#241 | ANO 21 | SETEMBRO 2020
ISBN 1807-779X

JUSTIÇA & CIDADANIA

ESPAÇO OAB
REFORMA TRIBUTÁRIA DEVE SER AMPLA

OPINIÃO
O PAPEL DA JUSTIÇA PARA A RETOMADA DO DESENVOLVIMENTO

ENTREVISTA EXCLUSIVA COM O NOVO PRESIDENTE DO SUPREMO TRIBUNAL FEDERAL, MINISTRO LUIZ FUX

"O JUDICIÁRIO NÃO PODE SER UM MUSEU DE PRINCÍPIOS"

HOME OFFICE E SEGURANÇA DA INFORMAÇÃO

Tendência e desafios

MARCELO COSTA SOARES
Advogado

A tendência de se trabalhar em *home office* cresceu muito ao longo da pandemia de covid-19. Com base em pesquisa da Fundação Getúlio Vargas realizada em abril deste ano, existe a expectativa de que o trabalho remoto em nosso País cresça 30% após o período de estabilização dos casos do novo coronavírus e a retomada da normalidade. No entanto, vale dizer que antes mesmo da pandemia, a prática ou adoção do trabalho remoto já era uma realidade em vários países, inclusive no Brasil.

É importante entender que a adoção de metodologias para esta nova realidade no ambiente corporativo demanda um processo de análise e reorganização cultural para que as empresas consigam acompanhar o ritmo das mudanças e desafios, tais como a mitigação de riscos em relação à violação de dados fora do ambiente corporativo e, consequentemente, uma maior segurança da informação para o trabalho remoto.

Primeiramente, é importante ressaltar que o trabalho na modalidade teletrabalho foi incluído no ordenamento jurídico brasileiro pela Lei nº 13.467/2017, que acrescentou à Consolidação das Leis Trabalhistas seus artigos 75-A a 75-E para regulamentar esta nova realidade laboral. Tratou-se, portanto, de importante medida na busca de melhor compatibilização entre a esfera profissional e pessoal, ou seja, a procura de equilíbrio para a efetivação do trabalho fora do ambiente tradicional corporativo. Ainda que o teletrabalho venha a ser estipulado apenas de maneira temporária diante da covid-19, não há vedação para que o mesmo seja ajustado entre empresa e funcionário por um período determinado, desde que, nesse ínterim, as atividades sejam prestadas predominantemente fora do ambiente corporativo.

Por outro lado, é importante ressaltar que o *home office* se caracteriza quando o trabalho é realizado remotamente de maneira eventual na residência do funcionário, podendo ou não configurar a hipótese de teletrabalho. Portanto, se por um lado a nova modalidade de trabalho trouxe uma suposta flexibilização na realização de tarefas podendo ser feitas em horários as vezes mais condizentes às exigências da empresa e às necessidades dos funcionários, por outro lado, trouxe consigo desafios antes não tão evidentes na cultura das empresas.

Por isso, o entendimento sobre as boas práticas de governança corporativa torna-se fundamental para a disseminação de uma cultura voltada à prevenção e mitigação de riscos. Esta, portanto, pode ser entendida como um conjunto de relacionamentos na gestão de uma empresa que fornece a estrutura através da qual os objetivos da mesma são definidos, como também, os meios de os atingir por meio de um monitoramento de desempenho.

Dito isso, se faz necessário observar algumas caraterísticas que vêm acompanhando essa nova realidade de trabalho ao longo de recentes anos. Com o avanço tecnológico são poucos os funcionários que se contentam em utilizar apenas os equipamentos que a empresa disponibiliza, ou seja, muitas vezes preferem utilizar seus próprios dispositivos, seja porque não querem portar dois dispositivos ao mesmo tempo, seja porque acreditam que sua performance será melhor com a utilização dos equipamentos com os quais têm maior afinidade.

