REVISTA DA

ESCOLA NACIONAL DA MAGISTRATURA

A JUSTIÇA DO TRABALHO NO MUNDO PÓS-PANDÊMICO

Organização Científica

Renata Gil de Alcantara Videira

Caetano Levi Lopes

Claudia Marcia Carvalho Soares

Paulo Roberto Dornelles Junior

ENM
ESCOLA NACIONAL DA MAGISTRATURA

Nº 11

O TRABALHO NO PÓS-PANDEMIA, O "E-MAIL CORPORATIVO" E A LEI GERAL DE PROTEÇÃO DE DADOS

Carlos Alberto Pereira de Castro[1]

Resumo: Trata, o presente estudo, de uma análise sobre a utilização de endereços eletrônicos (*e-mails*) fornecidos por empregadores a seus empregados − conhecidos como *e-mails corporativos* −, bem como da possibilidade (ou não) de que o empregador tenha o direito de checar o conteúdo e os destinatários das mensagens enviadas e recebidas por esses empregados, sob o prisma da garantia constitucional da inviolabilidade do sigilo das correspondências e comunicações interpessoais e, mais hodiernamente, à luz dos princípios protetivos da privacidade e da inviolabilidade do sigilo das comunicações, bem como da Lei Geral de Proteção de Dados (LGPD). Para tanto, é necessário considerar que o trabalho no pós-pandemia deve manter-se, ao menos em parte, na forma de teletrabalho, com a utilização de equipamentos do empregado, e não mais do empregador, para o acesso às correspondências eletrônicas. Tem-se como premissa que a jurisprudência do Tribunal Superior do Trabalho considera lícita tal verificação e, a partir daí, é proposta uma revisão desse entendimento, pautada na Carta Magna de 1988, na LGPD e no entendimento do Supremo Tribunal Federal ao julgar o Tema 1.041 de Repercussão Geral.
Palavras-chave: *e-mail* corporativo; Lei Geral de Proteção de Dados; inviolabilidade; comunicações interpessoais; jurisprudência.

[1] Mestre em Ciência Jurídica. Juiz do Trabalho titular da 7ª Vara do Trabalho de Florianópolis do TRT da 12ª Região, Florianópolis/SC, Brasil. Titular da Cadeira n. 20 da Academia Catarinense de Letras Jurídicas. *E-mail*: capcastro@hotmail.com

INTRODUÇÃO

No início de 2020, fomos surpreendidos com a avassaladora pandemia da Covid-19, causada pelo coronavírus, que afetou significativamente as relações interpessoais, entre as quais aquelas ligadas ao mercado de trabalho.

Uma das mudanças significativas foi o aumento das atividades prestadas de modo remoto, utilizando-se, empregados e empregadores, dos meios telemáticos disponíveis, seja para a realização dos misteres de cada atividade econômica, seja para a comunicação interpessoal, em que o diálogo oral cedeu espaço às mensagens de texto.

O crescimento da comunicação por meios telemáticos, deve-se frisar, já era bastante visível antes mesmo do contexto vivido no período mais agudo da pandemia, é dizer, pode-se dizer que houve a aceleração desse crescimento em níveis acima da curva em razão das medidas de isolamento social.

Nesse contexto, ainda que o trabalho presencial − que envolve as mais diversas áreas de atividades − seja retomado de modo paulatino, parece certo que "nada será como antes", na medida em que grande parte das atividades ligadas ao trabalho, bem como das comunicações interpessoais, deve permanecer, em paralelo ao modelo pré-pandemia.

O trabalho remoto, teletrabalho ou *home office* é um desses fenômenos. O trabalho realizado em ambiente diverso do "estabelecimento" da empresa empregadora é uma realidade crescente, com um acréscimo trazido pela pandemia: o empregado, em seu ambiente *outsider*, utiliza-se não necessariamente de *Personal Computers (PCs)*, *Notebooks* ou *Smartphones* disponibilizados pelo empregador, mas, sim, dos seus equipamentos pessoais, ainda que a serviço da empresa.

Daí a importância, a nosso pensar, de trazer a debate, mais uma vez, a questão relacionada ao uso dos correios eletrônicos, ou *e-mails*, ditos corporativos, e em que isso deve ser (re)analisado em face das novas facetas do fenômeno do trabalho remoto, e à luz dos princípios protetivos de direitos fundamentais à privacidade e à inviolabilidade das comunicações, bem como das regras postas pela Lei Geral de Proteção de Dados (LGPD) e à vista da jurisprudência nacional.

1. ENDEREÇO ELETRÔNICO: DEFINIÇÃO E BREVE HISTÓRICO

Electronic Mail (E-mail), email, ou, em Língua Portuguesa, correio eletrônico, é um serviço que permite compor, enviar e receber mensagens através de redes e sistemas eletrônicos de comunicação. Organizado em múltiplas caixas de correio, o serviço funciona como uma central de distribuição: recebe e entrega as mensagens. O termo é aplicado tanto aos sistemas que utilizam a Internet como as Intranets, que permitem a troca de mensagens dentro de uma empresa ou organização. A funcionar como intermediário, um servidor de *e-mail* transfere mensagens de um usuário para outro.[2]

Ian Peter ressalta que o correio eletrônico é mais antigo que a Internet e foi, de fato, uma ferramenta crucial para criá-la, mas os serviços de comunicação globais iniciaram no início da *Arpanet,* em 1973.[3]

Chama a atenção, de pronto, que tanto no vocábulo criado em Língua Inglesa, quanto na expressão cunhada em Língua Portuguesa, a palavra "correio" se encontra presente, demonstrando a origem inafastável de sua concepção como invento científico − a correspondência escrita e remetida a um destinatário, em um endereço geográfico (logradouro).

