

VAZAMENTO DE INFORMAÇÕES

“Meu ex-funcionário levou informações da minha empresa. E agora?”

Atualmente tem ocorrido cada vez mais a seguinte situação no meio corporativo: um colaborador desliga-se da empresa onde trabalha, passa a trabalhar em uma concorrente à sua ex-empregadora ou cria seu próprio negócio, passando a atuar no mesmo mercado da antiga empresa onde exercia suas funções. Até aqui, pode não haver problema, tendo em vista que o indivíduo provavelmente atuará em sua área de expertise, e considerando-se que não existia em seu contrato de trabalho cláusulas impeditivas, que criam uma proibição de atuação no mesmo nicho por determinado período, ou cláusulas de não concorrência, proibindo expressamente o colaborador de exercer suas atividades em empresas concorrentes.

Contudo, o problema se inicia a partir do momento em que o colaborador, ao assumir nova empreitada profissional, faz uso de informações privilegiadas às quais teve acesso em seu trabalho anterior ou viola expressamente cláusulas contratuais.

Nesse sentido, é muito comum o ex-funcionário ter acesso a banco de dados, cadastro de clientes e fornecedores, dados pessoais sensíveis, planos estratégicos de negócios, segredos comerciais e profissionais, bem como demais informações de alto know-how, por conta de suas funções ou do cargo de confiança que exercia previamente. Na rotina de trabalho, ao participar do desenvolvimento dos negócios ou ao ter acesso a este fluxo privilegiado de informações, muitas pessoas tem a falsa crença de que estas informações também lhe pertencem, o que é um engano, e acabam armazenando consigo todo esse histórico, levando para si próprio uma cópia desses dados, sem qualquer autorização. E assim, repassam isso para uma empresa concorrente ou utilizam na construção de seu próprio negócio autônomo.

Esse tipo de comportamento é muito grave, pode configurar alguns crimes, gerando responsabilidade para o indivíduo que o pratica e ocasionando danos (patrimoniais e de imagem) à empresa lesada.

Esses dados e informações portados indevidamente pelo ex-colaborador são de propriedade da empresa, fazem parte de seu core business e podem ser restritos.

(11) 3075-2843  (11) 98584-9279 contato@truzzi.com.br www.truzzi.com.br

Avenida Paulista, 1765, Conj. 72, CV 8828 - Bela Vista, São Paulo/SP - CEP 01311-200

 /truzziadvogados

 /truzziadvogados

 /giseletruzzi

 /giseletruzzi

 /giseletruzzi

Ao desligar-se de uma empresa e levar consigo informações privilegiadas ou ao repassar tais informações a um concorrente sem autorização, o ex-colaborador acaba incidindo numa prática que muitos chamam de “vazamento de informação”, que possui alguns desdobramentos jurídicos.

Quais são as implicações jurídicas relacionadas ao “vazamento de informação”?

O colaborador, no exercício de suas funções, ou após desligar-se da empresa, caso revele informações privilegiadas às quais teve acesso em razão de suas atividades, poderá estar incurso nas penas do crime de **violação do segredo profissional**, previsto no artigo 154 do Código Penal: *Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: Pena – detenção, de três meses a um ano, ou multa.*

Isso acaba ocorrendo quando o indivíduo repassa à concorrente ou à terceiro informações sigilosas da empresa onde trabalhou, às quais teve acesso justamente em função das atividades que exercia. Muitas vezes, o ex-colaborador faz uso próprio dessas informações, ao utilizá-las indevidamente como base para a construção de seu próprio negócio. Desta forma, além deste crime, ele poderá ter praticado também o delito de **concorrência desleal**, definido no artigo 195 da Lei 9279/96:

Comete crime de concorrência desleal quem:

I – publica, por qualquer meio, falsa afirmação, em detrimento de concorrente, com o fim de obter vantagem;

II – presta ou divulga, acerca de concorrente, falsa informação, com o fim de obter vantagem;

III – emprega meio fraudulento, para desviar, em proveito próprio ou alheio, clientela de outrem;

IV – usa expressão ou sinal de propaganda alheios, ou os imita, de modo a criar confusão entre os produtos ou estabelecimentos;

V – usa, indevidamente, nome comercial, título de estabelecimento ou insígnia alheios ou vende, expõe ou oferece à venda ou tem em estoque produto com essas referências;

