

QUANTO VALE A INFORMAÇÃO DA SUA EMPRESA? ELA ESTÁ DEVIDAMENTE PROTEGIDA?

Cristina Moraes Sleiman¹

INTRODUÇÃO

Em época de disputa por know-how e liderança de mercado a busca pelo avanço tecnológico passa a ser essencial para qualquer modelo de negócio. Desenvolvem-se sistemas robustos, os quais suprem a necessidade de contratações humana, mas é certo que muitos negligenciam nos quesitos jurídicos.

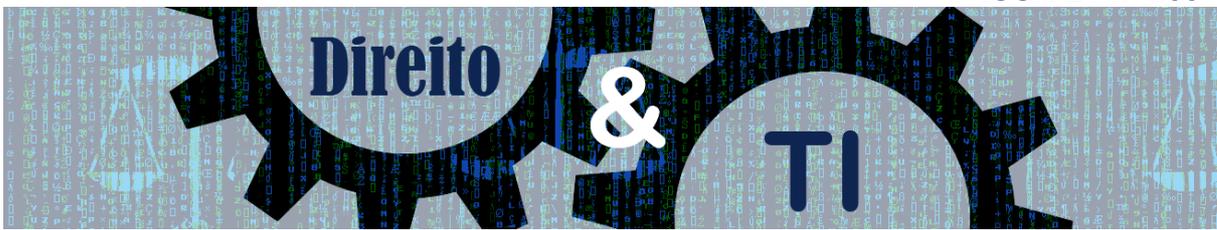
Em tecnologia quase tudo é possível, ou seja, tecnicamente o sistema pode sofrer comandos que determinam que faça o que for necessário para atender ao negócio da empresa, mas quem determina tais comandos é o ser humano, que também deve ser preparado.

Historicamente, sabemos que tudo que foi criado para o bem também teve utilidade para o mal. Assim ocorreu com a pólvora e o avião e assim ocorre também com a tecnologia, que passa a ser uma poderosa arma para a concorrência desleal.

Dentro deste cenário a blindagem legal se faz necessária, através de regulamentos internos, sendo que a capacitação e conscientização de pessoas também é um fator importante para caracterização de boa fé da empresa em caso de incidentes e demandas judiciais.

Neste cenário, faz-se necessário alguns esclarecimentos jurídicos tanto em relação a responsabilidade das empresas na disponibilização de recursos tecnológicos a seus colaboradores, quanto às informações que detém.

¹ Mestre em Sistema Eletrônicos/ Engenharia Elétrica pela Escola Politécnica da USP. Advogada (OAB/SP 234.349) formada pela Faculdades Capital (2004) e graduação em Pedagogia pela Universidade São Judas Tadeu (1992). Extensão em Educador Virtual pelo Senac em parceria com Simon Fraser University e extensão em Direito Da Tecnologia pela FGV/RJ. Atua na área de Direito Digital. Experiência na área educacional pedagógica e jurídica voltada à tecnologia e à legislação educacional. Atuou no Senac São Paulo na Gerencia de Desenvolvimento Educacional como supervisora educacional e no projeto de Novas Tecnologias de Informação e Comunicação em Educação e posteriormente na Gerência de Sistemas com projetos de internet e Política de Segurança da Informação. Ex sócia do escritório Patrícia Peck Pinheiro Advogados. Coautora do Audiolivro e pocket book Direito Digital no Dia a Dia e da Cartilha Boas Práticas de Direito Digital Dentro e Fora da Sala de Aula. Atual consultora do Colégio Bandeirantes para implementação do Projeto de Ética e Cidadania Digital. Sócia do escritório Cristina Sleiman Sociedade de Advogados e responsável pela Coordenadoria de Gestão do Risco Eletrônico no ambiente Corporativo da Comissão de Direito Eletrônico e Crimes de Alta Tecnologia da OAB/SP. Professora de Pós Graduação na Faculdade Impacta de Tecnologia e Palestrante sobre os temas de Direito Digital e Ética e Cidadania Digital.