Entre as décadas de 70 e 80 do século passado, o uso do e-mail ainda estava limitado apenas àqueles usuários com acesso à tecnologia: pesquisadores ligados à comunidade científica e, ainda assim, bastante limitado em relação ao seu conteúdo (que permitia apenas texto e bem poucas palavras), sem a possibilidade de incluir, por exemplo, quaisquer anexos.[4]

Na década de 1990, principalmente com o surgimento do serviço de *webmail*, expandiu-se o uso das mensagens interpessoais pela Internet, permitindo-se que, de forma rápida e de qualquer lugar, sem a necessidade de instalar um programa, a pessoa consiga acessar sua "caixa postal",

---

[2] Disponível em: <http://www.tipografos.net/internet/email-funcionamento.html.> Acesso em: 20 set. 2021.

[3] PETER, Ian. **The history of email**. Net history. Disponível em: http://www.nethistory.info/History%20of%20the%20Internet/email.html. Acesso em: 25 set. 2021.

[4] CRUZ, Glenda Demes da. O e-mail e sua produção no meio eletrônico: o suporte afeta o gênero? **Revista Letra Magna**, ano 3, n. 5, p. 7, 2º sem. 2006.

emitindo e recebendo mensagens (com anexos, incluindo-se documentos e fotografias) no navegador de sua escolha (*browser*).

Inicialmente utilizados em contas individuais, com o tempo o webmail passou a ser também ferramenta de uso corporativo, na situação em que um provedor cria uma conta para a empresa com diversos endereços e o espaço de armazenamento disponível, "hospedando" os endereços que esta forneça a seus diretores, ou trabalhadores.

Existem, atualmente, serviços de *e-mail* de hospedagem compartilhada, que consistem em uma grande quantidade de caixas de correio hospedadas em um servidor. As pessoas em um serviço de *e-mail* de hospedagem compartilhada compartilham endereços IP,[5] pois estão hospedadas no mesmo servidor.

E, em um estágio mais recente, temos os serviços de *e-mail* hospedados em nuvem, utilizando um provedor de serviços *cloud e-mail*. O armazenamento em nuvem é um modelo de armazenamento de dados de computador no qual os dados digitais são armazenados em *pools* lógicos, ditos "na nuvem". O armazenamento físico, por sua vez, abrange vários servidores (às vezes em vários locais), e o ambiente físico normalmente pertence e é gerenciado por uma empresa de hospedagem. Esses provedores de armazenamento em nuvem são responsáveis por manter os dados disponíveis e acessíveis, e o ambiente físico protegido e funcionando. Pessoas e organizações compram ou alugam capacidade de armazenamento dos fornecedores para armazenar dados de usuários, organizações ou aplicativos.[6] As organizações podem escolher entre opções de armazenamento em nuvem local ou externo, ou uma mistura das duas opções.

Desse modo, o que antes se realizava, em termos de comunicações interpessoais, por meio de textos escritos em meio físico (as

---

[5] Um endereço de protocolo da Internet (endereço IP) é um rótulo numérico, como 192.0.2.1, conectado a uma rede de computadores que usa o protocolo da Internet para comunicação. Um endereço IP tem duas funções principais: identificação da interface de rede e endereçamento de localização. **Wikipedia. IP Adress.** Disponível em: https://en.wikipedia.org/wiki/IP_address. Acesso em: 20 out. 2021.

[6] WIKIPEDIA. **Cloud computing.** Disponível em: <https://en.wikipedia.org/wiki/Cloud_computing.> Acesso em: 30 set. 2021.

correspondências em geral, como cartas, cartões, mensagens) ou por mensagens telegráficas, e que, comparando-se com o serviço de *e-mail*, era de difícil execução − pois impunha, ao remetente, levar o conteúdo da mensagem a um serviço de correio; e deste serviço, fazer chegar ao do destinatário em tempo hábil −, exigindo-se que houvesse toda uma estrutura logística pelo serviço responsável pelo recebimento e entrega e, ainda, pela necessidade de que o destinatário estivesse em seu endereço quando da chegada do "carteiro", transformou-se gradativamente, em termos cronológicos, em meio eletrônico de envio e recebimento, em velocidade sem dúvida imensamente maior que o seu precursor, e sem o problema da necessidade de sincronismo entre o envio pelo serviço e a presença física do destinatário em um endereço geográfico – razão pela qual as missivas escritas, os telegramas e até os "cartões de Natal" tiveram crescente e drástica redução.

Outra diferença importante entre o "correio postal" e o seu sucessor "eletrônico" é a possibilidade de armazenamento – tanto pelo "servidor" quanto pelos sujeitos da comunicação interpessoal – das mensagens enviadas e recebidas, de modo a evitar a perda de informações importantes que, por exemplo, fosse uma mensagem "em papel", em um incêndio poderia ser destruída sem deixar vestígios.

É de se destacar, ainda, que:

> O uso do e-mail tornou-se imprescindível para a comunicação das empresas por diversos motivos. Em especial para empresas que fazem negócios internacionalmente, quando os fusos horários se cruzam, dificultando o agendamento de chamadas telefônicas. Com essa ferramenta, é possível criar e colocar em prática campanhas de *marketing* de baixo custo. Isso com a garantia de que a mensagem será recebida pelo cliente em potencial, por exemplo.[7]

[7] GAIDARGI, Juliana. **A importância do e-mail corporativo**. Disponível em: https://www.infonova.com.br/artigo/a importancia-do-email-corporativo/. Acesso em: 30 set. 2021.

Em uma mensagem de *e-mail*, assim, sempre há conteúdos que possuem dados, seja na mensagem, seja em anexos − de forma estruturada e/ou não estruturada − de modo que é fundamental que se use criptografia, preferencialmente a que se tem como padrão de mercado, PGP (*Pretty Good Privacy*), garantindo que a mensagem saia de um local e somente seja aberta no destinatário. Somente assim é possível garantir o sigilo dos dados enquanto trafegam pela Internet.[8]

O questionamento que se coloca é se, a considerar uma mensagem de *e-mail* como interlocutor um empregado de certa empresa (empregador) e veiculada por intermédio de um servidor de *e-mail* da mesma empresa empregadora (por ex.: nome_empregado@nome_empresa.com), o ordenamento jurídico autoriza (ou não) que esta mensagem possa ser aberta por outra pessoa que não o remetente nem o destinatário, a mando da empresa empregadora.

