Universidade da Beira Interior
Faculdade de Engenharia
Departamento de Informática

Segurança Informática
Aula 1.5
Licenciatura em Engenharia Informática
Licenciatura em Informática Web
Licenciatura em Tecnologias e Sistemas da Informação

Computer Security
Lecture 1.5
Degree in Computer Science and Engineering
Degree in Web Informatics
Degree in Information Technologies and Systems

Sumário
Lei Portuguesa sobre o Cibercrime e Centro Nacional de Cibersegurança.

Summary
Portuguese Cybercrime Law and National Center for Cybersecurity.

1 Introdução
Introduction

Contrariamente ao que, por vezes, possa ser **imaginado**, a legislação portuguesa contempla o cibercrime na Lei n.º 109/2009 de 15 de Setembro. Esta lei, conhecida como a **Lei do Cibercrime**, entrou em vigor no dia 15 de Outubro de 2009. O conjunto de leis que regulam o crime informático, ou em sistemas informáticos, ou relacionados com informação e informática, é naturalmente mais vasto e, se a curiosidade for móbil suficiente, é possível encontrar informação mais completa no site da **Comissão Nacional de Proteção de Dado**s – Secção *criminalidade informática*, a que esta designação liga diretamente.
Atualmente, e também por força europeia, encontra-se estabelecido um **Centro Nacional de Cibersegurança**, determinado no Decreto Lei n.º 69/2014 de 09 de Maio, cuja principal missão é a de **contribuir para que Portugal use o ciberespaço de uma forma segura**. A Lei e o Decreto Lei antes enunciados são tema parcial desta aula.

2 Lei n.º 109/2009 de 15 de Setembro
Law number 109/2009, September 15

2.1 Sumário
Summary

[A Lei n.º 109/2009 de 15 de Setembro] **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 **adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa**.

⋮

2.2 CAPÍTULO I – Objeto e definições
CHAPTER I – Subject and definitions

Artigo 1.º – Objecto
A presente lei **estabelece 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**, (...), relativa a ataques contra sistemas de informação, e **adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa**.

Orientações do Ministério Público (MP)

1. Cfr. Despacho n.º 14115/2013 da PGR in D.R. n.º 213, Série II de 2013-11-04
   Atribuição de **competência ao Departamento Central de Investigação e Ação Penal (DCIAP)** para iniciar, exercer e dirigir a ação penal relativamente a **crimes sexuais praticados contra menores com recurso aos meios informáticos** ou divulgados através destes, cuja notícia de crime seja adquirida através de comunicações provindas de outro Estado e organizações internacionais.

⋮

Artigo 2.º – Definições
Para efeitos da presente lei, considera-se:

a) **<<Sistema informático>>, qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção;**

b) **<<Dados informáticos>>, 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;

c) **<<Dados de tráfego>>**, 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;

d) **<<Fornecedor de serviço>>**, qualquer entidade, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, bem como qualquer outra entidade que trate ou armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviço ou dos respectivos utilizadores;

e) **<<Intercepção>>**, o acto destinado a captar informações contidas num sistema informático, através de dispositivos electromagnéticos, acústicos, mecânicos ou outros;

⋮

2.3 CAPÍTULO II – Disposições penais materiais
CHAPTER II – Material penal provisions

Artigo 3.º – Falsidade informática

1. Quem, **com intenção** de provocar engano nas relações jurídicas, **introduzir, modificar, apagar ou suprimir dados informáticos** ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com **pena de prisão até 5 anos ou multa de 120 a 600 dias**.

2. Quando as acções descritas no número anterior incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, a pena é de 1 a 5 anos de prisão.

3. Quem, actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar documento produzido a partir de dados informáticos que foram objecto dos actos referidos no n.º 1 ou cartão ou outro dispositivo no qual se encontrem registados ou incorporados os dados objecto dos actos referidos no número anterior, é punido com as penas previstas num e noutro número, respectivamente.

4. Quem importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das acções prevista no n.º 2, é punido com pena de prisão de 1 a 5 anos.

5. Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de 2 a 5 anos.

1 - Jurisprudência

1. Ac. TRP de 24-04-2013 , sumário retirado da CJ, 2013, T2, pág.223: I. **Comete o crime de falsidade informática aquele que cria informaticamente contas**, nas quais produz dados de perfil não genuínos de outra pessoa, através da ultilização dos seus dados pessoais que, simulando ser a própria, introduz no sistema informático, para criar, via internet, um sítio próprio da plataforma da rede social **facebook**, imagem psicológica, carácter, personalidade e identidade daquela pessoa, que não correspondem'á realidade, com intenção de serem considerados genuínos; e, através daquelas contas, fingindo ser tal pessoa, divulgar conteúdos íntimos da sua vida pessoal, provocando dessa forma engano, com intenção de que fossem tomadas por verdeiras e reais, aquelas contas, dessa forma causando prejuízo á honra e imagem de tal pessoa, como era seu desiderato.

II. Neste crime, **o prejuízo não tem de ser patrimonial**, pois o bem jurídico que nele se protege não é o património, mas a confidencialidade, integridade e disponibilidade de sistemas informáticos, das redes e dados informáticos.

Artigo 4.º – Dano relativo a programas ou outros dados informáticos

1. Quem, **sem permissão legal** ou **sem** para tanto **estar autorizado pelo proprietário**, por outro titular do direito do sistema ou de parte dele, **apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos** alheios ou por qualquer forma lhes afectar a capacidade de uso, é punido com **pena de prisão até 3 anos ou pena de multa**.

2. **A tentativa é punível**.

3. Incorre na mesma pena do n.º 1 quem **ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos** destinados a produzir as acções não autorizadas descritas nesse número.

4. Se o dano causado for de valor elevado (mais do que 50 Unidades de Conta (UC)[1]), a pena é de prisão até 5 anos ou de multa até 600 dias.

[1] A UC é fixada. Normalmente vale 1/4 da remuneração mínima mensal mais elevada, garantida no momento da condenação.

5. Se o dano causado for de valor consideravelmente elevado (maior que 200 UCs), a **pena é de prisão de 1 a 10 anos**.

6. Nos casos previstos nos n.os 1, 2 e 4 o procedimento penal depende de queixa.

Artigo 5.º – Sabotagem informática

1. Quem, **sem permissão legal** ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, **entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático**, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, é punido com **pena de prisão até 5 anos ou com pena de multa até 600 dias**.

2. Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior.

⋮

5. A pena é de prisão de **1 a 10 anos** se:

   a) **O dano** emergente da perturbação for de **valor consideravelmente elevado**;

   b) A perturbação causada atingir de **forma grave ou duradoura um sistema informático** que apoie uma actividade destinada a assegurar funções sociais críticas, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos.

Artigo 6.º – Acesso ilegítimo

1. Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo **aceder a um sistema informático**, é punido com **pena de prisão até 1 ano** ou com pena de multa até 120 dias.

⋮

Artigo 7.º – Intercepção ilegítima

1. Quem, **sem permissão legal** ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, e através de meios técnicos, **interceptar transmissões de dados informáticos** que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes, é punido com **pena de prisão até 3 anos** ou com pena de multa.

2. A tentativa é punível.

3. (...)

Artigo 8.º – Reprodução ilegítima de programa protegido

1. Quem ilegitimamente **reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei** é punido com pena de **prisão até 3 anos** ou com pena de multa.

⋮

Artigo 9.º – Responsabilidade penal das pessoas colectivas e entidades equiparadas

As **pessoas colectivas e entidades equiparadas são penalmente responsáveis** pelos crimes previstos na presente lei nos termos e limites do regime de responsabilização previsto no Código Penal.

Artigo 10.º – Perda de bens

1. O tribunal **pode decretar a perda a favor do Estado dos objectos, materiais, equipamentos ou dispositivos** que tiverem servido para a prática dos crimes previstos na presente lei e pertencerem a pessoa que tenha sido condenada pela sua prática.

