

CARLOS F. SANTOS CARVALHO

ADVOGADO

Circular:

5-8^a

MÊS

Junho

Assunto: Cibercrime; sabotagem e espionagem informática.

Reparou, por acaso, que no D.R. n.º 113, 1.ª Série, 12 Junho 2015, foi publicada a **RESOLUÇÃO CONSELHO MINISTROS N.º 36/2015?**

Não reparou! – É natural; com tanta produção legislativa, tentando transformar-nos em mais uma "ovelha" deste grande rebanho que os Governos da Europa, --- e o nosso em particular ---, transformaram o velho continente,

Ninguém ligou nenhuma. É mais uma e, só neste ano, já lá vão... 36! – Contudo, **olhe que esta é importante**. Trata da segurança do ciberespaço, que dizem ser "... uma prioridade nacional". Pretende-se definir linhas de orientação para algo que, como INDUSTRIAL, lhe deve interessar: combater o cibercrime; protecção do ciberespaço e infraestruturas; educação, sensibilização e prevenção; investigação e desenvolvimento. Vejamos:

O "roubo de identidade", entendendo-se como tal a fuga de dados e o acesso não autorizado a informação sensível de uma empresa, --- ou de um indivíduo ---, é uma realidade. Milhões de euros são perdidos em propriedade intelectual quando o software; o desenho de um produto; contratos de todo o tipo; listas de clientes ou fornecedores; formulários ou ordens escritas; planos gerais ou sectoriais são roubados, ilegalmente copiados. E,

A perda pode resultar de actuação interna ou externa. Estes últimos, os conhecidos "hackers" (ladrões), actuam de 2 maneiras: ou entram nas instalações das empresas e roubam os dados; ou, do exterior, acedem (mesmo remotamente) aos sistemas, usando software criminoso, roubando informação e transferindo-a para equipamento sofisticado, que controlam. Mas,

Tem crescido o perigo, a ameaça, que constituem os utilizadores internos, --- os próprios trabalhadores da organização industrial. O que pode também revestir várias formas: perda dos portáteis (computadores, pens); por mero acidente, não propositado; ou o roubo de dados, com o fim de vender, obtendo lucros, --- de várias espécies: dinheiro; pagamento favores; acesso a nova empresa, com a entrega de segredos.

Infelizmente, pois é uma má prática, os trabalhadores transportam informação do trabalho para casa; ou, deste para a empresa, por meio de dispositivos móveis. Em, clara violação, por ex., do n.º 1, art.º 214, C.T. (vá ver).

CARLOS F. SANTOS CARVALHO
ADVOGADO

É opinião dos especialistas que, mesmo altos níveis de segurança transversal, --- tecnologia de ponta; sofisticadas soluções de gestão de identidade; antivírus de alta estabilidade ---, não garantem, só por sim, níveis altos de segurança informática. Pelo que, a segurança dos dados das organizações industriais ou comerciais; ou das pessoas, tem de ser uma prioridade no estado actual das tecnologias de comunicação e de informação. Daí,

Não confie nos Tribunais. Estes, valorizam o princípio da privacidade: acesso ao computador do trabalhador, sem sua autorização; ou, da presença dos representantes do mesmo, ou das autoridades, --- veja o art.º 22, CT.

Conhecendo a dimensão e complexidade do problema, os governos tentam combater o mesmo. Em Portugal, temos (não é exaustivo):

- Decreto do Presidente da República n.º 91/2009, 15 Setembro – aprova a Convenção sobre o Cibercrime, Budapeste 23 Nov. 2011.
- Lei n.º 109/2009, 15 Setembro – dita, Lei do Cibercrime, estabelecendo disposições penais, materiais e processuais.
- Portaria n.º 372/2012, 16 Novembro – fixa requisitos técnicos mínimos das câmaras fixas e portáteis. E, já gora,
- O Código do Trabalho, arts. 16; 17 e 22, devendo ter em especial atenção o n.º 2, deste art.º 22.
- O Centro Nacional de Cibersegurança – CNCS.

Não obstante esta quantidade de normas, o Governo veio lembrar agora, que estas novas tecnologias são vulneráveis, criando "...riscos sociais e materiais". Em anexo à Res. Cons. Min. N.º 36/2015, apresenta a Estratégia Nacional de Segurança do Ciberespaço. São 6 os objectivos desta Estratégia. Não interessa à iniciativa privada, o primeiro: "Estrutura de segurança do ciberespaço". Mas, já interessa os outros cinco objectivos: combate ao cibercrime; protecção do ciberespaço e das infraestruturas; educação, sensibilização e prevenção; investigação e desenvolvimento; cooperação.

No que refere ao combate ao cibercrime (Eixo 2), um dos objectivos é a permanente actualização da legislação; do sistema judicial (PJ).

O segundo objectivo, em importância, é o "Eixo 3", Protecção do ciberespaço e das infraestruturas. Veja em especial o n.º 9.

Falce-nos conhecimentos para tratar de assunto de tanta importância. Pelo que, apenas nos resta dar conhecimento desta Resolução n.º 36/2015; e, solicitar, se for do seu interesse, uma leitura. E, já agora, temos a certeza que será do interesse do Sr. Industrial ou Comerciante.