Para tanto, cumpre revisitar a evolução histórica da proteção das comunicações interpessoais até a presente quadra da nossa ordem jurídica.

2. A INVIOLABILIDADE DO SIGILO DE CORRESPONDÊNCIAS E COMUNICAÇÕES INTERPESSOAIS

A proteção da correspondência vem de longa data, em razão de sua importância para a intimidade e a privacidade das comunicações escritas, e por estar muitas vezes fortemente ligadas a relações de poder entre os povos e seus governantes. Conforme observa Frederick Burrowes,

> Desde o advento da escrita, a troca de informações sempre foi importante na história da humanidade. A preocupação com o sigilo tornou-se uma constante. Nesse contexto, há muito o sigilo das correspondências é preocupação

[8] ARANTES, Francine Nunes. **O e-mail corporativo pode ser considerado dado pessoal?** Disponível em: <https://www.nextlawacademy.com.br/blog/o-e-mail-corporativo-pode-ser-considerado-dado-pessoal.> Acesso em: 29 set. 2021.

> presente no Direito. No Direito Penal Romano, por exemplo, a violação da correspondência já era tipificada.[9]

O desenvolvimento científico permitiu que as comunicações fossem tendo outros meios que não a escrita, e o Direito tratou de protegê-las, pois a proteção da privacidade "sempre foi diretamente condicionada pelo estado da tecnologia em cada época e sociedade", de modo que "o advento de estruturas jurídicas e sociais que tratem do problema da privacidade são respostas diretas a uma nova condição da informação, determinada pela tecnologia".[10]

Acerca da proteção concedida constitucionalmente à comunicação (e seus interlocutores), define o art. 5º de nossa atual Constituição que:

> XII − é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Já em consonância com o advento de novas tecnologias, o Constituinte de 1988 inseriu a proteção à inviolabilidade do sigilo das comunicações de dados, ampliando o espectro da norma já prevista nas Constituições republicanas, de modo ininterrupto, desde a Carta de 1946, que assegurava o sigilo da correspondência e de comunicações por outros meios até então existentes.

Importante anotar que, quando da promulgação da atual Carta, não havia sequer a noção de que as comunicações interpessoais viessem a assumir o formato existente, com o advento − e a popularização − do uso do *e-mail* e o desuso das mensagens postais escritas, sem falar, ainda neste estudo, por questões de delimitação, das comunicações por mensagens de aplicativos como o *Telegram* e o *WhatsApp.*

---

[9] BURROWES, Frederick B. A proteção constitucional das comunicações de dados: internet, celulares e outras tecnologias. **Revista Jurídica da Presidência da República**, Brasília, v. 9, n. 87, p. 09-24, out./nov. 2007.

[10] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados. 2. ed. rev. e atual. São Paulo: Thomson Reuters Brasil, 2019. p. 69.

Ao interpretar a garantia constitucional em comento, o Supremo Tribunal Federal (STF), no julgamento do Recurso Extraordinário 389.808, sendo relator o Ministro Marco Aurélio, em decisão publicada em DJE no dia 10.05.2011, considerou que as exceções ao preceito são apenas aquelas encerradas na parte final do texto da norma – portanto, em face do disposto no inciso XII do art. 5º da Constituição, a regra é a privacidade quanto à correspondência, às comunicações telegráficas, aos dados e às comunicações, "ficando a exceção – a quebra do sigilo – submetida ao crivo de órgão equidistante – o Judiciário – e, mesmo assim, para efeito de investigação criminal ou instrução processual penal". Conclui o ministro relator em seu voto que "conflita com a Carta da República norma legal atribuindo à Receita Federal – parte na relação jurídico-tributária – o afastamento do sigilo de dados relativos ao contribuinte".

Em 1996, adveio a Lei n. 9.296, que "regulamenta o inciso XII do artigo 5º da Constituição Federal" e dispõe sobre o procedimento a ser adotado quando da interceptação de comunicações telefônicas para fins de investigação criminal e instrução em processo penal, com a possibilidade de "interceptação do fluxo de comunicações em sistemas de informática e telemática", sempre por ordem judicial, no que é relevante frisar o artigo 1º da aludida Lei:

> Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.
> Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

O escopo da aludida regra é, sem dúvida, evitarem-se interceptações de comunicações interpessoais indevidas. Interceptar é, assim, "interromper o curso originário, impedir a passagem, sendo que, na lei, tem o sentido de captar a comunicação, conhecer seu conteúdo. Interceptar é ter contato com

teor da comunicação, não impedindo que ela chegue ao seu destinatário.".[11]

Para que ocorra uma interceptação lícita, a Lei n. 9.296 somente admite uma hipótese: a prévia ordem judicial de juiz competente para matéria penal. Isso porque, em todo o conteúdo da referida lei, todos os dispositivos tratam de estabelecer regras e procedimentos para que o magistrado com essa competência defira ou não a interceptação.

Nota-se, na lei em apreço, a inclusão da proteção aos dados que transitam em fluxo em "sistemas de informática e telemática". A telemática é concebida como ciência que trata da manipulação de dados e informações, conjugando o computador, sistemas de informática, com os meios de comunicação, telefônicas ou não. Assim, qualquer comunicação feita por meio de sistema de informática é protegida pela lei – como comunicações feitas no âmbito da Internet.

Ao encerrar desta pesquisa, em 20 de outubro de 2021, o Senado Federal aprovou a PEC 17/2019, que altera a Constituição Federal para "incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais", aguardando-se a sua sanção para os próximos dias – o que leva a não mais haver dúvidas sobre a natureza jurídica de direito fundamental atribuída a esta proteção.