1 QUANTO VALE A SUA INFORMAÇÃO?

Toda a empresa pode e deve decidir pelo grau de segurança jurídica de suas atividades, especialmente quando se fala em tecnologia. Além da questão de responsabilidade pelos meios que disponibiliza, as empresas possuem um bem muito valioso, a informação! Trata-se, portanto, de ativo intangível e que não pode ser negligenciado.

Com foco no próprio negócio, a empresa deve levantar quais são seus ativos e qual o seu valor. Para exemplificar, quanto vale seu banco de dados em sua totalidade ou mesmo em informações fragmentadas? As informações e dados de clientes, fornecedores, orçamentos, protótipos, informações de processos produtivos, entre outros.

Lida-se com tais ativos diariamente, mesmo que despercebidos por muitos. Mas é preciso tomar algumas precauções, pois tais informações “em mãos” erradas podem causar – e efetivamente causam – danos e perdas à empresa.

A primeira pergunta sobre esse assunto é: A empresa possui um modelo de NDA (*Non Disclosure Agreement* - Acordo de Confidencialidade) devidamente estruturado?

O contrato de confidencialidade é muito importante e, com certeza, grandes empresas exigem sua assinatura antes mesmo de mandar um desenho ou um protótipo para orçamento, por exemplo, mas esta prática, muitas vezes, é negligenciada por pequenas e médias empresas.

Preventivamente, o NDA deve ser assinado entre empresas e também com pessoas físicas, contratados ou prestadores de serviços que venham a tomar conhecimento de qualquer informação importante.

Nos casos de CLT, quanto aos já contratados, pode-se assinar um termo específico, já que para as novas contratações deve-se atualizar o contrato de trabalho com cláusulas de confidencialidade e também de Segurança da Informação, específicas de Direito Digital.

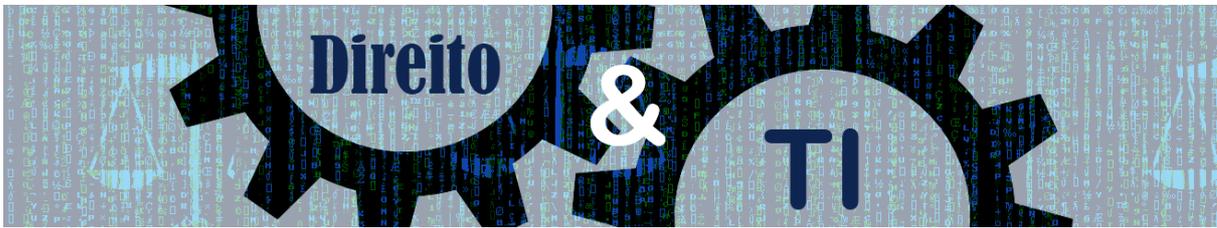
2 RESPONSABILIDADE CIVIL DA EMPRESA

Preceitua o art. 932 do Código Civil a responsabilidade objetiva das empresas em relação ao seu empregado:

Art. 932. São também responsáveis pela reparação civil:

I - os pais, pelos filhos menores que estiverem sob sua autoridade e em sua companhia;

II - o tutor e o curador, pelos pupilos e curatelados, que se acharem nas mesmas condições;



III - o empregador ou comitente, por seus empregados, serviçais e prepostos, no exercício do trabalho que lhes competir, ou em razão dele;

IV - os donos de hotéis, hospedarias, casas ou estabelecimentos onde se albergue por dinheiro, mesmo para fins de educação, pelos seus hóspedes, moradores e educandos;

V - os que gratuitamente houverem participado nos produtos do crime, até a concorrente quantia. (grifo nosso)

Para contribuir com este entendimento, podemos citar a sumula 341 do STF: **“É presumida a culpa do patrão ou comitente pelo ato culposo do empregado ou preposto.”** Portanto, ainda que não tenha culpa direta, o empregador responde pelos danos causados por seu colaborador, enquanto este estiver no exercício de suas funções ou fazendo uso dos recursos que este disponibiliza.

Art. 933. As pessoas indicadas nos incisos I a V do artigo antecedente, ainda que não haja culpa de sua parte, responderão pelos atos praticados pelos terceiros ali referidos.

