NOTA INFORMATIVA

PROPRIEDADE INTELECTUAL, MARCAS E PATENTES

LEI DO CIBERCRIME

I. INTRODUÇÃO

Foi publicada no passado dia 15 de Setembro a Lei n.º 109/2009 de 15 de Setembro, a qual aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

Simultaneamente com a publicação da Lei do Cibercrime, foram no mesmo dia aprovadas e ratificadas a Convenção sobre o Cibercrime, adoptada em Budapeste em 23 de Novembro de 2001[1]- e o Protocolo Adicional à Convenção sobre o Cibercrime Relativo à Incriminação de Actos de Natureza Racista e Xenófoba Praticados através de Sistemas Informáticos, adoptado em Estrasburgo em 28 de Janeiro de 2003[2].

A Lei do Cibercrime tem como objecto estabelecer as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico, em matéria relativa a ataques contra sistemas de informação.

[1] Aprovada pela Resolução da Assembleia da República 88/2009 e ratificada pelo Decreto do Presidente da República 91/2009. De referir que a Convenção sobre o Cibercrime foi aprovada com reserva, excluindo-se a possibilidade de Portugal conceder a extradição em determinados casos, como sejam a extradição: (i) de cidadãos portugueses, (ii) por crimes a que corresponda pena de morte segundo a lei do Estado requerente, (iii) por crime punível com pena privativa da liberdade inferior a um ano, ou (iv) nos casos em que a pessoa em causa deva ser julgada ou cumprir uma pena com carácter perpétuo ou decretada por um tribunal de excepção.

[2] Aprovada pela Resolução da Assembleia da República 91/2009 e ratificada pelo Decreto do Presidente da República 94/2009.

FUNDAÇÃO PLMJ

João Paulo Feliciano
Detalhe
Obra da Colecção
da Fundação PLMJ

"Sociedade de Advogados Portuguesa do Ano"
Chambers Europe Excellence 2009, IFLR Awards 2006 & Who's Who legal Awards 2006, 2008, 2009

"Melhor Sociedade de Advocacia de negócios da Europa do Sul"
ACQ Finance Magazine, 2009

"Melhor Sociedade de Advogados no Serviço ao Cliente"
Clients Choice Award - International Law Office, 2008

"Melhor Departamento Fiscal do Ano"
International Tax Review - Tax Awards 2006, 2008

Prémio Mind Leaders Awards ™
Human Resources Suppliers 2007

PLMJ
A.M.PEREIRA, SÁRAGGA LEAL, OLIVEIRA MARTINS, JÚDICE E ASSOCIADOS
SOCIEDADE DE ADVOGADOS, RL

II. DISPOSIÇÕES PENAIS MATERIAIS

A nova lei define 6 tipos de crimes, aos quais cabem as seguintes sanções:

(i)	Falsidade informática	Pena de prisão até 5 anos ou pena de multa de 120 a 600 dias (a tentativa não é punível).
(ii)	Dano relativo a programas ou outros dados informáticos	Pena de prisão até 3 anos ou pena de multa. Se o dano causado for de valor elevado, a pena é de prisão até 5 anos ou de multa até 600 dias. Se o dano causado for de valor consideravelmente elevado, a pena é de prisão de 1 a 10 anos (a tentativa é punível, dependendo o procedimento penal quase sempre de queixa).
(iii)	Sabotagem informática	Pena de prisão até 5 anos ou pena de multa até 600 dias. A pena é de prisão de 1 a 5 anos se o dano emergente da perturbação for de valor elevado, podendo ser de 1 a 10 anos em casos especiais (a tentativa é punível em alguns casos).
(iv)	Acesso ilegítimo	Pena de prisão até 1 ano ou pena de multa até 120 dias. A pena é de prisão até 3 anos ou multa se o acesso for conseguido através de violação de regras de segurança. A pena é de prisão de 1 a 5 anos quando: (i) através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou (ii) o benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado (a tentativa é quase sempre punível, dependendo o procedimento penal de queixa na maioria dos casos).
(v)	Intercepção ilegítima	Pena de prisão até 3 anos ou pena de multa (a tentativa é punível).
(vi)	Reprodução ilegítima de programa protegido	Pena de prisão até 3 anos ou pena de multa (a tentativa é punível).

De notar que as pessoas colectivas e entidades equiparadas são penalmente responsáveis pelos crimes mencionados acima nos termos e limites do regime de responsabilização previstos no Código Penal.