Quanto ao argumento de que haveria ausência de previsão constitucional de garantia da proteção das comunicações telemáticas – ao menos até a promulgação da PEC 17/2019, já noticiada – decidiu o STF, ao apreciar o Recurso em *Habeas Corpus* 132.115, tendo por relator o Ministro Dias Toffoli – em decisão publicada em 19.10.2018, que, em face da concepção constitucional moderna de que inexistem garantias individuais de ordem absoluta, mormente com escopo de salvaguardar práticas ilícitas, "a exceção constitucional ao sigilo alcança as comunicações de dados telemáticos, não havendo que se cogitar de incompatibilidade do parágrafo único do art. 1º da Lei 9.296/96 com o art. 5º, inciso XII, da Constituição Federal".

Importante para os fins deste estudo apontar a capitulação penal da

[11] CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus aspectos processuais**. Rio de Janeiro: Lumen Juris, 2001. p. 111.

conduta de interceptação dos referidos conteúdos, constante do artigo 10 da Lei n. 9.296, com a redação conferida pela Lei n. 13.869, de 2019: "constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei", cuja pena é de reclusão, de dois a quatro anos, e multa.

O bem jurídico tutelado na conduta delituosa citada é, sem sombra de dúvidas, "o sigilo das comunicações", como já decidiu o STF em âmbito de Repercussão Geral.

No que toca à primeira modalidade ("praticar interceptação, escuta, ou quebrar segredo de Justiça sem autorização judicial"), o sujeito ativo pode ser qualquer pessoa – o que incluiria, a um primeiro olhar, empresas/empregadores. É, portanto, um crime comum.

A outra conduta (interceptação "com objetivos não autorizados em lei") seria crime de mão própria, consubstanciada em abuso de poder pelo magistrado.[12]

Observa-se, portanto, uma linha tênue e radical que separa a interpretação acerca da conduta de quem intercepta conteúdo colhido na Internet*:* ou há licitude na atitude, ou pelo contrário há conduta penalmente tipificada e passível de punição.

Visto isso, é curial abordar os ditames da LGPD, norma que é ponto central deste estudo.

3. O CONTEÚDO DE *E-MAILS* NA LGPD E O CONCEITO DE "DADOS PESSOAIS"

Até aqui já é possível constatar que mensagens de *e-mail,* corporativo ou não, são meios de comunicação interpessoal, protegidos pelo sigilo e inviolabilidade, e passíveis, no espectro fático, de interceptação (lícita ou

[12] FRAGOSO, Chrystian Falk. Os crimes de interceptação indevida de comunicação telefônica, informática ou telemática e de quebra de segredo de justiça. *In*: SANTORO, Antonio Eduardo Ramires; MADURO, Flávio Mirza (orgs.). **Interceptação telefônica**: os 20 anos da Lei n. 9.296/96. Belo Horizonte: D'Plácido, 2016. p. 110.

não).[13]

Também já se frisou o fato de que, com o avanço da tecnologia, as mensagens de *e-mail* passaram de meros "bilhetes" de poucas palavras a "meio de transporte" virtual de arquivos, sejam eles de qualquer origem ou formato. Com isso, o tráfego de informações por essa ferramenta cresceu substancialmente em relevância e diversidade de conteúdo.

A LGPD (Lei 13.709/2018) tem como finalidade inequívoca "a proteção dos dados pessoais". E o que seriam esses "dados"?

Na LGPD, dado pessoal é toda "informação relacionada a pessoa natural identificada ou identificável" – artigo 5º, inciso I. Diz respeito a "informações pessoais coletadas e tratadas, entre as quais "nome, RG, CPF, número de passaporte, título de eleitor, endereço, profissão, hábitos de consumo, número de telefone, estado civil, *e-mail* e patrimônio".[14]

Observa-se que a LGPD não apresenta uma lista de quais dados são considerados dados pessoais, diferentemente do conceito de dado pessoal sensível, tal como também ocorre na regulação da matéria em âmbito da União Europeia. Dados pessoais sensíveis, na conformidade da LGPD, são "aqueles de maior potencial discriminatório e que possuem uma tutela maior", como os de origem racial, étnica, convicção política ou filosófica, crença religiosa, referentes à saúde ou opção sexual, e ainda, dados genéticos e biométricos "que identificam o indivíduo de forma inequívoca e que trazem um risco muito alto ao titular dos dados, caso haja algum incidente durante o tratamento".[15]

Os dados que constam de mensagens (e anexos) de *e-mails* são, em

---

[13] "O termo prova ilícita tem uma acepção variada. Em linhas gerais, a doutrina indica que a prova ilícita se divide em prova ilícita (em sentido restrito) e em prova ilegítima. Prova ilícita é aquela que viola norma de direito material, que protege direitos individuais, como o direito à privacidade. Prova ilegítima é a que viola norma de direito processual, como arrolar mais testemunhas que o número permitido e outros casos previstos no CPP" (CARVALHO, Luis Gustavo Grandinetti Castanho de. Direito à privacidade. **Revista da Escola da Magistratura do Estado do Rio de Janeiro**, n. 2. Disponível em: https://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista02/revista02_51.pdf. Acesso em: 19 out. 2021.

[14] CARLOTO, Selma. **Lei Geral da Proteção de Dados**: enfoque nas relações de trabalho. São Paulo: LTr, 2020. p. 54.

[15] CARLOTO, Selma. **Lei Geral da Proteção de Dados**: enfoque nas relações de trabalho. São Paulo: LTr, 2020. p. 55.

grande parte, de caráter pessoal, sejam dados sensíveis ou não, enquadrando-se de todo modo no bem jurídico tutelado pela LGPD.

O artigo 7º da LGPD indica, taxativamente, por outro lado, as hipóteses em que poderá haver o "tratamento de dados pessoais". O termo "tratamento", por seu turno, significa "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (inciso X do art. 5º da LGPD).

