÕES

À medida que novas tecnologias digitais são desenvolvidas e os mundos digital e físico ficam mais conectados, as desigualdades digitais e sociais se tornarão cada vez mais conectadas. Por isso, precisamos enfrentar simultaneamente as desigualdades sociais e digitais.

As políticas para resolver a divisão digital precisam ser multidimensionais: tecnológicas, econômicas, educacionais, sociais e persuasivas (conscientização). É isso que vemos nas diferentes perspectivas políticas ao lidar com a divisão digital:

- O foco da perspectiva tecnológica é o acesso físico para garantir a disponibilidade.
- A perspectiva econômica se concentra em apoiar o setor de TICs – mercados, concorrência e inovação, para aumentar a disponibilidade e a acessibilidade das TICs.
- A perspectiva educacional se concentra nas habilidades digitais das pessoas para usar soluções digitais.
- A perspectiva social preocupa-se com a inclusão e a participação de todos. Então o foco é a acessibilidade e relevância das aplicações digitais.
- A perspectiva de conscientização está mais relacionada aos países desenvolvidos e lida com pessoas que não usam soluções digitais porque não querem ou têm algumas preocupações digitais, com segurança de dados, por exemplo.
- A perspectiva mais recente apoia a digitalização dos setores produtivos e a transformação estrutural. O foco está na produção em vez de *e-commerce* ou finanças digitais.

A divisão digital é um problema complexo e todas essas perspectivas são válidas e necessárias.

Além disso, as políticas de enfrentamento à divisão digital também devem fazer parte das políticas sociais destinadas a enfrentar as disparidades socioeconômicas.

DUAS ONDAS DE MUDANÇA TECNOLÓGICA

As desigualdades também são afetadas por revoluções tecnológicas, como foi com a revolução industrial, a era do vapor e dos trilhos, a era da produção em massa e a revolução digital. Cada uma dessas pode ser vista como compostas por duas etapas: instalação e implantação[5]. Na fase de instalação, a renda dos trabalhadores e empresários nos setores centrais do novo paradigma pode aumentar muito mais rápido do que para o resto da força de trabalho, aumentando as desigualdades de renda. A segunda etapa é a implantação, que tende a ser desigual; nem todos têm acesso imediato aos benefícios do progresso, e as divisões resultantes podem levar ao descontentamento público.

É fundamental perceber que, atualmente, não há apenas uma, mas duas ondas de mudança tecnológica.

Uma delas é a revolução digital das tecnologias Web 2.0, e essa onda está no seu auge na fase de implantação. Já afetou a maioria dos setores dos países desenvolvidos e fez bons avanços nos países em desenvolvimento de maior renda. Estamos agora vendo um grande impulso para a digitalização e o comércio eletrônico nos países em desenvolvimento de baixa renda. Para se ter uma perspectiva, a UNCTAD estima que as vendas globais de comércio eletrônico atingiram US$ 26,7 trilhões em 2019[6]. Estima-se que 1,5 bilhão de pessoas, ou mais de um quarto da população mundial com mais de 15 anos, compraram *online* em 2019[7].

A outra onda tecnológica é baseada em tecnologias como inteligência artificial, robótica, Internet das Coisas (IoT), *blockchain* e outras associadas à indústria 4.0. Essa onda está em seu estágio inicial de instalação no paradigma da revolução tecnológica. Como apontado no Relatório de Tecnologia e Inovação 2021 da UNCTAD[8], essas tecnologias representam um mercado de US$ 350 bilhões, e alguns sugerem que ela pode crescer para mais de US$ 3,2 trilhões até 2025.

No entanto, essas revoluções tecnológicas ainda não são a realidade para a maioria das pessoas em países em desenvolvimento de baixa renda.

Essas grandes ondas de mudança tecnológica realmente se comportam como ondas que começam em um ou dois dos países mais tecnologicamente avançados e depois se espalham pelo mundo – primeiro para outras economias avançadas, depois para setores mais complexos de economias emergentes, e ao longo do tempo elas se movem em direção às economias mais periféricas.

