LEGISLAÇÃO, ÉTICA E CONFORMIDADE

AULA 6

Prof. Jailson de Souza Araújo

CONVERSA INICIAL

Crimes virtuais e relações de trabalho: legislação e conformidade na Era Digital

Nesta etapa, apresentaremos temas relacionados aos crimes virtuais e às relações de trabalho, analisando a legislação em vigor e iniciativas legislativas, bem como a necessidade da adoção de boas práticas de conformidade para prevenir riscos e crimes informáticos, com o objetivo de promover a segurança e a conformidade na era digital.

Abordaremos os impactos da pandemia de Covid-19 em relação ao teletrabalho, notadamente a Medida Provisória n. 927, de 2020, e a Lei 14.442/2022, que regulamentou o teletrabalho no Brasil.

Finalmente, analisaremos o direito à privacidade do trabalhador em sua atuação laboral, e avaliaremos boas práticas de conformidade relacionadas ao uso de tecnologia da informação e comunicação no local de trabalho, apresentando os direitos, as diretrizes e os limites relacionados ao direito do empregador em supervisionar e monitorar as atividades.

TEMA 1 – CRIMES VIRTUAIS

O desenvolvimento das Tecnologias da Informação e Comunicação (TICs) facilitou o acesso e a difusão de informações, o comércio de produtos e serviços – inclusive via internet –, eliminando barreiras geográficas e facilitando o acesso a produtos e serviços disponíveis no Brasil e no exterior.

Não por acaso, o desenvolvimento do comércio eletrônico está diretamente relacionado à disseminação do uso comercial da internet no Brasil, a partir da década de 1990.

Entretanto, junto com as facilidades trazidas pelas TICs, surgiram novas formas de criminalidade, amparadas pela nova realidade proporcionada pelas relações virtuais, no âmbito da internet.

Para Guilherme de Souza Nucci (2021), o direito penal corresponde ao corpo de normas jurídicas destinado ao combate à criminalidade e à defesa da sociedade, de acordo com o texto de leis penais como o Código Penal (Brasil, 1940).

O direito penal corresponde a um poder soberano do Estado, que se efetiva pela legislação penal, que permite, ao Estado, cumprir sua função originária, que é assegurar as condições de existência e continuidade da organização social.

O Código Penal brasileiro é fruto do Decreto-Lei n. 2.848/1940 (Brasil, 1940). Sua redação tem sido, desde então, atualizada e aperfeiçoada.

Entretanto, seu texto-base remonta a uma época em que a sociedade era analógica, ou seja, uma sociedade cuja comunicação se dava por mídia impressa, rádio, televisão, e na qual as relações negociais eram essencialmente presenciais.

O ritmo das inovações tecnológicas era mais lento se comparado ao de hoje, e os conceitos relacionados à dignidade da pessoa humana e à privacidade eram diferentes da forma como os conhecemos atualmente.

Com o surgimento da sociedade da informação, que Manuel Castells (1999, citado por Boff; Fortes; Freitas, 2018, p. 36) define como a organização social em que há a geração, o processamento e a comunicação da informação como fontes fundamentais de produtividade e poder propiciados por novas tecnologias. Diversas facilidades são proporcionadas pela internet, como oferta de comércio eletrônico, transações bancárias por meio de *internet banking*, realização de pagamentos digitais *on-line* – por intermédio de ferramentas como PayPal, PagSeguro, PicPay, Mercado Pago, Apple Pay, Pix, transferência eletrônica disponível (TED), documento de crédito (DOC), entre outras – ou presenciais, como uso de *Quick Response (QR) Code* ou por aproximação, via comunicação a curta distância (NFC).

Essas formas de pagamento dispensam o uso de dinheiro em espécie (portamos cada vez menos dinheiro), cheque (usamos cada vez menos) ou mesmo a utilização de cartão de crédito de plástico.

Há ainda contratação de produtos e serviços via aplicativos, que também incentivam o uso de pagamento por meio eletrônico.

No contexto da disseminação de práticas comerciais envolvendo pagamentos, contratos e comércio eletrônicos, as empresas que adotam maciçamente tais práticas têm sido vítimas de quadrilhas especializadas em roubo de informações de clientes (senhas, cartões de crédito e dados pessoais) e clonagem de páginas (*phishing*, que induz clientes e consumidores ao erro recebendo pagamentos em nome da empresa clonada), furto de bases de dados

de clientes, fornecedores e colaboradores e sequestro de dados via criptografia (*ransomware*), por meio, inclusive, do uso de técnicas de engenharia social.

Em virtude da pandemia de Covid-19, a adesão a meios de pagamento eletrônicos foi acelerada, notadamente por aqueles que nunca haviam realizado compras pela internet ou utilizado meios de pagamento eletrônicos.

De acordo com Lucca Rossi (2020), o Capterra realizou um estudo sobre o uso de carteiras digitais com 1.002 entrevistados com mais de 18 anos, de diferentes faixas de renda (até 1 salário-mínimo, de 1 a 3, de 3 a 7, de 7 a 15, de 15 a 20, e mais de 20 salários-mínimos) de todas as regiões do país, entre os dias 14 e 21 de julho de 2020.

Os entrevistados deveriam ser trabalhadores em tempo integral ou parcial, *freelancers*/autônomos, estudantes em tempo integral, aposentados, ou terem perdido o emprego durante a crise.

O painel contou com 50% dos entrevistados do sexo feminino e 50% do sexo masculino. O estudo apontou um crescimento de 32% no volume de pagamentos frequentes por dispositivos móveis entre aqueles que possuem carteiras digitais, que permitem realizar as chamadas transações *contactless*, instaladas em seus celulares ou relógios inteligentes (Rossi, 2020).