2. (...)

2.4 CAPÍTULO III – Disposições processuais

CHAPTER III – Procedural provisions

⋮

Artigo 12.º – Preservação expedita de dados

1. Se no decurso do processo **for necessário à produção de prova**, tendo em vista a descoberta da verdade, obter dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego, em relação aos quais haja receio de que possam perder-se, alterar-se ou deixar de estar disponíveis, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que **preserve os dados em causa**.
2. A preservação pode **também ser ordenada pelo órgão de polícia criminal** mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo aquele, neste último caso, dar notícia imediata do facto à autoridade judiciária e transmitir-lhe o relatório previsto no artigo 253.º do Código de Processo Penal.
3. A ordem de preservação discrimina, sob pena de nulidade:
   a) A natureza dos dados;
   b) A sua origem e destino, se forem conhecidos; e
   c) O período de tempo pelo qual deverão ser preservados, até um máximo de três meses.
4. Em cumprimento de ordem de preservação que lhe seja dirigida, quem tenha disponibilidade ou controlo sobre esses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa, **protegendo e**

conservando a sua integridade pelo tempo fixado, de modo a permitir à autoridade judiciária competente a sua obtenção, e fica obrigado a assegurar a confidencialidade da aplicação da medida processual.

⋮

Artigo 14.º – Injunção para apresentação ou concessão do acesso a dados

1. Se no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de **punição por desobediência**.
2. (...)
3. Em cumprimento da ordem descrita nos n.os 1 e 2, quem tenha disponibilidade ou controlo desses dados comunica esses dados à autoridade judiciária competente ou permite, sob pena de punição por desobediência, o **acesso ao sistema informático onde os mesmos estão armazenados**.

6. **Não pode igualmente fazer-se uso da injunção prevista neste artigo quanto a sistemas informáticos utilizados para o exercício da advocacia, das actividades médica e bancária e da profissão de jornalista**.
7. (...)

Jurisprudência

1. Ac. TRL de 19-06-2014 :
   I. estando apenas em causa a obtenção da identificação de um utilizador de um endereço IP ou o número de IP usado por um determinado indivíduo, em circunstâncias temporais determinadas, a competência para a respectiva obtenção é do MP
   II. **a identificação de um determinado endereço de IP conjugada com a identidade de quem o utilizou num dado dia e hora não revela informação sobre o percurso da comunicação nem sobre outro eventual tráfego comunicacional** da pessoa em causa
   III. **os direitos constitucionais dos arguidos não são absolutos, face aos direitos dos restantes cidadãos**, mormente das vítimas em processo penal, e as entidades públicas, ao enquadrar o uso dos diversos meios de prova têm de considerar os direitos dos vários intervenientes processuais

Artigo 15.º – Pesquisa de dados informáticos

1. Quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se **proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência**.
2. O despacho previsto no número anterior tem um p**razo de validade máximo de 30 dias, sob pena de nulidade**.
3. O órgão de polícia criminal **pode proceder à pesquisa, sem prévia autorização da autoridade judiciária**, quando:
   (a) A mesma for **voluntariamente consentida** por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado;
   (b) Nos casos de **terrorismo**, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa.

⋮

Artigo 16.º – Apreensão de dados informáticos

1. Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem **encontrados dados ou documentos informáticos necessários à produção de prova**, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho **a apreensão** dos mesmos.
2. O órgão de polícia criminal **pode efectuar apreensões, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo anterior, bem como** quando haja urgência ou perigo na demora.
3. Caso sejam apreendidos dados ou documentos informáticos cujo c**onteúdo seja susceptível de revelar dados pessoais ou íntimos**, que possam pôr em causa a privacidade do respectivo titular ou de terceiro, sob pena de nulidade esses dados ou documentos são apresentados **ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto**.
4. As **apreensões efectuadas por órgão de polícia criminal são sempre sujeitas a validação pela autoridade judiciária**, no prazo máximo de 72 horas.