Quanto ao objeto deste estudo – possibilidade (ou não) de o empregador perscrutar o conteúdo de *e-mail* corporativo – destaca-se da regra constante do artigo 7º da LGPD, que está autorizado o tratamento de dados pessoais, quando: (a) houver o consentimento pelo titular dos dados (inciso I); (b) para o cumprimento de obrigação legal ou regulatória pelo controlador (inciso II); (c) para o exercício regular de direitos em processo judicial, administrativo ou arbitral; (d) para a proteção da vida ou da incolumidade física do titular ou de terceiro (inciso VII); ou (e) quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (inciso IX).

Essas exceções serão enfocadas, após analisarmos como vem decidindo os Tribunais do Trabalho brasileiros quanto à questão da possibilidade do empregador de perscrutar *e-mails* de empregados.

4. A JURISPRUDÊNCIA DO TRIBUNAL SUPERIOR DO TRABALHO SOBRE O TEMA

De fato, a jurisprudência do Tribunal Superior do Trabalho (TST) até aqui tem sido favorável a esta conduta patronal – abertura do conteúdo de mensagens por considerar que o *e-mail* dito corporativo é um instrumento de trabalho, sobre o qual possui total ingerência. Já o conteúdo de *e-mail* pessoal, particular, do empregado, mesmo quando acessado no ambiente da empresa, com equipamentos desta, não poderia ser fustigado pelo

empregador.

Naquele que se considera o *leading case* sobre a matéria – o julgamento, pela Primeira Turma do TST, do Recurso de Revista 61300-23.2000.5.10.0013, tendo como relator o Ministro João Oreste Dalazen –, decisão esta publicada no Diário da Justiça de 10.06.2005 –, o acórdão foi assim ementado:

> PROVA ILÍCITA. -E-MAIL– CORPORATIVO. JUSTA CAUSA. DIVULGAÇÃO DE MATERIAL PORNOGRÁFICO. 1. Os sacrossantos direitos do cidadão à privacidade e ao sigilo de correspondência, constitucionalmente assegurados, concernem à comunicação estritamente pessoal, ainda que virtual (e-mail particular). Assim, apenas o e-mail pessoal ou particular do empregado, socorrendo-se de provedor próprio, desfruta da proteção constitucional e legal de inviolabilidade. 2. Solução diversa impõe-se em se tratando do chamado e-mail corporativo, instrumento de comunicação virtual mediante o qual o empregado louva-se de terminal de computador e de provedor da empresa, bem assim do próprio endereço eletrônico que lhe é disponibilizado igualmente pela empresa. Destina-se este a que nele trafeguem mensagens de cunho estritamente profissional. Em princípio, é de uso corporativo, salvo consentimento do empregador. Ostenta, pois, natureza jurídica equivalente à de uma ferramenta de trabalho proporcionada pelo empregador ao empregado para a consecução do serviço. 3. A estreita e cada vez mais intensa vinculação que passou a existir, de uns tempos a esta parte, entre Internet e/ou correspondência eletrônica e justa causa e/ou crime exige muita parcimônia dos órgãos jurisdicionais na qualificação da ilicitude da prova referente ao desvio de finalidade na utilização dessa tecnologia, tomando-se em conta, inclusive, o princípio da proporcionalidade e, pois, os diversos valores jurídicos tutelados pela lei e pela Constituição Federal. A experiência subministrada ao magistrado pela observação do que ordinariamente acontece revela que, notadamente

o e-mail– corporativo, não raro sofre acentuado desvio de finalidade, mediante a utilização abusiva ou ilegal, de que é exemplo o envio de fotos pornográficas. Constitui, assim, em última análise, expediente pelo qual o empregado pode provocar expressivo prejuízo. A estreita e cada vez mais intensa vinculação que passou a existir, de uns tempos a esta parte, entre Internet e/ou correspondência eletrônica e justa causa e/ou crime exige muita parcimônia dos órgãos jurisdicionais na qualificação da ilicitude da prova referente ao desvio de finalidade na utilização dessa tecnologia, tomando-se em conta, inclusive, o princípio da proporcionalidade e, pois, os diversos valores jurídicos tutelados pela lei e pela Constituição Federal. A experiência subministrada ao magistrado pela observação do que ordinariamente acontece revela que, notadamente o e-mail corporativo, não raro sofre acentuado desvio de finalidade, mediante a utilização abusiva ou ilegal, de que é exemplo o envio de fotos pornográficas. Constitui, assim, em última análise, expediente pelo qual o empregado pode provocar expressivo prejuízo ao empregador. 4. Se se cuida de e-mail corporativo, declaradamente destinado somente para assuntos e matérias afetas ao serviço, o que está em jogo, antes de tudo, é o exercício do direito de propriedade do empregador sobre o computador capaz de acessar à INTERNET e sobre o próprio provedor. Insta ter presente também a responsabilidade do empregador, perante terceiros, pelos atos de seus empregados em serviço (Código Civil, art. 932, inc. III), bem como que está em xeque o direito à imagem do empregador, igualmente merecedor de tutela constitucional. Sobretudo, imperativo considerar que o empregado, ao receber uma caixa de email– de seu empregador para uso corporativo, mediante ciência prévia de que nele somente podem transitar mensagens profissionais, não tem razoável expectativa de privacidade quanto a esta, como se vem entendendo no Direito Comparado (EUA e Reino Unido). 5. Pode o empregador monitorar e rastrear a atividade do empregado

> no ambiente de trabalho, em e-mail corporativo, isto é, checar suas mensagens, tanto do ponto de vista formal quanto sob o ângulo material ou de conteúdo. Não é ilícita a prova assim obtida, visando demonstrar justa causa para a despedida decorrente do envio de material pornográfico a colega de trabalho. Inexistência de afronta ao art. 5º, incisos X, XII e LVI, da Constituição Federal. 6. Agravo de Instrumento do Reclamante a que se nega provimento.