Ao mesmo tempo em que a TIC aproxima as pessoas, reduz barreiras e promove facilidades para o dia a dia, ela também promove reflexos sociais extremamente negativos, pois gera novas formas de criminalidade capazes de comprometer a segurança do cidadão.

De um dispositivo informático devidamente conectado à internet, é possível realizar crimes contra o patrimônio.

Quadrilhas estão se especializando em crimes que envolvem o uso de carteiras digitais, inclusive com a presença da vítima, como é o caso de sequestros-relâmpagos para coagir a vítima a realizar pagamentos via Pix.

Essa antiga modalidade de crime voltou a ganhar destaque nos meios de comunicação, dada a possibilidade de se transferir rapidamente significativas quantidades de dinheiro, bastando, para isso, que a vítima tenha um celular e saldo bancário.

Neste momento, cabe descrever o que é o crime de estelionato, previsto no art. 171 do Código Penal:

> Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou

> qualquer outro meio fraudulento: Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis. (Brasil, 1940)

Tal tipo penal recebeu novos contornos, pois a cada dia surgem novos golpes proporcionados pelo uso do *e-mail* e do WhatsApp, viabilizados por sofisticadas técnicas de engenharia social

O mais corriqueiro é a clonagem de celular, em que o estelionatário clona o número de celular da vítima, assumindo o controle de seu WhatsApp, e solicita dinheiro emprestado para amigos e familiares da vítima, que, de boa-fé, fazem transferências para a conta bancária indicada pelo estelionatário.

Tem também se tornado comum a utilização indevida de ambientes virtuais (redes sociais, portais de notícias, grupos de aplicativos de mensagens como WhatsApp e Telegram etc.) para a prática de crimes contra a honra, descritos entre os arts. 138 e 140 do Código Penal (1940):

> **Calúnia**
> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:
> Pena - detenção, de seis meses a dois anos, e multa.
> § 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.
> § 2º - É punível a calúnia contra os mortos.
> **Exceção da verdade**
> § 3º - Admite-se a prova da verdade, salvo:
> I - se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível;
> II - se o fato é imputado a qualquer das pessoas indicadas no nº I do art. 141;
> III - se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível.
> **Difamação**
> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
> Pena - detenção, de três meses a um ano, e multa.
> **Exceção da verdade**
> Parágrafo único - A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções.
> **Injúria**
> Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:
> Pena - detenção, de um a seis meses, ou multa.
> § 1º - O juiz pode deixar de aplicar a pena:
> I - quando o ofendido, de forma reprovável, provocou diretamente a injúria;
> II - no caso de retorsão imediata, que consista em outra injúria.
> § 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes:
> Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência.
> § 3o Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência: (Redação dada pela Lei nº 10.741, de 2003)
> Pena - reclusão de um a três anos e multa. (Incluído pela Lei n. 9.459, de 1997)

Diante desses novos fatos sociais e do aprimoramento dos meios utilizados pela criminalidade, a sociedade precisa da adequada proteção do direito penal, que, por sua vez, necessita ser repensado e atualizado para atender adequadamente à sociedade, por meio da proteção do cidadão, evitando que seus bens jurídicos mais relevantes, quais sejam, sua vida, sua liberdade, sua dignidade, sua privacidade e seu patrimônio, sejam lesados, tema que será abordado a seguir.

TEMA 2 – A PREVENÇÃO E O COMBATE AOS CIBERCRIMES

Há inúmeras formas de criminalidade que foram alavancadas pelas TICs, como fraudes bancárias, fraudes em compras públicas, fraudes fiscais, lavagem de dinheiro, clonagem de cartões de crédito, crimes raciais praticados em redes sociais, disseminação de pornografia infantil, entre outras condutas que ferem a dignidade da pessoa humana e violam os direitos humanos.

Tal contexto demanda, inclusive, o aperfeiçoamento das estruturas de atuação do Estado, notadamente dos órgãos responsáveis pela investigação criminal, como é o caso da Polícia Civil (PC) e da Polícia Federal (PF). Não por acaso, vemos a criação de delegacias especializadas em combater a cibercriminalidade.

No âmbito estadual, o Núcleo de Combate aos Cibercrimes (Nuciber), órgão específico da Polícia Civil do Paraná (PCPR), foi criado para combater crimes cometidos por meios eletrônicos, e é responsável pela investigação das infrações penais cometidas com o emprego de recursos tecnológicos de informação computadorizada (*hardwares*, *softwares*, redes de computadores e sistemas móveis de telefonia), e pelo auxílio aos demais órgãos da PC nas investigações e inquéritos policiais ou administrativos em crimes da mesma natureza (Nuciber, 2022).

Já na esfera federal, a Polícia Federal (PF) conta com uma diretoria especializada em crimes cibernéticos, o Serviço de Repressão a Crimes Cibernéticos (SRCC). É importante destacar que a PF, diferentemente da atuação da PC (de âmbito estadual), assume a responsabilidade pela investigação de crimes de natureza transnacional com que o Brasil se comprometeu, por meio de tratados internacionais, e pela apuração de crimes que atentem contra a Administração Pública federal direta ou indireta.

Para tanto, de acordo com o Delegado Federal Marco Aurélio de Macedo Coelho (2017, citado por Combate, 2017), para atuar da melhor forma possível, a PF necessita de ferramentas que auxiliem a corporação a acompanhar o avanço tecnológico; entretanto, em muitos casos, a corporação precisa adquirir as tecnologias. O Delegado Federal Marco Coelho (2017, citado por Combate, 2017), afirma:

> As ferramentas de investigação são essenciais para uma efetiva apuração de crimes cibernéticos em tempo razoável. Quando há o desenvolvimento de ferramentas pela própria PF, uma das vantagens é que não há necessidade de se pagar pela atualização delas.