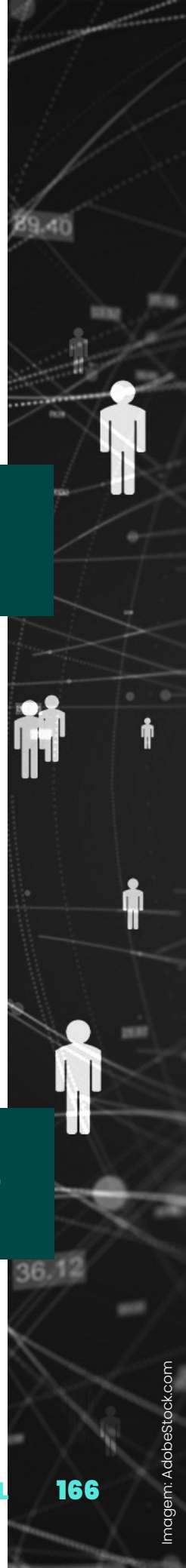
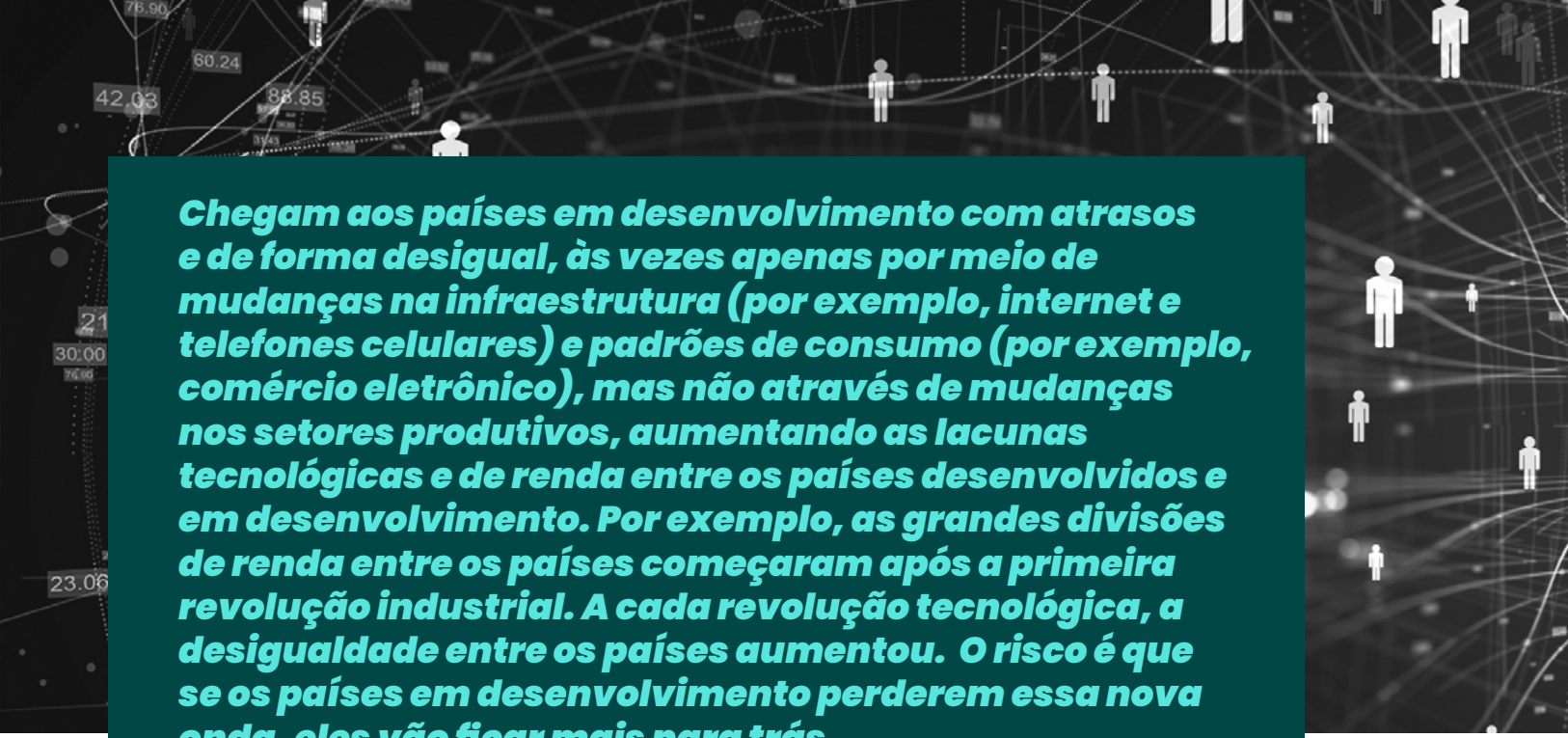