⋮

8. No caso da apreensão efectuada nos termos da alínea b) do número anterior, **a cópia é efectuada em duplicado**, sendo uma das cópias selada e confiada ao secretário judicial dos serviços onde o processo correr os seus termos e, se tal for tecnicamente possível, **os dados apreendidos são certificados por meio de assinatura digital**.

Artigo 17.º – Apreensão de correio electrónico e registos de comunicações de natureza semelhante
Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, **o juiz pode autorizar ou ordenar**, por despacho, **a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova**, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.

Artigo 18.º – Intercepção de comunicações

1. **É admissível o recurso à intercepção de comunicações em processos relativos a** crimes:

   a) **Previstos na presente lei**; ou

   b) **Cometidos por meio de um sistema informático** ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, quando tais crimes se encontrem previstos no artigo 187.º do Código de Processo Penal.

⋮

Artigo 19.º – Acções encobertas

1. É admissível o recurso às acções encobertas previstas na Lei n.º 101/2001, de 25 de Agosto, nos termos aí previstos, no decurso de inquérito relativo aos seguintes crimes:

   a) Os previstos na presente lei;

   b) Os cometidos por meio de um sistema informático, quando lhes corresponda, em abstracto, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os **crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infracções económico-financeiras, bem como os crimes consagrados no título iv do Código do Direito de Autor e dos Direitos Conexos.**

2. (...)

2.5 CAPÍTULO IV – Cooperação Internacional
CHAPTER IV – International cooperation

Artigo 20.º – Âmbito da cooperação internacional
As autoridades nacionais competentes **cooperam** 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 n.º 67/98, de 26 de Outubro.

Artigo 21.º – Ponto de contacto permanente para a cooperação internacional

1. Para fins de cooperação internacional, tendo em vista a prestação de assistência imediata para os efeitos referidos no artigo anterior, a **Polícia Judiciária** assegura a manutenção de uma estrutura que garante um ponto de contacto disponível em permanência, **vinte e quatro horas por dia, sete dias por semana**.

⋮

Artigo 22.º – Preservação e revelação expeditas de dados informáticos em cooperação internacional

1. **Pode ser solicitada a Portugal a preservação expedita de dados informáticos** armazenados em sistema informático aqui localizado, relativos a crimes previstos no artigo 11.º, com vista à apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos mesmos.

2. (...)

3. Em execução de solicitação de autoridade estrangeira competente nos termos dos números anteriores, a autoridade judiciária competente **ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que os preserve.**

4. A ordem de preservação especifica, sob pena de nulidade:

   a) A natureza dos dados;

   b) Se forem conhecidos, a origem e o destino dos mesmos; e

   c) O período de tempo pelo qual os dados devem ser preservados, **até um máximo de três meses.**

5. Em cumprimento de ordem de preservação que lhe seja dirigida, quem tem disponibilidade ou controlo desses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa pelo período de tempo especificado, **protegendo e conservando a sua integridade**.

6. A autoridade judiciária competente, ou a Polícia Judiciária mediante autorização daquela autoridade, podem ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea c) do n.º 5, desde que se verifiquem os respectivos requisitos de admissibilidade, **até ao limite máximo de um ano**.

⋮

Artigo 23.º – Motivos de recusa

1. A **solicitação de preservação ou revelação** expeditas **de dados informáticos é recusada** quando:
   a) Os dados informáticos em causa **respeitarem a infracção de natureza política** ou infracção conexa segundo as concepções do direito português;
   b) **Atentar contra a soberania, segurança, ordem pública ou outros interesses da República Portuguesa**, constitucionalmente definidos;
   c) O **Estado terceiro requisitante não oferecer garantias** adequadas de protecção dos dados pessoais.
2. (...)

Artigo 24.º – Acesso a dados informáticos em cooperação internacional

1. Em execução de pedido de autoridade estrangeira competente, a autoridade judiciária competente **pode proceder à pesquisa, apreensão e divulgação de dados informáticos armazenados em sistema informático localizado em Portugal**, relativos a crimes previstos no artigo 11.º, quando se trata de situação em que a pesquisa e apreensão são admissíveis em caso nacional semelhante.