Ele também esclarece que, mesmo quando a PF possui as ferramentas, são necessárias parcerias público-privadas, em especial com as empresas que oferecem as plataformas nas quais os crimes são cometidos, para que haja sucesso na investigação.

> Nas investigações de crimes cibernéticos é necessária a parceria com a iniciativa privada, até porque a maioria dos dados estão com eles. Acordos com empresas como a Microsoft e a Google possibilitam que os investigadores consigam as informações em tempo hábil. (Coelho, 2017, citado por Combate, 2017)

Coelho (2017, citado por Combate, 2017) sustenta ainda que, na luta contra o cibercrime, a PF tem tomado várias iniciativas. Algumas tecnologias e plataformas vêm auxiliando a corporação a identificar criminosos com mais rapidez.

Nesse sentido, a plataforma Orus permite que o policial insira nela uma requisição de dados judicial ou extrajudicial, que é enviada para as duas empresas aderentes ao projeto (Google e Microsoft), que respondem diretamente ao policial sobre a situação, sem a necessidade de a requisição passar por escritórios de advocacia, o que facilita os procedimentos.

De acordo com o princípio da anterioridade da lei, previsto no art. 1º do Código Penal, “Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal” (Brasil, 1940).

Para lidar com a crescente criminalidade digital, a legislação penal precisa se manter em constante atualização, criando tipos penais que contemplem as novas modalidades de delitos informáticos.

A Lei n. 12.737/2012, apelidada de *Lei Carolina Dieckmann*, atualizou o Código Penal e estabeleceu como crimes os seguintes delitos informáticos:

> Art. 154-A - Invasão de dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> [...]
> Art. 266 - Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública - Pena - detenção, de um a três anos, e multa.
> [...]
> Art. 298 - Falsificação de documento particular/cartão - Pena - reclusão, de um a cinco anos e multa. (Brasil, 2012)

Por sua vez, a Lei n. 14.155/2021 alterou o Código Penal, para tornar mais graves os crimes de violação de dispositivo informático efetuados com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo, ou de instalar vulnerabilidades para obter vantagem ilícita, bem como cometer furto e estelionato de forma eletrônica ou pela internet – modalidades de crimes que, infelizmente, estão se tornando cada vez mais frequentes, demandando, inclusive, a atuação das delegacias especializadas em cibercriminalidade (Brasil, 2021).

Evidentemente, com o surgimento de novas TICs, surgem novas práticas criminosas que precisam ser identificadas e adequadamente evitadas por meio de medidas de conformidade e prevenção, com a adoção de capacitação dos usuários para perceberem e prevenirem situações de risco e perigos informáticos, e por meio de medidas para combater novas formas de criminalidade, inclusive por meio da criação de novos tipos penais para desestimular e combater as novas formas de crimes virtuais.

Neste sentido, abordaremos a seguir uma projeto de lei para criminalizar o *ransomware*.

TEMA 3 – PROJETO DE LEI N. 879/2022: CRIME DE SEQUESTRO DE DADOS INFORMÁTICOS

O Projeto de Lei n. 879/2022, de iniciativa Senador Carlos Viana (PL/MG), pretende alterar o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal brasileiro), para qualificar o crime de invasão de dispositivo informático quando houver a obtenção de dados pessoais, e criar o crime de sequestro de dados informáticos.

A proposta objetiva a alteração do parágrafo 3º do art. 154-A do Código Penal, acrescentando a expressão “obtenção de dados pessoais” no contexto da

invasão de dispositivo informático, e a criação do art. 154-C, tipificando como crime a conduta descrita como “sequestro de dados informáticos”, inclusive tornando o crime mais grave quando for praticado em face de autoridade pública, conforme o seguinte texto inicial do projeto, a seguir descrito:

> Art. 1º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passa a vigorar com as seguintes alterações:
> Art.154-A. [...]
> § 3º Se da invasão resultar a obtenção de dados pessoais, conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, ou informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa, se a conduta não constitui crime mais grave.
> **Sequestro de dados informáticos**
> Art. 154-C. Tornar inutilizáveis ou inacessíveis, por qualquer meio, e com o fim de causar constrangimento, transtorno ou dano, sistemas ou dados informáticos alheios:
> Pena – reclusão, de três a seis anos, e multa.
> §1º Incorre na mesma pena quem oferece, distribui, vende ou dissemina códigos maliciosos ou programas de computador, com o intuito de permitir a prática da conduta definida no caput deste artigo.
> Forma qualificada
> §2º Se o agente pratica a conduta prevista no caput deste artigo, com o fim de obter, para si ou para outrem, qualquer vantagem como condição ou preço do resgate:
> Pena – reclusão, de quatro a oito anos, e multa.
> §3º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal;
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.
> §4º Aumenta-se a pena de metade a dois terços se o crime atingir dados ou sistemas informáticos de qualquer dos poderes da União, Estado, Distrito Federal ou Município, ou de autarquia, fundação pública, empresa pública, sociedade de economia mista ou empresa concessionária de serviços públicos.
> Art. 2º Esta Lei entra em vigor na data da sua publicação.

De acordo com a justificativa apresentada pelo Senador Carlos Viana, autor do projeto de Lei n. 879/2022 (Brasil, 2022), o direito tem buscado se atualizar e evoluir conforme as mudanças sociais trazidas pelos recentes avanços tecnológicos. Entretanto, para o autor do projeto de lei, novos paradigmas comportamentais exigem um olhar atento do legislador para garantir segurança jurídica às relações entre indivíduos e instituições e, especialmente, para reprimir e combater o crescimento do crime organizado digital.