No teor do voto constante do acórdão supra destaca-se o seguinte trecho:

> No *leading case* de *Smyth v. Pillsbury Co.*, determinado Empregado alegou que havia sido dispensado de forma contrária à política da empresa, pois sua privacidade teria sido violada.
> Neste caso, a Eg. *United States Court for the Eastern District of Pennsylvania* entendeu que o Empregado havia enviado várias mensagens de e-mail através do sistema da Empresa, que vieram a ser acessadas pelo seu Empregador, sem a sua anuência. Devido ao conteúdo impróprio destas mensagens, o Empregador rescindiu o contrato de emprego.
> Esta Eg. Corte da Pennsylvania, entretanto, negou procedência ao pedido do Empregado, a despeito de resultar comprovado que o Empregador havia reiterado aos seus Empregados que o *e-mail* poderia ser utilizado para fins pessoais e que as mensagens não seriam, em momento algum, interceptadas, mantendo-se confidenciais.
> A aludida Corte americana entendeu que, mesmo com as referidas concessões do Empregador, o Empregado não tinha expectativa de privacidade ao utilizar o sistema da empresa para enviar suas mensagens de e-mail.

No referido julgado do Estado americano da Pensilvânia, como consta também do acórdão do TST (já com tradução realizada), tem-se que aquela corte compreendeu que:

> Antes de mais nada, o interesse da companhia em prevenir comentários inadequados e anti-profissionais, e até mesmo atividades ilegais, em seu sistema de correio eletrônico supera qualquer direito à privacidade que o empregado possa ter com relação a esses comentários. Em suma, achamos que o réu não invadiu ilicitamente a privacidade do requerente e, consequentemente, não violou a política da empresa. Em vista disso, é concedida a autorização para demissão. (*Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 100 – E.D. Pa. 1996)

Relata o acórdão do TST, ainda, que, no estado do Texas, o Quinto Distrito da Corte de Apelação também se posicionou favoravelmente em relação ao empregador, decidindo que ao empregado não assiste razoável expectativa de privacidade nas mensagens arquivadas dentro daquela pasta ou dentro de sua caixa de *e-mail*. A mencionada conclusão baseou-se no argumento de que as mensagens de *e-mail* primeiro teriam circulado dentro de vários pontos do sistema de *e-mail* da Microsoft, onde poderiam ser acessadas a qualquer hora pela empresa e, somente depois, viriam a compor a esfera privada do empregado.

Porém, como bem relata o julgado paradigmático da Corte superior laboral brasileira, as decisões das cortes norte americanas se baseiam em entendimento da sua Suprema Corte – a qual reconheceu que os empregados têm direito à privacidade no ambiente de trabalho digna de proteção legal, entretanto, deve-se ponderar esta privacidade em relação às peculiaridades de cada ambiente de trabalho. A Suprema Corte assentou que, em certas áreas, os empregados podem ter uma razoável expectativa de privacidade *(expectation of privacy),* porém não de forma absoluta. Como consta em tradução livre do aresto: "se um empregado tem uma razoável expectativa de privacidade é uma questão de práticas específicas no seu local de trabalho, e o fato daquele ter uma razoável expectativa deve ser tratado caso a caso".

Constata-se que a jurisprudência norte-americana, em que se baseou o Ministro relator para amparar seu voto no julgado da Primeira Turma do

TST, e que norteia a jurisprudência brasileira até a presente data,[16] parte da premissa de que a privacidade pode ser relativizada pela expectativa de sua manutenção (por terceiros, no caso, o empregador), levando a questão para a casuística, longe de generalizar a situação e passando ao largo de aspectos ligados à LGPD, notadamente: (1) o consentimento prévio do empregado para essa investigação de sua correspondência eletrônica (artigo 7º, inciso I); e (2) a existência de interesses legítimos do controlador (art. 7º, inciso IX) – no caso, o empregador – que permita a prevalência destes mesmos interesses sobre a privacidade do titular dos dados pessoais.

Sequer há como justificar – e a jurisprudência disso não cogita – a existência de um direito à invasão das mensagens de *e-mail* em razão de cumprimento de obrigações legais ou regulatórias (LGPD, art. 7º, inciso II), sendo certo que o empregador não detém poderes para violar o sigilo de comunicações sem prévia autorização judicial para tanto. O que se nota é que a jurisprudência acolhe essa conduta patronal – a invasão da conta corporativa de *e-mail* do empregado – com fundamento em um "direito de propriedade", que lhe permitiria esse escrutínio, pois se trata de uma "ferramenta da empresa", o que lhe permitiria adentrar o conteúdo dos diálogos e arquivos para abrigar-se de eventual responsabilização por conduta irregular do empregado usuário.

E, em razão do teletrabalho – do qual não se cogitava ao nível em que chegamos na pandemia e no período posterior a ela – o fundamento de que o empregado se vale de equipamentos da empresa não mais prevalece, quando o acesso à conta de *e-mail* corporativo se dá por um *smartphone, notebook* ou PC do próprio empregado, e não mais o fornecido pelo empregador.

Por mais altaneiro que seja o objetivo – proteger a sociedade de condutas delituosas as mais diversas – os empregados que não cometem tais condutas também devem ser "vigiados" e ter suas correspondências (e os

[16] Veja-se, como exemplo, o julgamento, pelo TST, do Recurso de Revista 1347-42.2014.5.12.0059, cuja decisão foi publicada no Diário Eletrônico da Justiça do Trabalho em 26.06.2020. Neste julgado, conclui a Quarta Turma que o *e-mail* corporativo utilizado pelo empregado tem natureza jurídica de ferramenta de trabalho, pois fornecido pela empresa apenas para uso profissional. Por isso, pode a empresa rastreá-lo "tanto do ponto de vista formal (quantidade, horários de expedição, destinatários etc.) quanto sob o ângulo material ou de conteúdo".

arquivos enviados ou recebidos em anexo a essas correspondências) "analisados" por um empregador, com finalidades que são típicas de órgãos de segurança pública (investigação criminal)? E se não há porque vigiar todo e qualquer empregado, mas apenas os que estejam em prática criminosa, como se fará essa distinção, para fins investigatórios patronais?