Imagem: AdobeStock.com



Chegam aos países em desenvolvimento com atrasos e de forma desigual, às vezes apenas por meio de mudanças na infraestrutura (por exemplo, internet e telefones celulares) e padrões de consumo (por exemplo, comércio eletrônico), mas não através de mudanças nos setores produtivos, aumentando as lacunas tecnológicas e de renda entre os países desenvolvidos e em desenvolvimento. Por exemplo, as grandes divisões de renda entre os países começaram após a primeira revolução industrial. A cada revolução tecnológica, a desigualdade entre os países aumentou. O risco é que se os países em desenvolvimento perderem essa nova onda, eles vão ficar mais para trás.

O PAPEL DO ATIVISMO DIGITAL

Nesse contexto, qual é o papel do ativismo digital?

Vamos começar com o papel do ativismo social em geral. Podemos destacar cinco áreas em que o ativismo é crítico:

Primeiro, para continuar a conscientizar as pessoas sobre todas as formas de divisões socioeconômicas e digitais, atrair a opinião pública e promover ações coletivas de mudança. Existem diversos exemplos dessa forma de ativismo, como o movimento "*black lives matter*"[9], que utiliza plataformas *web* e mídia social para disseminar informações sobre racismo, para organizar petições pedindo mudanças nas regras e regulamentos que consideram tendenciosas, e organizar manifestações para conscientizar e pressionar o governo por mudanças.

Em segundo lugar, a disseminação de tecnologias digitais e de fronteira e as mudanças que elas resultam na economia exigirão transformações na sociedade e nas instituições, que tendem a ser atrasadas em relação à mudança econômica devido à inércia social e institucional. Leis, regulamentos e comportamentos adequados para lidar com os desafios das tecnologias anteriores são geralmente inadequados para enfrentar novos desafios, mas leva tempo para que sofram alterações. Em revoluções tecnológicas passadas, levou uma ou duas gerações para ter essas mudanças concluídas.

O ativismo social é necessário para que as pessoas percebam que existe o descompasso entre sistemas tecnoeconômicos e sistemas societário-institucionais, para quebrar a inércia e promover as mudanças sociais necessárias.

Um exemplo é a *Association for Progressive Communications,* que usa o ativismo social para mostrar a importância do acesso à internet no mundo de hoje e promove ações concretas para ajudar grupos locais a usar a tecnologia para desenvolver suas comunidades e promover seus direitos[10].

Em terceiro lugar, o ativismo social é necessário para manter governos e empresas, incluindo o setor financeiro, responsáveis pelos papeis que desempenham no desenvolvimento e disseminação das tecnologias digitais. E é necessário manter todos comprometidos com os objetivos de desenvolvimento sustentável, o desenvolvimento humano a longo prazo e a proteção do planeta.

Por exemplo, o *Grupo ETC,* das Filipinas, trabalha para abordar as questões socioeconômicas e ecológicas em torno de novas tecnologias que poderiam ter um impacto sobre as pessoas mais pobres e vulneráveis do mundo[11].

Em quarto lugar, alguns dos temas mobilizadores de movimentos organizados da sociedade civil já são bem conhecidos, como a igualdade de gênero, os riscos das mudanças climáticas e a necessidade de ação para evitá-los, ou a luta contra o racismo. Mas a mudança tecnológica apresenta essas questões em novas formas e também traz à tona novas questões, que para muitas pessoas ainda não estão "no radar", como privacidade de dados e questões éticas relacionadas ao uso das mídias sociais. Assim, o ativismo social nessas áreas serve ao propósito essencial de conscientização.