Segundo Viana, mesmo com as inovações trazidas pela Lei n. 14.155/2021, que torna mais graves os crimes de violação de dispositivo

informático, furto e estelionato cometidos de forma eletrônica, a sociedade demanda a criação de um tipo penal específico para desestimular a prática da conduta popularmente chamada de *sequestro de dados*, modalidade de ataque cibernético que não está perfeitamente caracterizada na legislação penal brasileira.

Viana esclarece que, nesse tipo de ataque cibernético, o autor do fato utiliza um código malicioso (vírus) do tipo *ransomware*, capaz de se esconder em arquivos e programas de computador que, quando executado, criptografa os sistemas e informações armazenadas no dispositivo, tornando-os inacessíveis aos seus legítimos usuários.

Para Viana, a disseminação desse tipo de vírus pode ocorrer de diversas formas, sendo as mais comuns através de *e-mails* de *spam*, golpes de engenharia social ou pela exploração de vulnerabilidades em sistemas. Entretanto, não é necessário que ocorra mediante a invasão do dispositivo informático objeto de ataque, considerando que, geralmente, a própria vítima dá o comando de execução ao programa que recebeu, sem saber que estava contaminado.

Após tornar indisponível o acesso às informações e sistemas informáticos, é comum que o agente tente extorquir vantagem indevida da vítima, com a promessa de restabelecer o acesso aos dados.

Viana explica que ataques de *ransomware* são direcionados a particulares e a organismos governamentais, a exemplo do que já ocorreu com o Ministério da Saúde, Conselho Nacional de Justiça (CNJ) e Superior Tribunal de Justiça (STJ), quando foram bloqueados o acesso às caixas de *e-mail* dos ministros, aos processos eletrônicos e outros sistemas. O prejuízo causado por tais ataques é imenso, razão pela qual tais condutas devem ser urgentemente reprimidas.

Outra alteração que Viana propõe, por meio do projeto de lei, é no tipo penal que trata da invasão de dispositivo informático, uma vez que o atual art. 154-A, parágrafo 3º, do Código Penal, não qualifica o crime quando da invasão resultar a obtenção de dados pessoais, invadindo a esfera da privacidade e segurança da vítima, pelo que deve ser punida de forma mais rigorosa.

Viana ressalta que o combate a crimes cibernéticos é um compromisso do Estado Brasileiro, que aderiu à Convenção sobre o Crime Cibernético (também conhecida por Convenção de Budapeste), firmada no âmbito do Conselho da Europa para promover a cooperação entre os países no combate

aos crimes praticados pela internet e com o uso de computadores, por meio do Decreto Legislativo n. 37, de 16 de dezembro de 2021 (Brasil, 2021).

Dessa forma, justifica-se a necessidade de promover constantemente o aperfeiçoamento e a atualização da legislação penal em relação às mencionadas modalidades de crimes virtuais.

O projeto de Lei n. 879/2022 segue em tramitação no Congresso Nacional.

TEMA 4 – NOVAS RELAÇÕES DE TRABALHO E EMPREGO NA INDÚSTRIA 4.0

Segundo Carlos Henrique Bezerra Leite (2021), o direito do trabalho pode ser conceituado como o ramo da ciência jurídica formado por um conjunto de princípios, regras, valores e institutos destinados à regulação das relações individuais e coletivas entre empregados e empregadores, bem como de outras relações de trabalho normativamente equiparadas à relação empregatícia, tendo por objetivo a progressividade da proteção da dignidade humana e das condições sociais, econômicas, culturais e ambientais dos trabalhadores.

É importante, neste momento, conceituarmos *trabalhador* e *empregador*.

De acordo com art. 3º da CLT (Brasil, 1943):

> Art. 3º Considera-se empregado toda pessoa física que prestar serviços de natureza não eventual a empregador, sob a dependência deste e mediante salário.

Por sua vez, o art. 2º da CLT:

> Art. 2º - Considera-se empregador a empresa, individual ou coletiva, que, assumindo os riscos da atividade econômica, admite, assalaria e dirige a prestação pessoal de serviço.
> § 1º - Equiparam-se ao empregador, para os efeitos exclusivos da relação de emprego, os profissionais liberais, as instituições de beneficência, as associações recreativas ou outras instituições sem fins lucrativos, que admitirem trabalhadores como empregados.

Novas formas de trabalho e emprego surgiram com o desenvolvimento das TICs. A chamada *quarta revolução industrial*, também chamada de *indústria 4.0*, mudou significativamente nossas rotinas em virtude da evolução tecnológica proporcionada pelo surgimento de produtos e serviços digitais, que alteraram a forma como contratamos, consumimos bens ou serviços, nos relacionamos em sociedade e trabalhamos.

Baseada fortemente em tecnologias de automação, internet das coisas (IoT), internet dos serviços (IoS), *big data analytic*, uso intensivo de inteligência artificial (IA) e computação em nuvem, a indústria 4.0 objetiva aumentar a

eficiência de processos produtivos, otimizando custos, reduzindo desperdício e perda de tempo, por meio da substituição de postos de trabalho de baixa complexidade e intensa repetição, e incentivo à aquisição de novas habilidades e competências para criação de uma nova geração de empregos, que demandam qualificação e proficiência no uso de ferramentas digitais.

