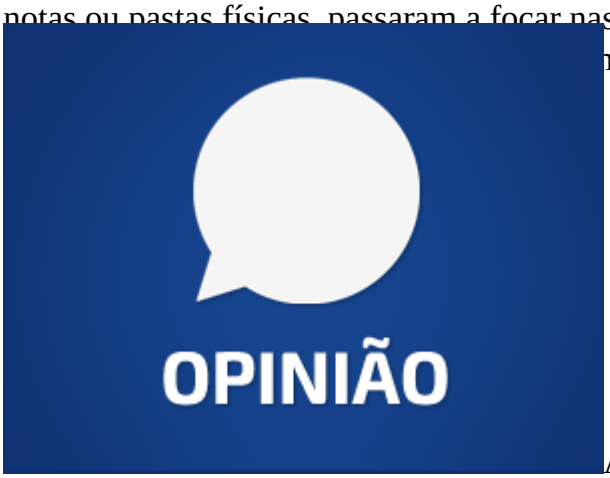
Opinião: Os limites do empregador nas investigações corporativas

As evoluções tecnológicas dos últimos anos fizeram com que as evidências de crimes e outros ilícitos, em especial a comunicação entre os agentes, migrassem cada vez mais para o mundo digital. As investigações corporativas, que alguns anos atrás dependiam da coleta e análise de agendas, blocos de notas ou pastas físicas, passaram a focar nas comunicações em tempo real, trocadas por aplicativos de



mo pela *deep web*.

A mudança impõe diversos desafios aos profissionais que conduzem investigações corporativas, que precisam acompanhar as evoluções tecnológicas para garantir a efetividade dos trabalhos, ao mesmo tempo em que devem respeitar os direitos fundamentais da relação empregatícia, sob pena de gerarem provas posteriormente anuladas pela Justiça do Trabalho.

O primeiro deles diz respeito à possibilidade de acesso pelos empregadores às comunicações digitais trocadas por seus colaboradores. Em se tratando de informações enviadas por dispositivos corporativos de propriedade do empregador, e desde que os empregados estejam cientes que as mensagens poderão ser consultadas, a doutrina e jurisprudência têm consolidado o entendimento de que a empresa poderá acessar tal conteúdo por configurarem ferramenta de trabalho [1]. Por exemplo, em casos de demissão por justa causa por uso inapropriado das ferramentas de comunicação, os tribunais vêm decidindo que as mensagens que partem das máquinas de propriedade da empresa podem ser lidas pelo empregador em eventual investigação, não havendo violação do sigilo de correspondência.

Esse foi o entendimento do Tribunal Superior do Trabalho (TST) recentemente, ao analisar a possibilidade de utilização de e-mail corporativo como meio de prova lícito, no tocante à aplicação de justa causa para a extinção do contrato de trabalho, destacando que *"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. […]"* [2].

Cabe destacar também recente entendimento do Superior Tribunal de Justiça de que não era preciso autorização judicial para a obtenção de provas a partir do registro de mensagens de WhatsApp encontradas na lixeira do e-mail corporativo de uma colaboradora. O colegiado confirmou acórdão do Tribunal de Justiça do Paraná que condenou um casal com base nas conversas encontradas no servidor da empresa sobre desvio de valores. Os réus alegaram nulidade absoluta e cerceamento de defesa, em razão da utilização de provas ilícitas, obtidas sem autorização judicial. Porém, o STJ confirmou que *"[…] como o arquivo de registro das mensagens encontrava-se em computador utilizado como ferramenta de trabalho e de propriedade da empresa, perfeitamente possível que o empregador tivesse acesso ao conteúdo de todas as informações existentes no equipamento, sem que fosse necessária autorização judicial. […]"* [3].

Também já existem julgados que reconhecem o direito do empregador em acessar o Skype ou WhatsApp se verificado que o aplicativo é utilizado em equipamento de propriedade da empresa, e se esse aplicativo servir para o exercício da função do empregado (a possibilidade de monitoramento/investigação deverá ser comunicada aos empregados, como já mencionado, o que vem sendo feito por meio de políticas destinadas a regular o uso de ferramentas eletrônicas). Em julgamento de recurso que discutia a demissão por justa causa de colaborador que se utilizava do Skype — enquanto ferramenta de trabalho — para assuntos pessoais e para depreciar seus colegas e superiores, o Tribunal Regional do Trabalho da 12ª Região entendeu que *"[…] Apesar de o skype se tratar de ferramenta de comunicação acessível ao público em geral, quando destinada pelo empregador como ferramenta de trabalho, equipara-se à ferramenta corporativa. Portanto, não ofende o direito à intimidade, tampouco viola o sigilo da correspondência, o acesso pelo empregador ao conteúdo das mensagens trocadas pelos seus empregados em computadores da empresa, durante o expediente de trabalho, mormente quando cientificados os trabalhadores dessa possibilidade. […]"* [4].

Nesse caso, constava expressamente em política interna da empresa que as ferramentas de comunicação deveriam ser usadas para fins estritamente profissionais. A política interna também dispunha que o e-mail e o computador postos à disposição do empregado seriam passíveis de inspeção periódica e rastreamento [5].

Outro desafio comumente enfrentado diz respeito à possibilidade de pagamento de dano moral decorrente de investigações corporativas. Estando comprovada a má conduta do colaborador, a empresa poderá aplicar medida corretiva correspondente. Entretanto, deve garantir que não ocorrerá irrazoável exposição do investigado perante os demais colaboradores e o mercado de trabalho. Caso haja qualquer forma de ofensa à honra, privacidade, intimidade, imagem ou nome do colaborador, tal conduta poderá ensejar pedido de condenação por dano moral em face da empresa (a divulgação do evento em redes sociais ou aplicativos de mensagens instantâneas por outros empregados, mesmo que de forma não autorizada pelo empregador, pode gerar risco à condenações, sendo recomendável que tais aspectos sejam igualmente regulados por política).