⋮

Artigo 25.º – Acesso transfronteiriço a dados informáticos armazenados quando publicamente disponíveis ou com consentimento
As **autoridades estrangeiras** competentes, **sem necessidade de pedido prévio** às autoridades portuguesas, de acordo com as normas sobre transferência de dados pessoais previstas na Lei n.º 67/98, de 26 de Outubro, podem:

a) **Aceder a dados informáticos armazenados em sistema informático localizado em Portugal, quando publicamente disponíveis**;
b) Receber ou aceder, através de sistema informático localizado no seu território, a **dados informáticos armazenados em Portugal, mediante consentimento legal e voluntário de pessoa legalmente autorizada** a divulgá-los.

Artigo 26.º – Intercepção de comunicações em cooperação internacional

1. Em execução de **pedido da autoridade estrangeira competente, pode ser autorizada pelo juiz a intercepção de transmissões** de dados informáticos realizadas por via de um sistema informático localizado em Portugal, desde que tal esteja previsto em acordo, tratado ou convenção internacional e se trate de situação em que tal intercepção seja admissível, nos termos do artigo 18.º, em caso nacional semelhante.
2. É competente para a recepção dos pedidos de intercepção a Polícia Judiciária, que os apresentará ao Ministério Público, para que os apresente ao juiz de instrução criminal da comarca de Lisboa para autorização.

⋮

2.6 CAPÍTULO V – Disposições finais e transitórias
CHAPTER V – Final and transitory provisions

Artigo 27.º – Aplicação no espaço da lei penal portuguesa e competência dos tribunais portugueses

1. Para além do disposto no Código Penal em matéria de aplicação no espaço da lei penal portuguesa, e salvo tratado ou convenção internacional em contrário, para efeitos da presente lei, a lei penal portuguesa é ainda aplicável a factos:
   a) **Praticados por Portugueses**, se aos mesmos não for aplicável a lei penal de nenhum outro Estado;
   b) Cometidos em benefício de pessoas colectivas com sede em território português;
   c) Fisicamente praticados em território português, ainda que visem sistemas informáticos localizados fora desse território; ou
   d) Que visem sistemas informáticos localizados em território português, independentemente do local onde esses factos forem fisicamente praticados.
2. Se, em função da aplicabilidade da lei penal portuguesa, forem **simultaneamente competentes** para conhecer de um dos crimes previstos na presente lei **os tribunais portugueses e os tribunais de outro Estado membro da União Europeia**, **podendo em qualquer um deles ser validamente instaurado ou prosseguido o procedimento penal** com base nos mesmos factos, a autoridade judiciária competente recorre 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.
3. **A decisão de aceitação ou transmissão do procedimento** é tomada pela autoridade judiciária competente, tendo em conta, sucessivamente, os seguintes elementos:
   a) **O local onde foi praticada a infracção;**
   b) A **nacionalidade** do autor dos factos; e
   c) **O local onde o autor dos factos foi encontrado.**

⋮

Artigo 29.º – Competência da Polícia Judiciária para a cooperação internacional
A competência atribuída pela presente lei à **Polícia Judiciária**

para efeitos de cooperação internacional é desempenhada pela unidade orgânica a quem se encontra cometida a investigação dos crimes previstos na presente lei.

Artigo 32.º – Entrada em vigor
A presente lei entra em vigor 30 dias após a sua publicação.
Aprovada em 23 de Julho de 2009.
O Presidente da Assembleia da República, Jaime Gama.
Promulgada em 29 de Agosto de 2009.
Publique-se.
O Presidente da República, **Aníbal Cavaco Silva**.
Referendada em 31 de Agosto de 2009.
O Primeiro-Ministro, **José Sócrates Carvalho Pinto de Sousa**.

Diversos
Entrou em vigor em 15.09.2009.