Se, por um lado, com isso, inúmeros empregos e profissões desapareceram, novas relações de trabalho e emprego surgiram na era digital, e tiveram grande crescimento notadamente por causa da internet, como as funções de *web designer*, programador, analista de sistemas, consultor de *e-business*, analista de marketing digital, gerente de *compliance*, influenciador digital, gestor de mídia social, arquiteto de informação, analista de segurança da informação, analista de *big data*, para citar apenas alguns exemplos, no contexto da nova economia fortemente baseada nas TICs.

Por sua vez, a pandemia de Covid-19 também gerou reflexos nas relações de trabalho, na medida em que, entre as decisões tomadas pelas autoridades públicas e de saúde para o enfrentamento da pandemia, houve a restrição de circulação de trabalhadores de atividades e serviços considerados como não essenciais, afetando significativamente o regular funcionamento de inúmeras empresas e atividades profissionais.

Neste contexto, o teletrabalho, que à época não era uma prática largamente difundida no Brasil, tornou-se uma alternativa viável para evitar a interrupção de atividades profissionais, mantendo-as em funcionamento.

Evidentemente, por se tratar de uma medida adotada às pressas, o teletrabalho foi implementado por diversos empregadores de maneira improvisada, tendo os trabalhadores que adaptar, da noite para o dia, algum espaço em suas residências para realizar a atividade profissional até então realizada na sede da empresa.

Um fato que facilitou substancialmente o teletrabalho foi o acesso prévio à TIC nos lares brasileiros. De acordo com o relatório *PNAD Contínua TIC 2019*, a internet chegou a 82,7% dos domicílios do país (IBGE, 2019, p. 5).

Sem dúvida, a TIC existente no início da pandemia facilitou muito tal empreitada, com a existência de *softwares* de comunicação em tempo real, compartilhamento de informações em nuvem, e a pré-existência de aplicativos de videoconferência. Tais aplicativos, maciçamente utilizados durante a pandemia, receberam significativos aportes financeiros para manter a

disponibilidade e estabilidade do serviço, e promover o desenvolvimento e aperfeiçoamento de suas plataformas.

Bigtechs, como Microsoft e Google, alocaram recursos tecnológicos e financeiros em suas plataformas Teams e Meet, respectivamente, além da plataforma Zoom, que também se destacou no período, viabilizando a realização de reuniões, conferências, eventos e, inclusive, aulas telepresenciais síncronas.

Entretanto, sob o ponto de vista legal, o teletrabalho no início da pandemia estava regulamentado juridicamente de maneira superficial, descrita no capítulo II-A da CLT, entre os arts. 75-A a 75-E, e no art. 134, parágrafos 1º e 3º, alterado em virtude da Reforma Trabalhista (Lei n. 13.467/2017).

Tal fato era preocupante, pois da mesma forma que o teletrabalho se tornou uma prática comum já no início da pandemia, rapidamente também foram constatados os impactos negativos na saúde física e mental dos trabalhadores, surgindo discussões sobre o direito à desconexão (efetivo encerramento de jornada de teletrabalho), controle e limite de jornada, disponibilidade para o atendimento de demandas e, de maneira geral, o respeito aos direitos dos trabalhadores estabelecidos na constituição e na legislação trabalhista.

Neste contexto, surgem iniciativas legislativas, entre elas a Medida Provisória n. 927, de 22 de março de 2020, para proporcionar o devido cumprimento da legislação trabalhista, com regras específicas relacionadas não apenas ao teletrabalho, mas também sobre férias, banco de horas e outras diretrizes trabalhistas, ainda que em caráter provisório, dada a relevância e a urgência da situação.

A Medida Provisória n. 927/2020 foi editada como o objetivo de proteger os direitos dos trabalhadores em tempos excepcionais, e oferecer alguma segurança jurídica aos empregadores para, desse modo, poderem disciplinar a relação de trabalho telepresencial, estabelecendo diretrizes e regras de trabalho a fim de supervisionar e dirigir a atividade do empregado nos termos da legislação específica, com previsibilidade, transparência e conformidade à lei, em respeito ao trabalhador e prevenindo passivos trabalhistas.

Atualmente, a regulamentação do teletrabalho está disposta na Lei n. 14.442, de 2 de setembro de 2022, que aborda dois temas trabalhistas: teletrabalho e o pagamento do auxilio alimentação ao trabalhador.

Sobre o tema que diz respeito ao nosso estudo, a Lei n. 14.442/2022 objetiva modernizar e oferecer maior clareza conceitual e segurança jurídica às

relações trabalhistas regidas pela modalidade, em complemento às inovações introduzidas pela Reforma Trabalhista (Lei n. 13.467/2017).

Entre os pontos que merecem destaque, há o detalhamento relacionado a regras e aspectos juridicamente relevantes do teletrabalho, previstos no art. 75-B da CLT, e a criação do art. 75-C, parágrafo 3º, que estabelece que "o empregador não será responsável pelas despesas resultantes do retorno ao trabalho presencial, na hipótese de o empregado optar pela realização do teletrabalho ou trabalho remoto fora da localidade prevista no contrato".

Finalmente, o art. 75-F da CLT, incluído pela Lei n. 14.442/2022, garante prioridade aos empregados com deficiência e empregados com filhos ou crianças sob guarda judicial com até 4 anos de idade na alocação em vagas para atividades que possam ser efetuadas por meio do teletrabalho ou trabalho remoto.

Além das novas demandas do mercado de trabalho, que hoje se adapta ao "novo normal", inclusive com crescente aumento do teletrabalho, surgem implicações jurídicas tanto para o empregado, quanto para o empregador, que demandam novas políticas e práticas de conformidade relacionadas à forma de trabalhar, inclusive no que diz respeito à privacidade do trabalhador diante desse novo cenário, tema que abordaremos a seguir.