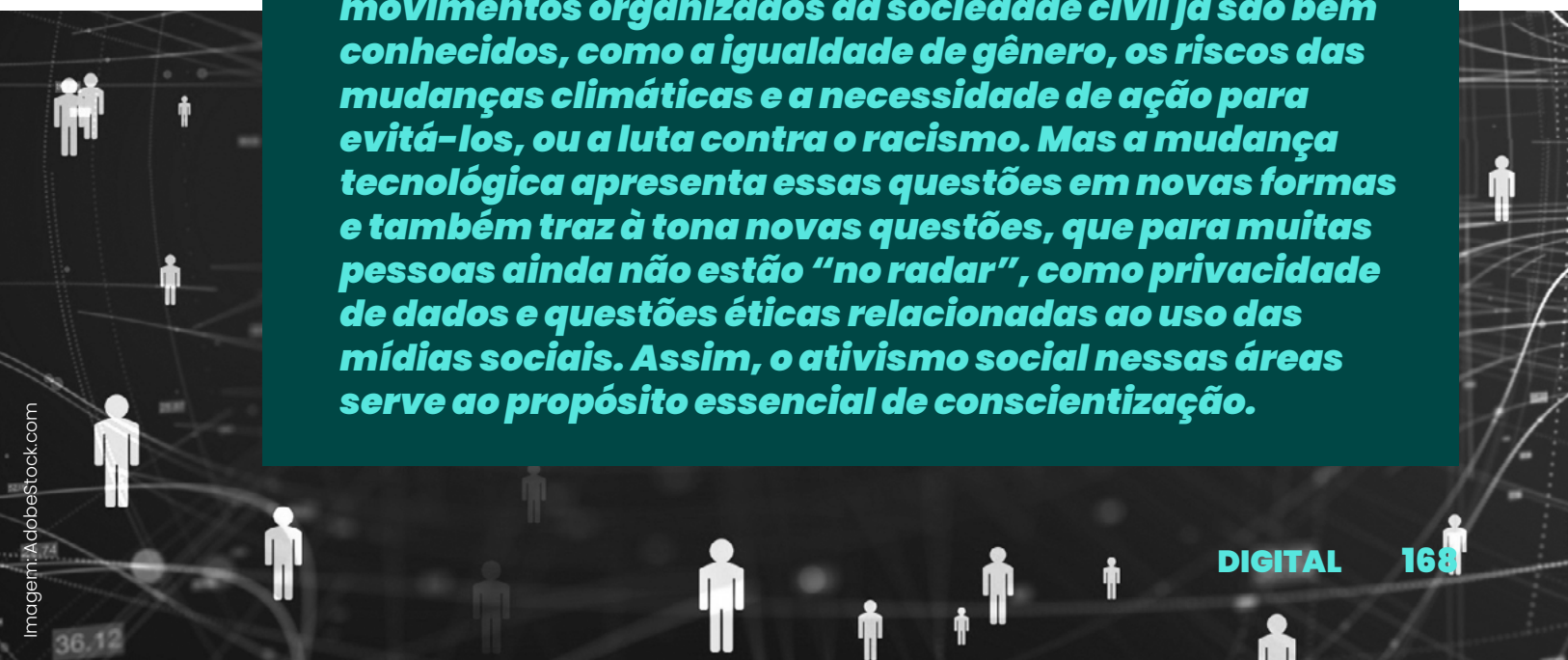


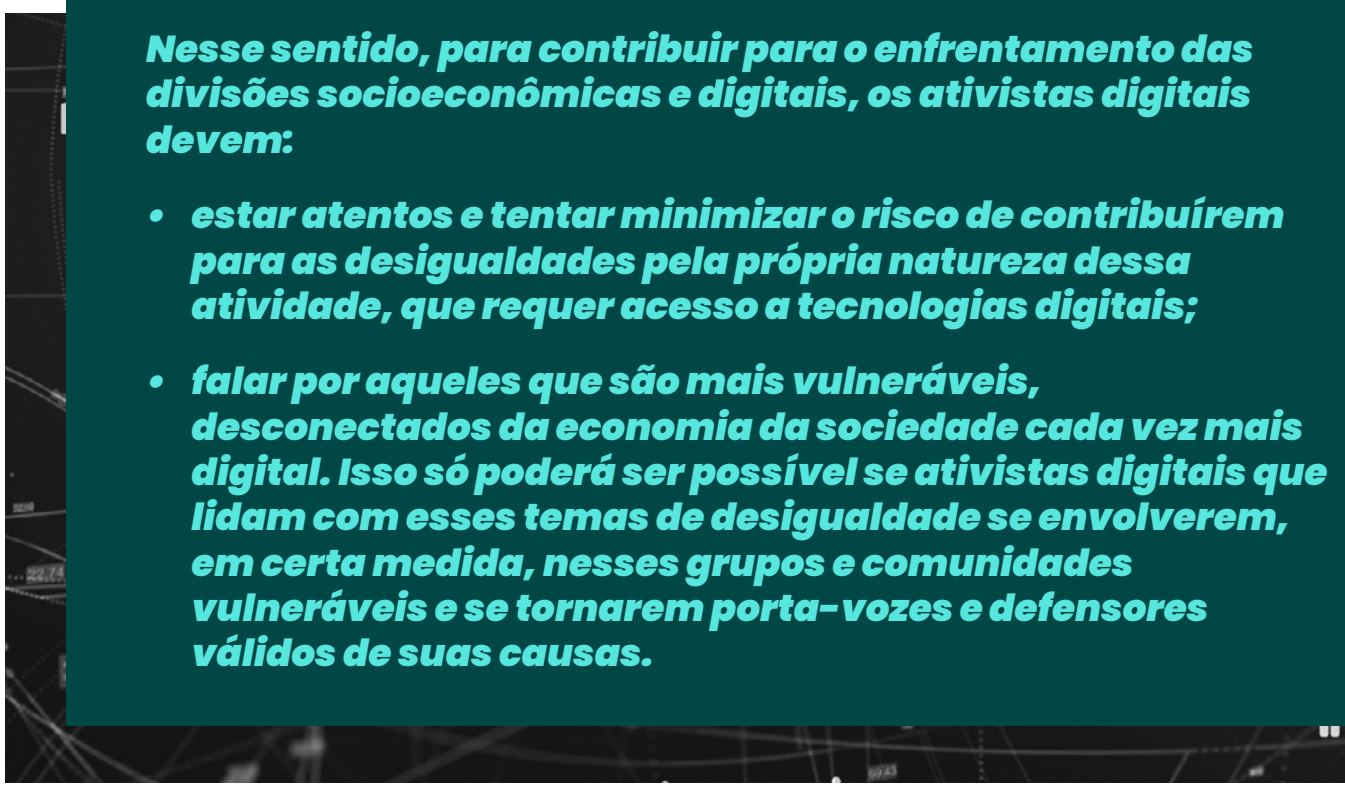
Imagem: AdobeStock.com

No caso da privacidade de dados, por exemplo, existem várias organizações com diferentes afiliações políticas que promovem questões de segurança e privacidade de dados, como o Center for Democracy and Technology (CDT)[12] e a Electronic Frontier Foundation (EFF).[13]

E, quinto, pode levar tempo, mas os esforços combinados dos grupos da sociedade civil podem eventualmente criar uma massa crítica que poderia desencadear mudanças no comportamento