



## **Intervenção do Ministro da Administração Interna na conferência «O Desafio da Cibersegurança»**

16 de fevereiro de 2012

Exmo Senhor Secretário Geral do Sistema de Segurança Interna  
Exmo Senhor Secretário Geral do Sistema de Informações da República Portuguesa  
Exma Senhora Procuradora Geral Adjunta  
Exmos Senhores Dirigentes e Membros das Forças e Serviços de Segurança  
Minhas Senhoras e Meus Senhores

Esta conferência sobre os Desafios da Cibersegurança, organizada pelo Observatório de Segurança, Crime Organizado e Terrorismo e pela Portugal Telecom é uma excelente oportunidade para pormos em comum preocupações, objetivos e metas em matéria de tão crucial relevância para a segurança.

Durante estes trabalhos foram abordadas temáticas diversas relacionadas com estratégias, perfis, prevenção e reação perante as ameaças concretas que impendem sobre toda a infraestrutura que sustenta a sociedade da informação e que é hoje parte integrante do nosso modo de vida em sociedade.

Aqui estiveram representantes do Estado e do sector privado, sublinhando-se assim o carácter transversal dos desafios da Cibersegurança.

De facto, não existe Governo, Grupo Empresarial, Organização Não Governamental ou Universidade que prescindam hoje das capacidades que as novas tecnologias da informação e da comunicação digitais oferecem.

A organização administrativa da sociedade assenta sobre esta plataforma de comunicação, encarada também como uma condição para aproximar os Cidadãos do Estado, os utentes das instituições ou os Clientes de Empresas. É um recurso indispensável para garantir eficiência e eficácia a qualquer organização.

Trata-se, por isso, de um meio insubstituível para a promoção da transparência e publicidade dos atos garantindo portas de acesso dos cidadãos à informação e ao conhecimento.

Como sempre que se criam novas oportunidades, também neste caso surgem novos riscos que impendem sobre a segurança dos sistemas públicos e privados e sobre a segurança dos dados neles contidos, muitas vezes dados pessoais.

Este desenvolvimento tecnológico é também susceptível de criar ferramentas capazes de transformar ataques cibernéticos em verdadeiros atos de guerra, através de intrusões



hostis como manipulação ou sabotagem de infraestruturas críticas, sejam estas de comunicações, estruturas industriais sensíveis, sistemas de navegação e transportes, redes de energias, banca e serviços financeiros e outros sistemas determinantes para o nosso viver coletivo.

Por tudo isto, só asseguramos a plenitude das vantagens e oportunidades que o ciberespaço nos oferece se garantirmos a confiança da sua fiabilidade e resiliência a ameaças externas.

Por esta razão, também a sociedade da informação necessita de mecanismos reguladores capazes de certificar o acesso à informação em condições de segurança por forma a garantir os direitos dos Cidadãos, a inviolabilidade da privacidade nas comunicações e a funcionalidade em segurança dos sistemas e infraestruturas sensíveis.

A cibersegurança estende-se, por isso, a todos os atos relativos à proteção da confidencialidade, integridade e disponibilidade da informação no ciberespaço, independentemente da sua classificação e fins para os quais tenha sido criada.

Minhas Senhoras e Meus Senhores,

A universalidade que o ciberespaço promove constitui uma ferramenta comunicacional intransponível entre Governos e governados à qual os primeiros não têm sido alheios através do chamado *e-government*.

A própria União Europeia, com os vários planos de ação **eEurope** veio incentivar o desenvolvimento de serviços, aplicações e conteúdos em banda larga securizada à Internet.

A Agência europeia de Segurança das Redes e da Informação (ENISA), criada em 2004, traduz precisamente a valorização da ciber-ameaça, visando assegurar um elevado e efetivo nível de segurança informática na União Europeia, através do desenvolvimento de estratégias de cibersegurança que espelham a prioridade de todos os Estados-Membros da União no sentido de uma política concertada neste domínio.