TEMA 5 – PRIVACIDADE E CONFORMIDADE NO AMBIENTE DE TRABALHO NA ERA DIGITAL

Um dos aspectos jurídicos mais relevantes relacionados ao trabalho em meios digitais, notadamente no trabalho à distância, é o respeito ao direito à privacidade e à intimidade por parte do trabalhador, em virtude da possibilidade de seu monitoramento por parte do empregador, mesmo quando o trabalho exerce sua atividade laboral em sua residência, por meio do teletrabalho.

Nessa hipótese, os referidos direitos, inseridos na categoria dos direitos de personalidade, podem ser ameaçados, especialmente quando inexistir uma política clara em relação ao uso da internet no ambiente de trabalho.

É evidente que o empregador possui o direito de monitorar, disciplinar e regular o uso de ferramentas informáticas por ele concedidas como instrumentos de trabalho, inclusive para evitar o uso não apropriado (ou mesmo criminoso) dessas ferramentas no ambiente de trabalho ou no contexto da atividade laboral.

A regulamentação por parte do empregador ou do tomador de serviço em relação ao uso de ferramentas informáticas, por meio de manuais de conduta, código de ética, ou regras relativas ao *compliance* empresarial, deve sempre observar a legislação em vigor, pois há normas e critérios jurídicos que devem ser cumpridos, especialmente para se disciplinar corretamente o monitoramento que o empregador pode realizar durante a realização do trabalho do empregado; eis que um dos limites para tal prática reside no direito à privacidade do trabalhador.

A Constituição Federal (CF/88) estabelece, entre os direitos e garantias fundamentais de qualquer cidadão, previstos em seu art. 5º, o direito à privacidade (Brasil, 1988).

Evidentemente, tal privacidade se estende às relações de emprego. Porém, tal direito não é absoluto, encontrando seu limite em seu inter-relacionamento com as demais normas que regulamentam a relação de emprego, inclusive as que permitem ao empregador o direito de organizar, regular e disciplinar as atividades do empregado, nos termos do art. 2º da CLT (Brasil, 1943).

No exercício do poder de direção do empregador, a lei lhe faculta fiscalizar e monitorar a forma como o empregado realiza seu trabalho, podendo ainda aplicar, em caso de nela encontrar desconformidades, sanções disciplinares desde que previstas em lei, ou outras fontes do direito do trabalho, como acordos e convenções coletivas, ou mesmo previsão expressa em regulamento interno da empresa ou de contrato de trabalho, e não violadoras das demais normas do ordenamento jurídico pátrio, especialmente a CF/88 (Brasil, 1988).

Para os empregadores, a constante vigilância sobre as ferramentas de comunicação, notadamente o *e-mail* de uso corporativo, justifica-se na medida em que eles possuem o direito de fiscalizar o uso adequado dos recursos colocados à disposição de seus empregados, tal como ocorre no uso de veículos (mediante, por exemplo, de cadastro de motoristas com horários, itinerários e quilometragens rodadas), de telefones (com acesso via senha do funcionário, registro dos números por este discados, da duração e do custo de cada chamada etc.); e, no controle de despesas com reembolso de passagens aéreas, hospedagem, alimentação, e mesmo com materiais de almoxarifado, principalmente os de maior valor.

No caso específico das ferramentas de comunicação via internet, o monitoramento do empregador se justifica ainda pelo receio da prática de violação de segredos da empresa, de negociação não autorizada pela empresa e que lhe cause prejuízo ou concorrência, de incontinência de conduta ou mau procedimento, de desídia no desempenho das respectivas funções funcionais, de cometimento de atos de indisciplina ou insubordinação, ou atos lesivos à honra ou à boa fama, hipóteses que amparam até a demissão de funcionários por justa causa, conforme previsão do art. 482 da CLT (Brasil, 1943).

Além disso, pretende-se com isso evitar o uso recreativo da rede da empresa e minimizar a exposição da rede corporativa a vírus e demais ameaças presentes no mundo virtual, como *trojans*, *spywares*, *adwares*, *phishing*, *keyloggers* etc., o que poderia causar desde lentidão no tráfego corporativo de informações, até indisponibilidade de sistemas (o que geraria prejuízos significativos), e até destruição de dados e de informações corporativas.

Ademais, de acordo com o art. 932, inciso III, do Código Civil brasileiro (Brasil, 2002), que estabelece a responsabilidade civil por ato do preposto, a empresa que fornece as mencionadas ferramentas de comunicação via internet é diretamente responsável pelo uso que seus empregados fazem, principalmente quando o funcionário utiliza tais meios, no ambiente de trabalho, para realizar atos ilícitos, podendo a empresa, nos termos do referido inciso, responder civilmente pelos danos porventura causados pelos seus empregados, em razão de sua conduta culposa, justamente por não fiscalizar, vigiar e disciplinar adequadamente o exercício das atividades realizadas por seus funcionários.

Portanto, diante dos riscos apresentados, torna-se necessário que o empregador, por questão de segurança, utilize seu poder de direção para orientar sobre o correto uso das ferramentas de comunicação via internet utilizadas pelos seus empregados e realizar varreduras impessoais rotineiras, tendo controle e conhecimento das informações que entram e saem de seus sistemas informáticos, não com o propósito de devassar a privacidade de seus funcionários, mas com o exclusivo propósito de coibir o uso imoral daqueles sistemas e evitar transtornos decorrentes de fraudes que possam, inclusive, causar danos a terceiros.