dos usuários e consumidores e mudanças em regulamentações, leis e práticas no lado da oferta que poderiam alinhar o desenvolvimento tecnológico com os objetivos sociais.

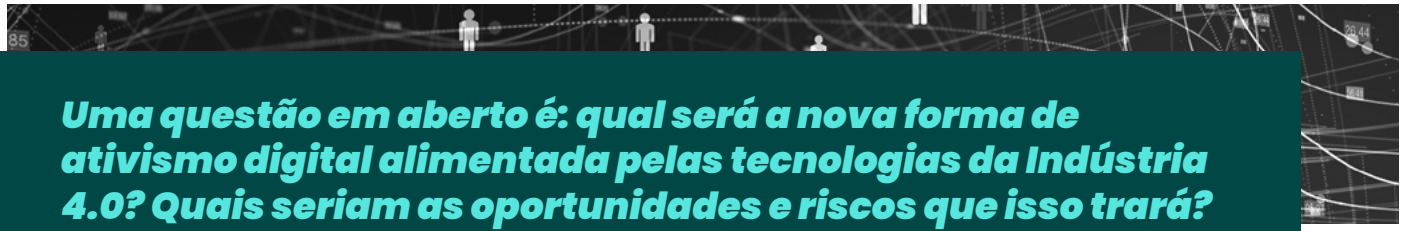
O ativismo digital, como parte do ativismo social, pode e deve contribuir para cada uma dessas áreas. O que é particular ao ativismo digital é que ele é fruto da revolução tecnológica das TIC. Portanto, pode aproveitar tecnologias digitais para aumentar o impacto do ativismo social no enfrentamento das disparidades em todas as suas formas.