Naturalmente, o empregado submetido a uma investigação corporativa irá vivenciar um processo invasivo e desgastante, que deve ser conduzido com cautela e profissionalismo, de forma a evitar situações vexatórias. Aos profissionais envolvidos nas investigações recai, assim, o dever de apurar corretamente os fatos, de maneira isenta, objetiva, imparcial, célere, proporcional, sigilosa e confidencial [6].

Como terceiro e último desafio, trazemos aqui as problemáticas envolvendo políticas como a do *bring your own device* (Byod), em que a empresa permite que o colaborador utilize dispositivos próprios para trabalhar, por questões de comodidade e funcionalidade.

As empresas devem considerar que os dispositivos de propriedade do colaborador são protegidos pelo direito constitucional à privacidade — a vida privada, a honra e a reputação são invioláveis, sendo assegurado o direito à indenização pelos danos materiais ou morais decorrentes de eventual violação cometida pela empresa. Se, no entanto, o colaborador consentir com a coleta de seus dispositivos ou com o monitoramento por parte do empregador, isso mitigaria o risco de eventuais questionamentos [7] (é importante que a coleta e/ou o monitoramento observe o limite da privacidade, evitando-se a investigação sobre aplicativos e/ou *softwares* não relacionados ao trabalho).

Além disso, é recomendável que a empresa regule o tema em seu programa de integridade, divulgando as normas internas de forma clara, bem como invista na educação digital de seus empregados e parceiros, controle o acesso à rede interna/empresarial e busque soluções tecnológicas com vistas a proteger seus dados.

A empresa também pode definir os *softwares* permitidos para uso no ambiente de trabalho, determinar o tipo de informação que pode ser acessada através de equipamentos pessoais, bem como revisar e restringir os acessos de dados pelos colaboradores e criar um modelo de reembolso para casos de extravio do dispositivo pessoal no ambiente corporativo.

Relevante notar que o e-mail particular, em geral, não é considerado uma ferramenta de trabalho, mesmo quando utilizado em equipamento de propriedade da empresa [8]. Por isso, não é recomendável o acesso a contas de e-mail pessoal ou outros aplicativos de uso pessoal, ainda que instalados no dispositivo corporativo.

Dado o exposto, podemos concluir que cada vez mais tem se consolidado o entendimento de que, se os dispositivos são de propriedade da empresa, ela poderá ter acesso a todo o seu conteúdo no âmbito de suas investigações internas, desde que os empregados tenham ciência dessa possibilidade. Por outro lado, se o colaborador utilizar dispositivos pessoais para o desempenho das atividades profissionais, o acesso às informações poderá ser alvo de disputa, sendo recomendável que as empresas, sempre que possível, disponibilizem os equipamentos de trabalho necessários aos seus colaboradores, ou tentem regular a questão por política como forma de mitigação dos riscos.

[1] O TST já se manifestou pela viabilidade de monitoramento do e-mail corporativo sob certas condições, e decidindo também sobre a impossibilidade de monitoramento do e-mail pessoal do empregado – TST, AgIn em RR 1542/2005-055-02-40, 7.ª Turma., rel. Min. Ives Gandra Martins Filho,

06.06.2008 e TST, RR 9961/2004-015-09-00, 7.ª T., rel. Min. Ives Gandra Martins Filho, 18.02.2009.

[2] TST-RR-613/2000-013-10-00.7. 1ª Turma, rel. João Oreste Dalazen, 18.05.2005 e TST- RR-1347-42.2014.5.12.0059. 4ª Turma, rel. Alexandre Luiz Ramos, 23.06.2020.

[3] STJ, Resp nº 1.875.319 – PR (2020/0117825-7), 6.ª T., rel. Min. Nefi Cordeiro, 15.09.2020

[4] TRT-12, RO 0000702-38.2014.5.12.0052 SC., rel. Gisele Pereira Alexandrino, 11.09.2015.

[5] A previsão no contrato de trabalho ou em política interna de que o monitoramento pode acontecer é necessária, de forma a atender ao princípio da transparência previsto na Lei Geral de Proteção de Dados.

[6] Tais condutas devem ser aplicadas também para com eventuais vítimas, denunciantes e testemunhas. Quanto ao sigilo e confidencialidade dos resultados das investigações, ressalta-se que os resultados podem ser divididos internamente, com as pessoas que necessitem das informações para tomar medidas de remediação, ou com terceiros, como auditores e autoridades públicas.

[7] O assunto é controverso porque não se pode ferir a privacidade e a intimidade do empregado, mas o empregador, por ser responsável pelos atos de seus empregados, deve também se cercar de medidas para mitigar eventuais riscos. Afinal, a empresa é responsável por todos os dados corporativos que circulam nos dispositivos. É provável que a construção jurisprudencial em torno do BYOD siga a tendência de utilizar os princípios afirmados nas decisões sobre monitoramento eletrônico e teletrabalho. Logo, os e-mails corporativos e sistemas de exclusiva propriedade da empresa continuarão passíveis de vigilância por parte dela.

[8] Conforme entendimento de cortes como a Suprema Corte Norte Americana, em certas áreas, os empregados podem ter uma razoável expectativa de privacidade (*expectation of privacy*). Mas nunca de forma absoluta.

Date Created
09/07/2021