Em 1997, a Organização Internacional do Trabalho (OIT) publicou, em um de seus chamados *repertórios de recomendações*, diretrizes sobre a proteção

dos dados pessoais dos trabalhadores, visando ao estabelecimento de uma melhor prática de proteção de dados no contexto laboral, e com o objetivo de evitar a interferência arbitrária do empregador na vida privada do trabalhador, conforme especificam os títulos “Objetivos” e “Princípios gerais” do referido documento (OIT, 1997).

> 5.1. O tratamento de dados pessoais dos trabalhadores deve ser realizado em forma justa e legal e limitada exclusivamente a questões diretamente relevantes para a relação de trabalho do trabalhador.
> 5.2. Em princípio, os dados pessoais devem ser usados apenas para essa finalidade para o qual foram coletados.
> 5.3. Quando os dados pessoais são explorados para fins diferentes daqueles para aqueles que foram coletados, o empregador deve garantir que eles não sejam usados de forma incompatível com aquele propósito inicial e adotar as medidas necessário para evitar qualquer má interpretação devido à sua aplicação em outro contexto.
> 5.4. Dados pessoais coletados com base em disposições técnicas ou organização que visa garantir a segurança e o funcionamento adequado de sistemas de informação automatizados não devem ser usados para controlar o comportamento do trabalhador.

Dessa forma, em se tratando de ferramentas de comunicação de internet ofertadas pelo empregador (computadores e *notebooks* – *hardwares* –, e licenças de programas de computador – *softwares*), as informações trafegadas por tais vias, como regra, não dispõem da mesma proteção ao sigilo e privacidade a que teriam direito se aquelas ferramentas fossem uma extensão dos computadores pessoais usados pelos empregados na privacidade e intimidade de seus domicílios, pois o local de trabalho não pode ser visto como um ambiente privado e particular do empregado.

Atualmente, o entendimento predominante nos tribunais brasileiros é de que as mensagens que trafegam nas redes corporativas pertencem à empresa, sendo, portanto, tais contas de funcionários passíveis de monitoramento e fiscalização pelo empregador.

Entretanto, há limites para tal fiscalização. Há registros de empresas monitorando os funcionários por meio de suas *webcams*, realizando registros periódicos durante a jornada de trabalho.

A LGPD não disciplina explicitamente tal modalidade de monitoramento, mas a utilização de monitoramento por vídeo precisa ser devidamente justificada, e o monitoramento do empregador deve estar relacionado aos dados acessados e produzidos no contexto da atividade desempenhada; além disso, tal prática precisa ser anunciada previamente, especialmente quando o trabalho

for realizado de maneira remota, fora da sede da empresa, notadamente por teletrabalho.

Como se trata de uma realidade relativamente recente, com o tempo será criada uma ética nas relações de trabalho, moderada e influenciada pela Justiça do Trabalho e, principalmente, pela legislação trabalhista.

Finalmente, é fundamental que o empregador adote boas práticas de conformidade trabalhista, mapeando e avaliando adequadamente os riscos informáticos que a atividade enfrenta. Para tanto, os colaboradores devem ser capacitados para prevenir incidentes de segurança digital, devendo ser adotada a tecnologia necessária para a prevenção e enfrentamento de potenciais ataques informáticos e mitigar as consequências potencialmente danosas.

Nesse sentido, recomendamos gerenciar atentamente permissões e níveis de acessos concedidos a usuários, evitando atribuir acessos e permissões desnecessários, que possam viabilizar o acesso a informações ou recursos informáticos desvinculados ou desnecessários para a atuação profissional do trabalhador.

Da mesma forma, convém restringir o acesso aos recursos de *software* e *hardware* disponibilizados ao colaborador, limitando o acesso somente a recursos efetivamente necessários ao exercício de sua atividade profissional.

Para se certificar de que as medidas de conformidade para a prevenção e segurança digital estão sendo suficientes para preservar a rede corporativa, o empregador tem o dever de monitorar e auditar regularmente o ambiente de rede corporativa.

Além disso, é dever do empregador a criação de uma cultura corporativa de segurança digital, ofertando treinamentos periódicos para todos os funcionários que utilizam recursos digitais, pois a grande maioria dos colaboradores da uma empresa possui qualificação técnica para o uso de TICs em nível básico, típico de usuário final, não sendo razoável esperar o nível avançado ou a proficiência típica de profissional de TI.

Portanto, não podemos presumir que colaboradores compreendam e dominem determinados aspectos técnicos relacionados à segurança da informação, sem que tenham sido prévia e adequadamente qualificados para tanto.

Dessa forma, treinamentos periódicos são imprescindíveis para estabelecer condutas de segurança e conformidade no ambiente digital,

capacitando os colaboradores para identificarem adequadamente comportamentos de segurança e conformidade digital no ambiente de trabalho. Tais práticas são imperativas para evitar indisponibilidade de sistema e perda de dados decorrente de crimes informáticos.

É também importante esclarecer aos colaboradores, por meios inequívocos de ciência, que as ferramentas de comunicação via internet, sob nenhuma hipótese, deverão ser utilizadas com expectativa de privacidade e intimidade, em razão do monitoramento e fiscalização realizados, por ser essa questão inerente à indispensável transparência, lealdade e boa-fé que deve prevalecer nas relações de trabalho, mormente quando as atividades estão se desenvolvendo de forma preponderante em sistema de teletrabalho, em face da pandemia de Covid-19.

Tal comunicação deve estar prevista de forma clara, de preferência no regulamento da empresa, tendo redigida de maneira objetiva uma política específica referente à utilização das ferramentas de internet no trabalho, podendo, por exemplo, ser elaborada uma cartilha de orientação para o uso da internet, e vinculado o cumprimento de tais políticas ao contrato individual de trabalho.