Decorre também da Lei do Cibercrime a possibilidade de o tribunal decretar a perda a favor do Estado dos objectos, materiais, equipamentos ou dispositivos que tiverem servido para a prática dos crimes acima referidos e pertencerem a pessoa que tenha sido condenada pela sua prática, aplicando-se à avaliação, utilização, alienação e indemnização de bens apreendidos pelos órgãos de polícia criminal que sejam susceptíveis de vir a ser declarados perdidos a favor do Estado é aplicável o disposto no Decreto–Lei n.º 11/2007, de 19 de Janeiro[3].

[3] O qual regula o regime jurídico da avaliação, utilização, alienação e indemnização de bens apreendidos pelos órgãos de polícia criminal, no âmbito de processos crime e contra-ordenacionais, que sejam susceptíveis de vir a ser declarados perdidos a favor do Estado e regula os respectivos procedimentos.

III. DISPOSIÇÕES PROCESSUAIS

No que respeita ao âmbito de aplicação das disposições processuais é previsto que, com excepção do disposto relativamente a intercepção de comunicações e acções encobertas, as disposições processuais previstas na Lei do Cibercrime se apliquem a processos relativos a crimes (i) previstos nesta lei, (ii) cometidos por meio de um sistema informático ou (iii) em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico.

De referir que estas disposições processuais não prejudicam o regime da conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, plasmado na Lei n.º 32/2008, de 17 de Julho.

A quase totalidade das disposições processuais previstas prende-se com a necessidade de fazer ou manter a prova, sempre mais complexa no âmbito do Cibercrime, sobretudo no que toca a dados informáticos[4] e dados de tráfego[5]. Assim, são previstas disposições processuais relativas a: (i) preservação expedita de dados; (ii) revelação expedita de dados de tráfego; (iii) injunção para apresentação ou concessão do acesso a dados; (iv) pesquisa de dados informáticos; (v) apreensão de dados informáticos; (vi) apreensão de correio electrónico e registos de comunicações de natureza semelhante; (vii) intercepção de comunicações; (viii) acções encobertas.

[4] "Dados informáticos" são definidos como qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função.

[5] "Dados de tráfego" são definidos como os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.

Em sede de disposições finais e transitórias são clarificadas algumas regras relevantes sobre a aplicação no espaço da lei penal portuguesa e competência dos tribunais portugueses.

IV. COOPERAÇÃO INTERNACIONAL

A Lei do Cibercrime prevê ainda, no âmbito da cooperação internacional, que as autoridades nacionais competentes cooperem com as autoridades estrangeiras competentes para efeitos de investigações ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos, bem como para efeitos de recolha de prova, em suporte electrónico, de um crime, de acordo com as normas sobre transferência de dados pessoais previstas na Lei da Protecção de Dados Pessoais[6].

No âmbito desta cooperação, prevêem-se regras específicas para a cooperação internacional relativas: (i) à criação de um ponto de contacto permanente; (ii) à preservação e revelação expeditas de dados informáticos; (iii) ao acesso a dados informáticos; e (iv) à intercepção de comunicações.

V. DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Em sede de disposições finais e transitórias são clarificadas algumas regras relevantes sobre a aplicação no espaço da lei penal portuguesa e competência dos tribunais portugueses.

Assim, é esclarecido que a lei penal portuguesa é aplicável a factos: (i) praticados por Portugueses, se aos mesmos não for aplicável a lei penal de nenhum outro Estado; (ii) cometidos em benefício de pessoas colectivas com sede em território português; (iii) fisicamente praticados em território português, ainda que visem sistemas informáticos localizados fora desse território; ou (iv) que visem sistemas informáticos localizados em território português, independentemente do local onde esses factos forem fisicamente praticados.

Caso os tribunais portugueses e os tribunais de outro Estado membro da União Europeia sejam simultaneamente competentes para conhecer de um dos crimes previstos na Lei do Cibercrime, prevê-se que a autoridade judiciária competente recorra aos órgãos e mecanismos instituídos no seio da União Europeia para facilitar a cooperação entre as autoridades judiciárias dos Estados membros e a coordenação das respectivas acções, por forma a decidir qual dos dois Estados instaura ou prossegue o procedimento contra os agentes da infracção, tendo em vista centralizá-lo num só deles.

A Lei do Cibercime revoga a Lei da Criminalidade Informática (Lei n.º 109/91, de 17 de Agosto), entrando em vigor em 15 de Outubro de 2009.

[6] Lei n.º 67/98, de 26 de Outubro.