É por essa razão que ousamos propor uma revisão do entendimento assim posto.

5. PROPOSIÇÃO DE UM NOVO OLHAR SOBRE O ASSUNTO

Ao admitir-se a interceptação de dados pelo empregador como válida, sem que haja o prévio consentimento do empregado (LGPD, artigo 7º, inciso I), e sem ordem judicial prévia, como tem decidido a jurisprudência trabalhista, quando o teor da mensagem não contenha "dados pessoais", pergunta-se: como é possível a esse empregador – em termos fáticos – fazer a "triagem" das mensagens a serem "abertas" sem invadir os dados que a LGPD impõe sejam protegidos?

Pois, não é difícil compreender que, para se chegar a encontrar, como no caso concreto julgado pelo TST, material pornográfico em *e-mail* remetido ou recebido, há que se olhar "uma por uma" das correspondências, ou ainda que se faça uma "vistoria por amostragem", o que incluiria nessa perscrutação, indubitavelmente, também aquelas mensagens (e seus anexos) que possuam dados pessoais – inclusive os sensíveis – tanto do empregado quanto de terceiros, embora não tenham nada de conteúdo nocivo à empresa.

O direito pátrio – diferentemente do direito norte-americano – não concebe a privacidade como algo relativizável.

Pontua-se, a respeito, que o STF, ao analisar o mérito do Tema 1.041 em Repercussão Geral, definiu a seguinte tese, em decisão de 18.08.2020: "Sem autorização judicial ou fora das hipóteses legais, é ilícita a prova obtida mediante abertura de carta, telegrama, pacote ou meio análogo". No voto vencedor, da lavra do Ministro Edson Fachin, tem-se que "a mera suspeita de que o conteúdo de determinada correspondência é ilícito não justifica a devassa sem o pressuposto da autorização judicial ou da presença de um dos interessados". O douto ministro considerou a medida desproporcional,

ferindo não apenas garantias constitucionais, mas também tratados internacionais como o Pacto de São José da Costa Rica, segundo o qual "ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação".

Concordamos que, tanto nos Estados Unidos da América como aqui, não há direito fundamental de caráter absoluto, pois há de se observar a eventual colisão de interesses entre pessoas com direitos fundamentais contrapostos entre si. Todavia, diante da garantia constitucional não só da privacidade (inciso X) como da inviolabilidade do sigilo da comunicação de dados, incluindo-se os telemáticos, o direito fundamental pode ser limitado por outro valor jurídico de mesma estatura constitucional. Assim, "havendo conflito entre dois direitos constitucionais fundamentais, é possível à autoridade judiciária – e só a esta – limitar o sigilo de dados".[17]

E compreendemos, destarte, ser possível lançar-se novo olhar sobre o tema, em que ao empregador somente pudesse ser autorizado a perscrutar os *e-mails* de seus empregados mediante ordem judicial prévia, da autoridade competente para a matéria penal, como exige a Lei n. 9.296, e pela menção da decisão do STF no Tema 1.041 de Repercussão Geral, à ilicitude de violação de cartas e "meios análogos" de correspondência.

Pede-se vênia para recordar que o usuário de *e-mail* é tratado pela LGPD como titular de direitos sobre seus dados – seja ele o empregado, seja ele o destinatário da mensagem do empregado, ou o remetente a este, eventualmente um não empregado daquela empresa. E o empregador, na forma da LGPD, é um terceiro, que detém esses dados:

> O *E-mail* Corporativo, sendo uma ferramenta de comunicação com clientes, entenda-se aqui como sendo titulares, podem conter informações dos mesmos, tanto no corpo da mensagem, mesmo que através de um anexo, quanto na funcionalidade agenda, onde colaboradores

[17] CARVALHO, Luis Gustavo Grandinetti Castanho de. Direito à privacidade. **Revista da Escola da Magistratura do Estado do Rio de Janeiro.** n. 2, p. 55. Disponível em: https://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista02/revista02_51.pdf. Acesso em: 19 out. 2021.

> poderão armazenar informações de seus contatos, como sexo, idade, preferência religiosa e muito mais.
> Sendo assim, são dados de titulares. Sendo dados de titulares armazenados pela sua empresa, automaticamente sofrerão as sanções previstas na LGPD.[18]

De fato, o teor de um *e-mail* pode conter assuntos ligados ao sigilo profissional, ou industrial, mas também registros pessoais, como certidões, cópias de exames e atestados médicos, e até mesmo uma negociação salarial, bem como pode ser utilizado para fins escusos.

Em termos de direito comparado, convém apontar que o Parecer 4/2007 do Comitê Europeu para a Proteção de Dados *(European Data Protection Board)* dispõe sobre o conceito de dados pessoais e menciona, nas considerações gerais, que a definição possui interpretação ampla, mas que não deverá ser inadequadamente estendida. O Grupo de Trabalho analisa, separadamente, quatro pilares para definir dado pessoal, quais sejam: "qualquer informação"; "relativa a"; "identificada ou identificável"; "pessoa singular", muito embora esses elementos estejam intimamente relacionados, apoiando-se uns nos outros. Ao ponderar sobre o primeiro elemento – "qualquer informação" – o Grupo de Trabalho interpreta que:

> A expressão "dados pessoais" inclui informação que toca a esfera da vida privada e familiar da pessoa *stricto sensu,* mas inclui também informação sobre qualquer tipo de atividade realizada pela pessoa, tal como a que diz respeito às relações de trabalho ou ao seu comportamento económico e social. Inclui, assim, informação sobre pessoas singulares, independentemente do seu estatuto ou papel (consumidor, paciente, empregado, cliente, etc.).[19]

---

[18] ARANTES, Francine Nunes. **O e-mail corporativo pode ser considerado dado pessoal?** Disponível em https://www.nextlawacademy.com.br/blog/o-e-mail-corporativo-pode-ser-considerado-dado-pessoal. Acesso em 29 set. 2021.