FINALIZANDO

Nesta etapa, estudamos temas relacionados aos crimes virtuais e às relações de trabalho, analisando a legislação em vigor e iniciativas legislativas para promover a segurança e a conformidade na era digital.

Analisamos novas modalidades de criminalidade digital e as formas de combatê-las por meio de delegacias de polícia especializadas nas modalidades de crimes informáticos, bem como a necessidade da adoção de boas práticas de conformidade para prevenir incidentes envolvendo segurança digital.

Abordamos os impactos da pandemia de Covid-19 em relação ao teletrabalho, mencionando a Medida Provisória n. 927/2020, e a Lei n. 14.442/2022, que regulamenta o teletrabalho no Brasil.

Finalmente, abordamos a privacidade do trabalhador em sua atuação laboral, e boas práticas de conformidade relacionadas ao uso de tecnologia da informação e comunicação no local de trabalho, apresentando os direitos, as diretrizes e os limites relacionados ao direito do empregador em supervisionar e monitorar tais atividades.

Esperamos que os conhecimentos apresentados ao longo do estudo sejam úteis, e que promovam a disseminação de boas práticas para uma atuação profissional baseada em diretrizes éticas e de conformidade, alinhadas aos princípios jurídicos que promovem o respeito a valores constitucionalmente protegidos, como a valorização da dignidade da pessoa, a igualdade, a não discriminação, o respeito à privacidade e a promoção da boa-fé e da transparência em todas as etapas negociais.

Desejamos a você muito sucesso em sua jornada profissional!

REFERÊNCIAS

BRASIL. Constituição (1988). **Diário Oficial da União**, Brasília, DF, 5 out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 20 set. 2022.

BRASIL. Decreto-Lei n. 4.452, de 1º de maio de 1943. **Diário Oficial da União**, Brasília, 6 set. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm>. Acesso em: 20 set. 2022.

BRASIL. Decreto-Lei n. 5.452, de 1º de maio de 1943. **Diário Oficial da União**, Rio de Janeiro, 9 ago. 1943. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm>. Acesso em: 20 set. 2022.

BRASIL. Decreto legislativo n. 37, de 2021. **Diário do Senado Federal**, 14 out. 2021. Disponível em: <https://legis.senado.leg.br/norma/35289207/publicacao/35300588>. Acesso em: 20 set. 2022.

BRASIL. Lei n. 10.406, de 10 de janeiro de 2002. **Diário Oficial da União**, Brasília, 11 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em: 20 set. 2022.

BRASIL. Lei n. 14.155, de 27 de maio de 2021. **Diário Oficial da União**, Brasília, 28 maio 2021. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm>. Acesso em: 20 set. 2022.

BRASIL. Lei n. 14.442, de 2 de setembro de 2002. **Diário Oficial da União**, Brasília, 06 set. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Lei/L14442.htm>. Acesso em: 20 set. 2022.

BRASIL. Projeto de Lei n. 879/2022. **Senado Federal**, 27 abr. 2022. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/152669>. Acesso em: 20 set. 2022.

BRASIL. Decreto-Lei n. 2.848, de 7 de dezembro de 1940. **Diário Oficial da União**, Rio de Janeiro, 31 dez. 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 20 set. 2022.

BRASIL. Lei n. 12.737, de 30 de novembro de 2012. **Diário Oficial da União**, Brasília, 3 dez. 2012b. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 20 set. 2022.

BRASIL. Lei n. 13.467, de 13 de julho de 2017. **Diário Oficial da União**, Brasília, 14 jul. 2017. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13467.htm>. Acesso em: 20 set. 2022.

BRASIL. Medida Provisória n. 927, de 22 de março de 2020. **Diário Oficial da União**, Brasília, 22 mar. 2022. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv927.htm#:~:text=MPV%20927&text=Disp%C3%B5e%20sobre%20as%20medidas%20trabalhistas,)%2C%20e%20d%C3%A1%20outras%20provid%C3%AAncias>. Acesso em: 20 set. 2022.

BOFF, S. O.; FORTES, V. B.; FREITAS, C. O. de A. **Proteção de dados e privacidade**: do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018.

COMBATE ao crime cibernético. **ADPF**, 21 ago. 2017. Disponível em: <http://www.adpf.org.br/adpf/admin/painelcontrole/materia/materia_portal.wsp?tmp.edt.materia_codigo=9139&tit=Combate-ao-crime-cibernetico>. Acesso em: 20 set. 2022.

IBGE – Instituto Brasileiro de Geografia e Estatística. Acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal 2019. **PNAD contínua**. 2021. Disponível em: <https://biblioteca.ibge.gov.br/visualizacao/livros/liv101794_informativo.pdf>. Acesso em: 20 set. 2022.

LEITE, C. H. B. **Curso de direito do trabalho**. 13. ed. São Paulo: Saraiva Educação, 2021.

NUCCI, G. de S. **Manual de direito penal**. 17. ed. Rio de Janeiro: Forense, 2021.

NUCIBER – Núcleo de Combate aos Cibercrimes. **PCPR**, 2022. Disponível em: <https://www.policiacivil.pr.gov.br/NUCIBER>. Acesso em: 20 set. 2022.

OIT – Organização Internacional do Trabalho. **Protección de los datos personales de los trabajadores**. Genebra, 1997. (Repertorio de Recomendaciones Prácticas de la OIT). Disponível em: <https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_112625.pdf>. Acesso em: 20 set. 2022.

ROSSI, L. Pagamento com celular dispara após pandemia e promete mudar o mercado. **Capterra**, 1 set. 2020. Disponível em: <https://www.capterra.com.br/blog/1703/pagamento-movel>. Acesso em: 20 set. 2022.