Uma iniciativa muito recente vem propor a criação de uma Equipa de Resposta de Emergência Informática no quadro da União Europeia, tendo em vista a proteção do sistema contra ciberataques.

Igual preocupação expressou o Conselho da Europa, por exemplo, através da Convenção sobre Cibercrime, de 2001, onde se instou os Estados-membros a adotar um conjunto de medidas legislativas com vista a impedir o acesso e utilização não autorizada de dados informáticos, medidas de prevenção e controlo à pornografia infantil na internet, de defesa da propriedade intelectual, entre outras.

No trabalho desenvolvido nesta área no seio da União Europeia, concluído em 2010 com a aprovação da Estratégia de Segurança Interna da União Europeia, a cibercriminalidade é reconhecida como uma ameaça mundial, técnica, transfronteiriça e anónima para os nossos sistemas de informação.



Portugal acompanhou a doutrina internacional e integrou o normativo europeu na sua ordem interna, através da Lei do Cibercrime (nº 109/2009, de 15 de Setembro).

Neste diploma tipificam-se as disposições penais materiais para o cibercrime - falsidade informática, sabotagem informática, acesso ilegítimo, interceção ilegítima ou reprodução ilegítima – com diretas implicações em disposições do Código Penal, da Lei de Proteção de Dados Pessoais e com o Código do Direito de Autor e dos Direitos Conexos.

Neste contexto, interessa agora implementar a moldura existente e dotarmos o nosso país de sistemas fiáveis e seguros através de estratégias de prevenção e da constante monitorização dos riscos.

A definição de uma política de cibersegurança deverá estruturar-se em 4 vetores de atuação:

1. Garantir a segurança e confidencialidade da Infraestrutura de tecnologias de informação e da comunicação;
2. Definir estratégias políticas de segurança assentes na análise e gestão de riscos;
3. Alinhamento e integração operacional das organizações no equilíbrio necessário entre o direito à privacidade e a necessidade de acesso à informação por parte das Forças e Serviços de Segurança em nome da defesa da segurança;
4. E criação de uma relação de parceira entre o sector público e o sector privado em moldes aceites por todos, a funcionar em rede e de forma desburocratizada.

O primeiro passo está dado: a Resolução do Conselho de Ministros 12/2012, de 7 de Fevereiro, veio, na esteira das conclusões do **Grupo de Projecto para as Tecnologias da Informação e Comunicação**, definir as linhas gerais de uma **Estratégia Nacional de Segurança da Informação (ENSI)**.

É necessário assegurar partilha e distribuição de informação sobre ciber-ameaças, incorporar capacidade de reação articulada ao cibercrime e estruturar a formação técnica neste domínio em coordenação com escolas e centros de conhecimento especializados.

A implementação dessa estratégia passará pela criação de um **Centro Nacional de Cibersegurança**, pela melhoria das condições operacionais do **Sistema de Certificação Electrónica do Estado (SCEE)**, pelo desenvolvimento de uma solução de **criptografia de origem nacional** e pela **revisão do quadro legal** existente sobre informação classificada, ou seja, dos actuais SEGNA C's.

Foi decidido, o que releva a valoração que o Governo confere a esta matéria, que a Estratégia Nacional de Segurança da Informação deve estar revista no prazo de seis meses e a conclusão de todo o processo deve efetivar-se até Fevereiro de 2013.



Portugal não está isolado nesta preocupação e nesta prioridade. Lembro aqui, para citar só alguns exemplos, que os EUA aprovaram em Dezembro último uma nova estratégia nacional sobre cibersegurança e que o Reino Unido fez o mesmo em Novembro de 2011.

O Governo está aberto às oportunidades do ciberespaço mas não despreza nem ignora os riscos associados. Não desconhecemos que garantir um ciberespaço seguro fomenta o desenvolvimento económico e cria fatores de diferenciação positiva para os nossos agentes económicos.

Estamos ainda conscientes de que, também neste domínio, poderemos ser mais eficientes e eficazes e, mais importante, estamos decididos a sê-lo.

Obrigado.