
**INFORMATIVO**
**Nº 02**

# CORONAVÍRUS.

## PROTEÇÃO DE DADOS

Um estudo sobre as medidas práticas para conciliar saúde e proteção de dados pessoais e informações no contexto de trabalho remoto

MACHADO, MAZZEI & PINHO
ADVOGADOS

Stephanie Melo Sobral – Advogada Associada

Este pequeno texto tem como objetivo orientar gestores, diretores e empresários, principalmente no que se refere à segurança da informação e proteção de dados pessoais, em tempos de massificação do *home office* (teletrabalho).

Vive-se hoje no que é chamado de sociedade da informação, isto é, em ambiente condicionado pelas inovações tecnológicas, que permitem uma rápida difusão de informações e que se tornaram indispensáveis para o desenvolvimento pessoal e coletivo. Nesse contexto social, originado pelo desenvolvimento da internet e evolução da era industrial, o principal ativo de valor passam a ser dados. Passa-se a monetizar dados e, nesse cenário, toda informação tem valor.

Toda empresa armazena dados e informações necessárias à consecução de suas atividades e tomada de decisões, as quais interferem diretamente no lucro dos negócios.

Com o impacto mundial da pandemia da COVID-19, ou como amplamente conhecido coronavírus, atualmente há uma preocupação especial no que se refere à preservação e proteção de dados pessoais, assim como em relação à segurança das informações confidenciais corporativas.

Organizações públicas e privadas estão tomando as medidas necessárias para a defesa da saúde e, assim, conter a disseminação e mitigar os efeitos do COVID-19.

Por outro lado, os riscos estão se multiplicando com trabalhadores remotos e uso de dispositivos móveis, diante dos avançados mecanismos fraudulentos utilizados pelos criminosos para desbloquear, modificar e copiar arquivos do computador dos usuários.

As alternativas encontradas para superação da interrupção da rotina de trabalho conservadora, ainda muito cultivada no mundo corporativo, como a adoção de *home office* ou teletrabalho, exige superação de desafios aos empresários em relação a proteção dos dados de clientes e funcionários, além de informações da própria companhia.

Para garantir a disponibilidade dos recursos e informações, os cuidados com a segurança da informação e privacidade devem ser ampliados, garantindo-se a confidencialidade e integridade dos dados, especialmente em decorrência das determinações da Lei Geral de Proteção de Dados (LGPD) que entrará em vigor em agosto de 2020 e regulamenta o tratamento de dados pessoais.

Contudo, embora as multas estabelecidas sejam elevadas, podendo alcançar o valor de R$ 50.000.000,00 (cinquenta milhões de reais) por infração, não é pequeno o percentual de empresas brasileiras ainda não se adequaram à legislação.

Em um contexto global, é crescente o número, como já era de se esperar, de crimes virtuais envolvendo golpes com sites e e-mails falsos sobre a COVID-19, no intuito de difundir *malware* e *ransomware*[1], entre outros mecanismos de fraude e invasão que vem sendo criados diariamente.

Os hackers, ainda, estão cada vez mais voltados à vulnerabilidade das VPNs (Virtual Private Networks) corporativas, que podem não estar preparadas para lidar com milhares de colaboradores em *home office*. Apesar de primordiais à proteção das informações transmitidas entre colaboradores e organizações, na medida em que oferecem conexões seguras por meio da criptografia de dados, as VPNs podem não servir para proteger os dispositivos do funcionário remoto. E, se um hacker obtém acesso aos dispositivos dos colaboradores, os dados podem ser usados para acessar a rede e os servidores e, assim, a todo o conjunto de informações e dados de uma empresa.

Nesse cenário, para conciliar e promover o princípio basilar da dignidade humana, saúde dos colaboradores e de toda a sociedade, com os interesses e necessidade das empresas, sem menosprezar a proteção de dados pessoais e adequações da LGPD, bem como a segurança das informações corporativas, devem ser adotadas práticas de proteção de dados, servindo como sugestão:

- Definição do acesso de informação e de dados de acordo com as responsabilidades de cada colaborador, concedendo acesso apenas àqueles que precisam das informações para o desenvolvimento de suas atividades;

- Conscientização e orientação de políticas de segurança da informação e proteção de dados pessoais, interna e externa, delimitando as responsabilidades dos agentes de tratamento;

[1] Malware, em tradução livre, significa software malicioso. Já ransonware, basicamente, é um tipo de malware que bloqueio o computador e o proíbe de acessá-lo até que a vítima pague o resgate exigido. Fonte: https://pt.vpnmentor.com/blog/malware-e-ransomware-qual-e-diferenca/.

- Alteração periódica de usuário e senha, incluindo-se, aqui, também, a possibilidade de bloqueio automático da tela após um período sem uso (dispositivos pessoais e nos da empresa);

- Manutenção das ferramentas de sistemas de segurança atualizadas, especialmente em se tratando de dispositivo ou computador do próprio colaborador, que deve estar com os sistemas operacionais e de proteção instalados e atualizados, de modo a promover métodos de trabalho remoto atrelado à disponibilização de ferramentas com níveis de segurança a informação similares aos habitualmente adotados;

- Conscientização e orientação dos colaboradores sobre os cuidados pertinentes com o Wi-Fi público ou doméstico, e os riscos de abrir e responder a mensagem de remetentes desconhecidos, bem como acessar links ou baixar arquivos de origem, também, desconhecida;

- Conscientização e orientação dos colaboradores no sentido de evitar compartilhar informações confidenciais por e-mail ou por sistemas de mensagens;

- Instalação de monitoramento geográfico em dispositivos da empresa; utilização de autenticação de dois fatores; utilização da criptografia das informações, entre outros;

A partir da adoção de medidas de reforço na segurança para proteção dos dados e informações das empresas, é possível reduzir ou mitigar potencial danos, talvez irreparáveis para as empresas que deixarem de implementar procedimentos de segurança adequados, e não agirem com cautela, o que poderá comprometer até mesmo sua permanência no mercado.

Nesse contexto o trabalho remoto exige, das empresas, cuidado redobrado com a segurança e o sigilo das informações, as quais devem orientar seus colaboradores a seguir os procedimentos internos voltados a preservar a confidencialidade das comunicações e de dados a que tenham acesso.