VI – substitui, pelo seu próprio nome ou razão social, em produto de outrem, o nome ou razão social deste, sem o seu consentimento;

VII – atribui-se, como meio de propaganda, recompensa ou distinção que não obteve;

VIII – vende ou expõe ou oferece à venda, em recipiente ou invólucro de outrem, produto adulterado ou falsificado, ou dele se utiliza para negociar com produto da mesma espécie, embora não adulterado ou

(11) 3075-2843 (11) 98584-9279 contato@truzzi.com.br www.truzzi.com.br

Avenida Paulista, 1765, Conj. 72, CV 8828 - Bela Vista, São Paulo/SP - CEP 01311-200

falsificado, se o fato não constitui crime mais grave;
IX – dá ou promete dinheiro ou outra utilidade a empregado de concorrente, para que o empregado, faltando ao dever do emprego, lhe proporcione vantagem;
X – recebe dinheiro ou outra utilidade, ou aceita promessa de paga ou recompensa, para, faltando ao dever de empregado, proporcionar vantagem a concorrente do empregador;
XI – divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato;
XII – divulga, explora ou utiliza-se, sem autorização, de conhecimentos ou informações a que se refere o inciso anterior, obtidos por meios ilícitos ou a que teve acesso mediante fraude; ou
XIII – vende, expõe ou oferece à venda produto, declarando ser objeto de patente depositada, ou concedida, ou de desenho industrial registrado, que não o seja, ou menciona-o, em anúncio ou papel comercial, como depositado ou patenteado, ou registrado, sem o ser;
XIV – divulga, explora ou utiliza-se, sem autorização, de resultados de testes ou outros dados não divulgados, cuja elaboração envolva esforço considerável e que tenham sido apresentados a entidades governamentais como condição para aprovar a comercialização de produtos.
Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa.

§ 1º Inclui-se nas hipóteses a que se referem os incisos XI e XII o empregador, sócio ou administrador da empresa, que incorrer nas tipificações estabelecidas nos mencionados dispositivos.

Caso o indivíduo repasse à terceiros conteúdo de documento ou de correspondência confidencial ao qual possuiu acesso, seja por questões pessoais ou profissionais, por conta de suas atividades (o que pode ser exemplificado no encaminhamento não autorizado de um e-mail – tendo em vista que e-mail pode ser considerado como correspondência – ou de um contrato restrito), essa pessoa poderá ter praticado o crime de **divulgação de segredo**, definido no artigo 153 do Código Penal: *Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem: Pena – detenção, de um a seis meses, ou multa.*

Nesse exemplo podemos enquadrar aquelas situações em que o colaborador repassa para seu e-mail pessoal e para terceiros sem autorização, conteúdos privilegiados da empresa. Geralmente

este tipo de atitude visa fomentar algum concorrente ou alimentar futuras empreitadas autônomas do colaborador.

Quanto à divulgação de conteúdo restrito, contido em correspondência alheia, o indivíduo poderá ter cometido o crime de **violação de sigilo**, descrito no artigo 151 do Código Penal, ao acessar sem autorização e-mails, mensagens eletrônicas ou correspondência física de terceiros, sem a devida autorização:

*Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem:
Pena – detenção, de um a seis meses, ou multa.*

No ambiente corporativo, essa situação geralmente ocorre quando um colaborador de determinado departamento, por ter um cargo específico com maiores acessos ao ambiente eletrônico, acaba visualizando, sem a devida autorização, e-mails de outros colaboradores. É importante lembrar que o sócio também poderá praticar delitos semelhantes, em detrimento do outro sócio, relacionado ao desvio ou divulgação de correspondência, inclusive eletrônica, podendo estar incurso nas penas do artigo 152 do Código Penal, que trata do crime de **violação de correspondência comercial**: *Abusar da condição de sócio ou empregado de estabelecimento comercial ou industrial para, no todo ou em parte, desviar, sonegar, subtrair ou suprimir correspondência, ou revelar a estranho seu conteúdo:*

Pena – detenção, de três meses a dois anos.

Caso o indivíduo que divulgue informações privilegiadas da instituição onde trabalha seja servidor público, o crime praticado será o de **violação de sigilo funcional**, definido no artigo 325 do Código Penal: *Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação:*

Pena – detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave.