3 Decreto Lei n.º 69/2014 de 09 de Maio

Law Number 69/2014, May 9

3.1 Sumário

Summary

[O Decreto Lei n.º 69/2014 de 09 de Maio] Procede à segunda alteração ao Decreto-Lei n.º 3/2012, de 16 de janeiro, que **aprova a orgânica do Gabinete Nacional de Segurança** (GNS), estabelecendo os termos do **funcionamento do Centro Nacional de Cibersegurança** (CNCSeg) (...) [conforme] apresentado pelo Grupo de Projeto para as Tecnologias de Informação e Comunicação (GPTIC).

Posteriormente, (...) constituiu, na dependência do Primeiro-Ministro, a **Comissão Instaladora do CNCSeg**, com a missão de definir as medidas e os instrumentos necessários à criação, instalação e operacionalização do CNCSeg. O relatório final da mencionada Comissão Instaladora apontou para que **o CNCSeg fosse um novo serviço central da administração direta do Estado, dotado de autonomia administrativa**, a funcionar na dependência do Primeiro-Ministro. Como o Programa (...), o atual contexto económico e financeiro do País e o disposto na Lei n.º 83-C/2013, de 31 de dezembro, **desaconselham a criação de novos serviços públicos**, considera-se que **o aproveitamento das sinergias de um serviço já existente**, especialmente em matéria de instalações e equipamentos, constitui a solução mais adequada (...), [e] **entende-se que o GNS é o serviço indicado para albergar o CNCSeg** na fase inicial do seu funcionamento (...).

O CNCSeg **tem por missão contribuir para que Portugal use o ciberespaço de uma forma segura** e as suas competências não prejudicam as atribuições e competências legalmente cometidas a outras entidades públicas em matéria de segurança do ciberespaço, nomeadamente no que respeita a infraestruturas críticas e integridade das redes e serviços, sendo exercidas em coordenação com estas entidades.

3.2 Artigos

Articles

⋮

Artigo 2.º [– Alterações ao Decreto-Lei n.º 3/2012]
Os artigos 2.º, 3.º, 4.º, 7.º do Decreto-Lei n.º 3/2012, de 16 de janeiro, alterado pelo Decreto-Lei n.º 162/2013, de 4 de dezembro, passam a ter a seguinte redação:

⋮

2 - No âmbito do GNS funciona o Centro Nacional de Cibersegurança, doravante designado por CNCSeg, que **tem por missão contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais**.

Artigo 3.º [– Aditamentos]
São aditados ao Decreto-Lei n.º 3/2012, de 16 de janeiro, alterado pelo Decreto-Lei n.º 162/2013, de 4 de dezembro, os artigos 2.º-A, 6.º-A e 12.º-A, com a seguinte redação:
Artigo 2.º-A
Competências do Centro Nacional de Cibergurança

1- Na prossecução da sua missão, o CNCSeg possui as seguintes **competências**:

a) **Desenvolver as capacidades nacionais de prevenção, monitorização, deteção, reação, análise e correção** destinadas a fazer face a incidentes de cibersegurança e ciberataques;
b) **Promover a formação e a qualificação de recursos humanos** na área da cibersegurança, com vista à formação de uma comunidade de conhecimento e de uma cultura nacional de cibersegurança;
c) **Exercer os poderes de autoridade nacional competente em matéria de cibersegurança**, relativamente ao Estado e aos operadores de infraestruturas críticas nacionais;
d) **Contribuir para assegurar a segurança dos sistemas de informação e comunicação** do Estado e das infraestruturas críticas nacionais;
e) Promover e **assegurar a articulação e a cooperação** entre os vários intervenientes e responsáveis nacionais na área da cibersegurança;
f) Assegurar a **produção de referenciais normativos** em matéria de cibersegurança;
g) Apoiar o **desenvolvimento das capacidades técnicas, científicas e industriais**, promovendo projetos de inovação e desenvolvimento na área da cibersegurança;

h) Assegurar o planeamento da **utilização do ciberespaço em situação de crise e de guerra** no âmbito do planeamento civil de emergência, no quadro definido pelo Decreto-Lei n.º 73/2013, de 31 de maio;

i) **Coordenar a cooperação internacional** em matérias da cibersegurança, em articulação com o Ministério dos Negócios Estrangeiros;

j) (...)