Também é importante notar que os ativistas digitais são, por definição, usuários de tecnologias digitais. Seu público-alvo imediato é composto por pessoas com algum nível de acesso a essas tecnologias.



Nesse sentido, para contribuir para o enfrentamento das divisões socioeconômicas e digitais, os ativistas digitais devem:

- ***estar atentos e tentar minimizar o risco de contribuírem para as desigualdades pela própria natureza dessa atividade, que requer acesso a tecnologias digitais;***
- ***falar por aqueles que são mais vulneráveis, desconectados da economia da sociedade cada vez mais digital. Isso só poderá ser possível se ativistas digitais que lidam com esses temas de desigualdade se envolverem, em certa medida, nesses grupos e comunidades vulneráveis e se tornarem porta-vozes e defensores válidos de suas causas.***



Uma questão em aberto é: qual será a nova forma de ativismo digital alimentada pelas tecnologias da Indústria 4.0? Quais seriam as oportunidades e riscos que isso trará?

Em resumo, o ativismo digital pode contribuir muito para o enfrentamento das divisões socioeconômicas e digitais. Ativistas digitais podem usar tecnologias para conscientizar as pessoas sobre várias disparidades, tanto as antigas quanto as novas, quebrar a inércia da mudança social e pressionar pelas mudanças de comportamento e instituições necessárias. No entanto, também é fundamental que o ativismo digital seja autoconsciente de como pode afetar as desigualdades de forma positiva e negativa e minimizar os riscos potenciais de contribuir para o problema.

Clovis Freire

Clovis Freire é economista e trabalha na Divisão de Tecnologia e Logística da Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD). É Engenheiro de Computação pelo ITA com doutorado em Economia pela UNU-MERIT/Universidade de Maastricht, especializado em Economia da Inovação e das Mudanças Tecnológicas. Ele coordenou e foi o principal autor do Relatório de Tecnologia e Inovação 2021 da UNCTAD, com foco em como os países em desenvolvimento podem navegar a nova onda de mudanças tecnológicas para impulsionar a transformação estrutural e o desenvolvimento sustentável, minimizando os riscos do aumento das desigualdades. Antes de ingressar na UNCTAD, em seus 18 anos na Organização das Nações Unidas, Clovis trabalhou no Departamento de Assuntos Econômicos e Sociais em Nova York e na Comissão Econômica e Social para a Ásia e o Pacífico, em Bangkok, em diversas questões relacionadas à tecnologia e desenvolvimento socioeconômico.

Imagem: AdobeStock.com

NOTAS E REFERÊNCIAS

1 https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf

2 https://unstats.un.org/sdgs/report/2019/goal-01/

3 Coffey C et al. (2020). Time to care: unpaid and underpaid care work and the global inequality crisis. Oxfam. https://oxfamilibrary.openrepository.com/bitstream/handle/10546/620928/bp-time-to-care-inequality-200120-en.pdf

4 https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf

5 Ver Perez C (2002). Technological Revolutions and Financial Capital: The Dynamics of Bubbles and Golden Ages. Edward Elgar Pub. Cheltenham.

6 UNCTAD (2020). Estimates of global e-commerce 2019 and preliminary assessment of COVID-19 impact on online retail 2020. UNCTAD Technical Notes on ICT for Development, Number 18. Geneva. https://unctad.org/system/files/official-document/tn_unctad_ict4d18_en.pdf

7 Ibid.

8 UNCTAD (2021). Catching Technological Waves: Innovation with Equity. (United Nations publication Sales No. E.21.II.D.8. New York and Geneva). https://unctad.org/system/files/official-document/tir2020_en.pdf

9 https://blacklivesmatter.com/

10 https://apc.org/

11 https://www.etcgroup.org/

12 https://cdt.org/

13 https://www.eff.org/

patrocínio

ABDI Agência Brasileira de Desenvolvimento Industrial

cgee Centro de Gestão e Estudos Estratégicos *Ciência, Tecnologia e Inovação*

SEBRAE

stefanini GROUP

TecBan

TOTVS

realização

FDC