Neste novo cenário surge uma sigla conhecida como BYOD (*bring your own device*), acrônimo do termo em inglês que significa "traga seu próprio dispositivo", ou seja, prática que se explica pelo fato da empresa permitir ou sugerir que o funcionário utilize seus próprios equipamentos, como *notebooks*, celulares pessoais, *tablets*, etc. Consequentemente, começam a surgir problemas cuja análise deve considerar que o universo tecnológico vivencia uma forte tendência de virtualização, que gera reflexos no ambiente de trabalho.

As informações corporativas necessárias para a execução das atividades profissionais não estão mais armazenadas em arquivos físicos, dentro das dependências das empresas, ao contrário, ficam guardadas na nuvem, e os funcionários podem ter acesso a partir dos dispositivos que preferirem, em qualquer horário ou localização geográfica. Diante de tal situação a segurança da informação, guiada pelas boas práticas da governança corporativa, deve ser entendida como gerenciamento, monitoramento e controle de ativos informacionais (dados) para a mitigação de riscos. Vale lembrar que dados são representações de conceitos disponibilizados em dispositivos para interpretação ou processamento, seja por humanos ou por sistemas automatizados.

Diante do exposto, é possível supor que as empresas que queiram conferir maior segurança aos seus dados deveriam adotar postura extremamente restritiva e conservadora, impedindo a realização do trabalho a partir de dispositivos particulares e o acesso à aplicativos pessoais. Nessa toada, a política corporativa de segurança da informação deveria conter previsão expressa no sentido de proibir o uso de dispositivos e aplicações particulares para finalidades corporativas, estabelecendo que o manuseio e comunicação de dados desta natureza somente poderia ocorrer por meio da infraestrutura tecnológica da empresa. Esta conduta, no entanto, seria de difícil implementação, já que segue na direção contrária da realidade da sociedade atual, cada vez mais conectada virtualmente.

Frente a iminente entrada em vigor da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD), existe a necessidade e obriga-

toriedade de regularizar as atividades de tratamento de dados pessoais para maior proteção dos mesmos. O *home office* passou a expor os dados pessoais tratados pelas empresas a uma realidade distinta daquela existente no ambiente corporativo tradicional. Ou seja, a violação de dados entendida como evento no qual um dado confidencial é colocado em risco, seja em formato eletrônico ou até mesmo em papel, acarretou novas possíveis oportunidades de soluções para a segurança da informação.

Estas soluções podem ocorrer de várias maneiras, desde o simples bloqueio da tela do dispositivo após o não uso por determinado período de tempo, até soluções mais sofisticadas como o caso da conteinerização. Importante ressaltar que com o número crescente de ataques cibernéticos no ambiente remoto de trabalho, incríveis 330% a mais entre os meses de fevereiro e abril deste ano, de acordo com o recente levantamento feito pela empresa de segurança em TI russa Kaspersky, a cultura empresarial diante desta modalidade laboral deverá treinar seus funcionários para o correto uso de dispositivos fora do ambiente corporativo, vale dizer, através de maior participação e debate entre a alta direção e seus colaboradores. Vale lembrar que o processo de participação dentro da boa governança corporativa oferece oportunidades para que as pessoas expressem suas ideias, dúvidas e preocupações.

A conteinerização poderia ser uma solução técnica possível apesar de não existir ainda previsão legal sobre o tema no Brasil diante da Justiça do Trabalho. Esta prática consiste em criar um contêiner dentro do dispositivo particular do funcionário para armazenar os dados da empresa, com a adoção de todos os controles de segurança necessários. Seria um espaço de trabalho segregado, criado dentro do dispositivo, com a funcionalidade de proteger os dados corporativos. Estes estariam separados do ambiente pessoal do funcionário naquele determinado dispositivo. Ou seja, o controle da empresa, portanto, seria restrito a este contêiner digital com a anuência do funcionário a fim de evitar eventuais problemas no tocante a violação da privacidade frente a esta solução.

Em suma, é sabido que nas crises é que se encontram as oportunidades. O *home office* que já era uma realidade em âmbito global e que com a atual crise sanitária se consolidou, trouxe à pauta novos desafios a superar. Ao mesmo tempo, com um mundo cada vez mais conectado virtualmente, oportunidades com base em boas soluções farão o diferencial na gestão das empresas no novo normal pós-pandemia.