Além destes crimes relacionados à violação do sigilo das informações privilegiadas da instituição, dependendo do conteúdo divulgado e dos detalhes dessa divulgação, o indivíduo poderá também sofrer as penas do crime de **violação de direitos autorais**, descrito no artigo 184 do Código Penal:

Violar direitos de autor e os que lhe são conexos:

Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa.

Há situações em que esta prática ocorre quando o ex-colaborador faz uso de conteúdos da empresa em seu próprio nome, atribuindo a si próprio a autoria exclusiva de um material.

O que fazer se minha empresa for vítima dessas práticas?

Havendo indícios dessas práticas por algum colaborador ou ex-colaborador, é essencial que a empresa trate do caso com total sigilo e se municie de todas as provas possíveis, tomando as seguintes providências emergenciais:

1. Armazenar todas as provas eletrônicas do ocorrido (guardar os e-mails e mensagens originais, telas de sistemas, etc. Jamais apagar o conteúdo relacionado);
2. Lavrar uma ata notarial do ocorrido (a ata notarial é uma espécie de certidão, elaborada por Tabelião de Notas, onde este descreverá o que está sendo visualizado em um e-mail, mensagem, site, etc., podendo inserir prints de imagem. Pelo fato do Tabelião ter fé pública, a ata notarial é uma prova totalmente válida em juízo);
3. Caso se trate de uma situação possível de ser visualizada publicamente em um site na internet, a prova deste material poderá ser efetuada através de sites que disponibilizam tecnologia blockchain para comprovação de autenticidade de conteúdo digital;
4. Dependendo da situação, poderá ser necessária a contratação de perícia específica (perito em computação forense) para produção de provas;
5. Registrar Boletim de Ocorrência (poderá ser feito na delegacia mais próxima);
6. Procurar um advogado capacitado para tratar destas questões. O advogado poderá analisar a possibilidade de se ingressar com ações judiciais específicas para o caso (ação cível para coibir o uso das informações, por exemplo; ou ação criminal com o intuito de punir o indivíduo pelos crimes cometidos).

O que fazer para evitar essas situações?

A fim de prevenir a ocorrência de tais problemas, é recomendável:

1. Elaboração e assinatura de Termo de Confidencialidade por todos os colaboradores, gestores e diretores;
2. Criação de um Código de Conduta para inibir o vazamento de informações privilegiadas pelos funcionários;
3. Elaboração de Normas de Segurança da Informação e Política de Segurança da Informação;
4. Revisão/elaboração de contratos de trabalho ou de prestação de serviços com cláusulas específicas

(11) 3075-2843 (11) 98584-9279 contato@truzzi.com.br www.truzzi.com.br

Avenida Paulista, 1765, Conj. 72, CV 8828 - Bela Vista, São Paulo/SP - CEP 01311-200

ou constantes de Regimento Interno comprovando a ciência e aceitação de todos. (O Regimento Interno serve para criar uma comissão ou conselho de ética e apurar denúncias ou indícios de vazamento, por exemplo, a fim de fiscalizar os atos preparatório ou de execução como o envio aos poucos de conteúdo restrito ao e-mail pessoal, pen drives com armazenamento de dados estratégicos ou em desenvolvimento, etc.). Isso ajuda nas advertências na carteira de trabalho (CTPS) e até em demissão por justa causa, além de facilitar as diligências de autoridades;

5. Implantação de monitoramento eletrônico no ambiente online da empresa, mediante prévio aviso aos colaboradores;
6. Elaboração e assinatura de Termo de Uso de Dispositivos Móveis;
7. Realização de backups frequentes no ambiente online da empresa;
8. Segregação de redes no ambiente online da empresa, com acessos disponíveis conforme os cargos e atividades exercidas;
9. Segregação de funções para realização de atividades complexas e extremamente sigilosas.

Em se tratando de tecnologia e pessoas, não há como garantir 100% de proteção contra riscos, mas adotando-se melhores procedimentos jurídicos e tecnológicos é possível mitigar tais riscos, reduzindo-se assim, eventuais danos à empresa e sua reputação.

Gisele Truzzi

Advogada especialista em Direito Digital e fundadora de Truzzi Advogados.