Com base neste dispositivo, caso um empregado cometa o crime de ameaça utilizando recursos tecnológicos da empresa e, por consequência, seja caracterizado dano moral ou material proveniente destas ameaças, a empresa poderá figurar no polo passivo de uma ação civil para fins de reparação de danos.

O mesmo se aplica às instituições de ensino em relação a seus educandos e aos hotéis em relação aos seus hóspedes, conforme dispõe o art. 932 do Código Civil citado cima, em seu inciso IV.

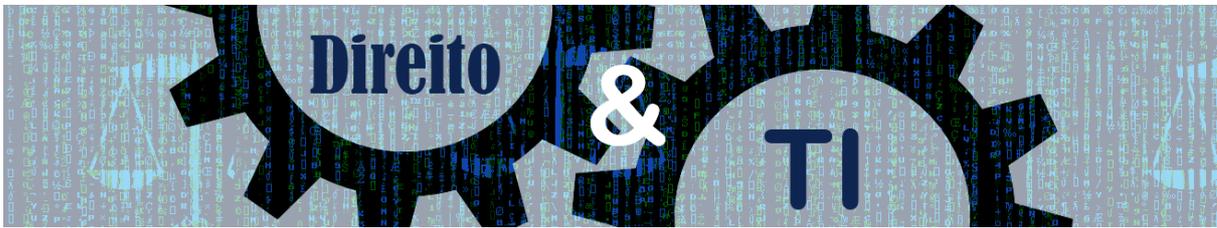
Cabe esclarecer, que embora a empresa tenha responsabilidade objetiva, ocorrendo uma eventual condenação esta poderá pleitear em juízo o ressarcimento do dano que lhe foi causado por determinado agente:

Art. 934. Aquele que ressarcir o dano causado por outrem pode reaver o que houver pago daquele por quem pagou, salvo se o causador do dano for descendente seu, absoluta ou relativamente incapaz.

Por fim, cabe esclarecer que a responsabilidade civil é independente da responsabilidade penal, ou seja, tratam-se de processos independentes. No entanto, o resultado da ação penal poderá interferir na ação civil:

Art. 935. A responsabilidade civil é independente da criminal, não se podendo questionar mais sobre a existência do fato, ou sobre quem seja o seu autor, quando estas questões se acharem decididas no juízo criminal.

Cabe, também, menção ao art. 1016 do Código Civil, que preceitua a responsabilidade solidária dos administradores: *Os administradores respondem solidariamente perante a sociedade e os*



terceiros prejudicados, por culpa no desempenho de suas funções.

CONCLUSÃO

O tema escolhido para este artigo é extenso e pode ser discutido em detalhes, diferenciando segmentações e tecnologias. No entanto, o intuito foi apenas uma introdução ao assunto a fim de possibilitar novos artigos específicos para determinadas situações.

Desta feita, conclui-se que – no quesito legal – as empresas ainda não atingiram o nível de segurança desejável a fim de blindar sua estrutura para prevenção de eventuais incidentes que tragam responsabilidade jurídica a seus gestores.

É preciso planejamento e aplicar princípios de Gestão de Risco considerando as questões jurídicas de forma que, essencialmente, o *compliance* passa a ser requisito para a maior nível de segurança e proteção às empresas.

Resta, assim, possibilitar a adoção de algumas ações:

1. Criar regras em relação à Segurança da Informação (Políticas e Normas);
2. Considerar a criação de Norma de classificação e tratamento da informação (rotulagem, confidencial, publica etc.);
3. Atualizar os contratos de trabalho e prestadores de serviços com cláusulas de Direito Digital, incluindo responsabilidade e confidencialidade;
4. Criar termos de responsabilidade e de confidencialidade para os colaboradores já contratados;
5. Monitorar as informações e ferramentas exclusivas, pois a divulgação de sua informação pode custar muito caro.

REFERÊNCIAS

BRASIL. Lei nº 10.406 de 10 de janeiro de 2002. Institui o Código Civil. **Portal da Legislação**. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm>. Acesso em: 15 set. 2015.