Rony Vainzof: Data loss prevention e a JustiÃ§a do Trabalho

O monitoramento e a coleta de evidências digitais de colaboradores no ambiente de trabalho é muito relevante, no mínimo: (1) como forma de mitigar riscos corporativos; (2) para a adoção de sanções administrativas; e (3) como prova para eventuais procedimentos repressivos em casos de práticas ilícitas, improbidade, incontinência de conduta, entre outros.

O Tribunal Superior do Trabalho (TST) já havia consolidado o entendimento de que *"o empregador pode monitorar e traçar a atividade do empregado em um e-mail corporativo, ou seja, verificar mensagens, tanto do ponto de vista formal (quantidade, prazo de entrega, destinatários etc.) quanto do ângulo material ou conteúdo, e as provas obtidas não constituem provas ilícitas"* [1].

Assim, o empregador pode monitorar ferramentas corporativas de trabalho (*hardware* e *software*), o que inclui conteúdo de *e-mail* corporativo, desde que atenda a determinados requisitos:

(1) Estabelecer regras internas para informar ao empregado sobre o monitoramento de forma clara e transparente, preferencialmente utilizando técnicas de *visual law* e campanhas de conscientização;

(2) O empregado deve ter conhecimento inequívoco sobre o monitoramento para não haver eventual expectativa de privacidade. Ou seja, é necessário que os funcionários estejam inequivocamente cientes das ferramentas de *data loss prevention* (DLP), com antecedência, o que não deve ser confundido com consentimento, pois a base legal aqui é o exercício regular de direito;

(3) O monitoramento deve cobrir ferramentas de trabalho (*hardware* e *software*).

Ou seja, o acesso aos dispositivos, ferramentas e aplicativos pessoais do empregado devem ser vistos com cautela, pois o TST entende que:

(1) O *e-mail* pessoal ou privado do empregado, utilizando seu próprio provedor, goza da proteção constitucional e legal da inviolabilidade [2]; e

(2) O acesso a dispositivos privados pode ser classificado como abuso de poder e pode dar origem a indenização por danos morais [3].

Se houver suspeita de que um funcionário (ex ou atual) tenha extraviado dados ou informações confidenciais ou praticado outros ilícitos utilizando aplicações ou equipamentos pessoais na relação de emprego é possível propor medidas judiciais para:

- Que os dispositivos pessoais do funcionário sejam analisados por um perito nomeado pelo magistrado, mediante busca e apreensão, por exemplo;
- A obtenção de dados e comunicações privadas junto aos provedores de aplicações pessoais utilizados pelo réu, para que sejam analisados por um perito nomeado pelo magistrado;
- A obtenção de ordem judicial para a abstenção de utilização dos dados ou informações desviadas, bem como a respectiva exclusão.

Porém, recentemente, o TST limitou a quebra de sigilo de *e-mail* pessoal de empregado aos metadados das mensagens (como registros de data, horário, contas e endereços de IP), pois não seria válida ordem que autoriza o acesso ao conteúdo de todas as mensagens enviadas e recebidas de conta pessoal de *e-mail* utilizada por pessoa física, para fins de apuração de suposto ato ilícito, com a seguinte fundamentação [4] :

- O interesse público na apuração de infrações penais graves, puníveis com reclusão, pode permitir, em alguns casos, a relativização da inviolabilidade das comunicações;
- O Marco Civil da Internet (Lei 12.965/2014) não prevê a possibilidade de requisição judicial de "conteúdo da comunicação privada" para formação de conjunto probatório em ação cível;
- O que se autoriza, no artigo 22 da lei, é o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet;
- Há notável distinção entre a requisição dos registros das comunicações e seus conteúdos propriamente ditos. Essa segunda hipótese está reservada, como regra geral, à instrução de processo criminal; e
- Ressalvadas situações extremas, em que há risco à vida ou à integridade física de pessoas, é inviável a quebra do sigilo do conteúdo de mensagens de *e-mail* privado para fins de instrução de demanda cível.

Nesse ponto, importante lembrar acórdão paradigmático do Supremo Tribunal Federal, relatado pelo ministro Sepúlveda Pertence, diante da alegada ilicitude da prova oriunda de busca e apreensão de computadores e disquetes em determinada empresa para análise dos dados ali existentes e apuração de ilícitos tributários, no qual entendeu-se que não houve quebra de sigilo das comunicações de dados (interceptação das comunicações), mas, sim, apreensão física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial", asseverando que "a proteção a que se refere o artigo 5º, inciso XII, da Constituição, é da comunicação de dados e não os dados, o que tornaria impossível qualquer investigação administrativa, fosse qual fosse" [5].

O Marco Civil da Internet (MCI) prevê a possibilidade de ordem judicial para a disponibilização de conteúdo de comunicações privadas, não excluindo o procedimento cível (artigo 10, §2º).

O dispositivo acima referido não deve ser confundido com a interceptação do fluxo de comunicações em sistemas de informática e telemática (Artigo 1º, parágrafo único, da Lei 9.296/96, que regulamenta o inciso XII, do artigo 5º, da Constituição), que somente pode ocorrer mediante ordem judicial para prova em investigação criminal, além de outros requisitos.

A diferença é entre passado e futuro: enquanto ordem judicial, inclusive na esfera cível (conforme o MCI), pode determinar a obtenção de comunicações privadas que já ocorreram e estão armazenadas nos provedores de aplicações de internet, a interceptação do fluxo de comunicações (ou seja, algo que ainda não ocorreu), somente pode ser objeto à instrução de processo criminal.

Portanto, a nossa legislação trata e protege de forma distinta não só a sensibilidade de cada espécie de dado ou informação, mas também o momento em que são, de alguma forma, coletados, ou seja, se já trafegaram e agora permanecem estáticos (passado) ou se ainda transitarão por algum meio de comunicação (futuro).

Essa distinção é de extrema importância, sob pena de se inviabilizar relevantes apurações de ilícitos civis, em que a obtenção do conteúdo de comunicações privadas que já ocorreram são cruciais para a comprovação de condutas indevidas, desde que haja ordem judicial e se preserve a privacidade e a intimidade do envolvido, restringindo/segregando o acesso ao conteúdo de comunicação que não seja objeto da apuração.

[1] TST: RR – 1347-42.2014.5.12.0059, 23/6/2020 e RR-1347-42.2014.5.12.0059.

[2] TST: RR – 61300-23.2000.5.10.0013, 18/5/2005.

[3] TST: Ag. 1241520155080129, 25/2/2022.

[4] Subseção II Especializada em Dissídios Individuais (SDI-2) do Tribunal Superior do Trabalho. O processo tramita em segredo de justiça (fonte: https://www.tst.jus.br/noticias/-/asset_publisher/89Dk/content/id/31190922)

[5] . STF – HC: 83168 SC, relator: min. Sepúlveda Pertence, j. 10/5/2006, Tribunal Pleno, DJ 2/2/2007.