[19] UNIÃO EUROPEIA. GRUPO DE TRABALHO DE PROTECÇÃO DE DADOS DO ARTIGO 29.º – SOBRE A PROTECÇÃO DAS PESSOAS SINGULARES NO QUE DIZ RESPEITO AO TRATAMENTO DE DADOS PESSOAIS. **Parecer n. 4** (2007). Disponível em: https://www.gpdp.gov.mo/uploadfile/others/wp136_pt.pdf. Acesso em: 28 set. 2021.

É dizer, se uma mensagem de *e-mail* é uma correspondência; se para o usuário externo (não empregado) existe a proteção do sigilo de suas correspondências, sejam elas "postais", sejam "eletrônicas" ou "telemáticas", não vemos sentido, com todas as vênias, para que seja diferente com o usuário que é empregado e se utiliza de uma conta de *e-mail* corporativo.

Comparando-se com o seu precursor – a mensagem escrita e encaminhada por meio físico, convém perquirir: a jurisprudência também consentiria em permitir que o empregador abrisse correspondências postais, "de papel", dirigidas a seus empregados e que tinham como endereço geográfico a sede da empresa, ou abrisse, de inopino, o armário do vestiário ou o escaninho de algum colaborador em que este guardasse seus pertences, por ser "um instrumento fornecido pela empresa"?

Por essa razão, parece incogitável admitir-se a referida interceptação de mensagens de *e-mails* e seus anexos por particulares, ou mesmo pelo Poder Público, sem prévia ordem judicial expressa e fundamentada, pelo que o empregador somente poderia agir de tal forma amparado pelo Judiciário, com o escopo de investigação de supostos delitos, o que aqui se sugere.

CONSIDERAÇÕES FINAIS

O presente estudo, longe de tentar esgotar o tema relativo à existência do direito do empregador em interceptar (no sentido de captar, perscrutar) dados constantes de conteúdos de e-mails de seus empregados, pretendeu realizar o repensar acerca da matéria, uma vez que a jurisprudência do TST firmou-se no sentido do acórdão formulado no *leading case* datado de 2005, e a construção do entendimento jurisprudencial deve caminhar de modo a reconhecer os avanços da sociedade, inclusive nos aspectos tecnológicos, mas sempre em respeito extremo aos direitos e garantias constitucionais.

Em vista especialmente do fenômeno do teletrabalho, com o uso de instrumentos (*notebooks, smartphones*) não mais de propriedade do empregador, mas sim de cada empregado, cujo "endereço IP" não tem ligação com a empresa, e no entanto, ante a continuidade de uso *e-mails* corporativos, cujo armazenamento tende a ser, cada vez mais, feito "em nuvem", há ainda

que se ter maior cuidado ao gerar uma permissão para que empregadores vasculhem contas de *e-mail* sob o único argumento de terem de fiscalizar seus empregados. Afinal, o poder empregatício, como todo poder, há de ter limites.

Importante salientar, ao final deste singelo estudo, a necessidade de revisitar, constantemente, os conceitos operacionais ligados à informática, ou à tecnologia da informação, para que o Direito possa oferecer respostas que estejam em consonância com o que há de novo nesse "mundo cibernético".

REFERÊNCIAS

ARANTES, Francine Nunes. **O e-mail corporativo pode ser considerado dado pessoal?** Disponível em: https://www.nextlawacademy.com.br/blog/o-e-mail-corporativo-pode-ser-considerado-dado-pessoal. Acesso em: 29 set. 2021.

BURROWES, Frederick B. A proteção constitucional das comunicações de dados: internet, celulares e outras tecnologias. **Revista Jurídica da Presidência da República**, Brasília, v. 9, n. 87, p. 9-24, out./nov., 2007.

CARLOTO, Selma. **Lei Geral da Proteção de Dados**: enfoque nas relações de trabalho. São Paulo: LTr, 2020.

CARVALHO, Luis Gustavo Grandinetti Castanho de. Direito à privacidade. **Revista da Escola da Magistratura do Estado do Rio de Janeiro**, n. 2. Disponível em: https://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista02/revista02_51.pdf. Acesso em: 19 out. 2021.

CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais**. Rio de Janeiro: Lumen Juris, 2001.

CRUZ, Glenda Demes da. O e-mail e sua produção no meio eletrônico: o suporte afeta o gênero? **Revista Letra Magna**, ano 3, n. 5, 2º sem. 2006.

,

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados. 2. ed. rev. e atual. São Paulo: Thomson Reuters Brasil, 2019.

FRAGOSO, Chrystian Falk. Os crimes de interceptação indevida de comunicação telefônica, informática ou telemática e de quebra de segredo de justiça. *In*: SANTORO, Antonio Eduardo Ramires; MADURO, Flávio Mirza (orgs.). **Interceptação telefônica**: os 20 anos da Lei n. 9.296/96. Belo Horizonte: D'Plácido, 2016.

GAIDARGI, Juliana. **A importância do e-mail corporativo.** Disponível em: https://www.infonova.com.br/artigo/a importancia-do-email-corporativo/. Acesso em: 30 set. 2021.

PETER, Ian. **The history of e-mail.** Net history. Disponível em: http://www.nethistory.info/History%20of%20the%20Internet/email.html. Acesso em: 25 set. 2021.

UNIÃO EUROPEIA. GRUPO DE TRABALHO DE PROTECÇÃO DE DADOS DO ARTIGO 29.º – SOBRE A PROTECÇÃO DAS PESSOAS SINGULARES NO QUE DIZ RESPEITO AO TRATAMENTO DE DADOS PESSOAIS. **Parecer n. 4** (2007). Disponível em: https://www.gpdp.gov.mo/uploadfile/others/wp136_pt.pdf. Acesso em: 28 set. 2021.

WIKIPEDIA. **Cloud computing.** Disponível em: https://en.wikipedia.org/wiki/Cloud_computing. Acesso em: 30 set. 2021.