2- O disposto no número anterior **não prejudica as atribuições e competências legalmente cometidas a outras entidades públicas** em matéria de segurança do ciberespaço (...)

3- O CNCSeg a**tua ainda em articulação e estreita cooperação** com as estruturas nacionais responsáveis pela ciberespionagem, ciberdefesa, cibercrime e ciberterrorismo, **devendo comunicar à Polícia Judiciária**, no mais curto prazo, os factos de que tenha conhecimento relativos à preparação e execução de crimes.

⋮

Artigo 5.º – Avaliação de Funcionamento
O funcionamento do Centro Nacional de Cibersegurança no âmbito do Gabinete Nacional de Segurança **é objeto de avaliação no final do ano 2017**.

Artigo 7.º – Entrada em Vigor
Visto e aprovado em Conselho de Ministros de **10 de abril de 2014**. - **Pedro Passos Coelho** - Maria Luís Casanova Morgado Dias de Albuquerque - Rui Manuel Parente Chancerelle de Machete - Berta Maria Correia de Almeida de Melo Cabral - Miguel Bento Martins Costa Macedo e Silva. **Promulgado em 5 de maio de 2014.**
O Presidente da República, **Aníbal Cavaco Silva**.
Referendado em 8 de maio de 2014.
O Primeiro-Ministro, **Pedro Passos Coelho**.

3.3 Anexo II — Artigo 1º – Natureza

Annex II – 1st. Article – Nature

1. O **Gabinete Nacional de Segurança**, abreviadamente designado por GNS, é **um serviço central da administração direta do Estado, dotado de autonomia administrativa**, na dependência do Primeiro-Ministro ou do membro do Governo em quem aquele delegar.

2. A **Autoridade Nacional de Segurança**, abreviadamente designada por ANS, **dirige o GNS** e é a entidade que exerce, em exclusivo, a proteção e a salvaguarda da informação classificada.

3.4 Anexo II — Artigo 2º – Missão e Atribuições

Annex II – 2nd. Article – Mission and Responsabilities

1 - O GNS **tem por missão garantir a segurança da informação classificada no âmbito nacional e das organizações internacionais de que Portugal é parte** e exercer a função de **autoridade de credenciação de pessoas e empresas** para o acesso e manuseamento de informação classificada, bem como a de autoridade **credenciadora e de fiscalização de entidades** que atuem no âmbito do Sistema de Certificação Eletrónica do Estado - **Infraestrutura de Chaves Públicas** (SCEE).

2 - **No âmbito do GNS funciona o Centro Nacional de Cibersegurança** (...)

3 - O GNS prossegue as seguintes atribuições:

a) **Garantir a articulação e a harmonização dos procedimentos relativos à segurança da informação classificada** em todos os serviços, organismos e entidades, públicos ou privados, onde seja administrada tal informação, designadamente e em especial, os da **Administração Pública, das forças armadas e das forças e serviços de segurança**, bem como no âmbito das organizações, reuniões, programas, contratos, projetos e outras atividades internacionais em que Portugal participe;

b) **Assegurar** (...) **a proteção e a salvaguarda da informação classificada emanada das organizações internacionais de que Portugal faça parte** ou das respetivas estruturas internas, nomeadamente no âmbito da **Organização do Tratado do Atlântico Norte (OTAN), da União Europeia (UE), Unidade Europeia de Cooperação Judiciária (EUROJUST) e da Agência Espacial Europeia (AEE)**, (...) [etc.];

c) Exercer em Portugal os poderes públicos cometidos às autoridades nacionais de segurança, nomeadamente nas áreas da credenciação de segurança, segurança das comunicações, distribuição e outras, nos termos das normas aprovadas pelas entidades internacionais competentes;

d) **Proceder ao registo, distribuição e controlo da informação classificada** (...)

e) **Fiscalizar e inspecionar os órgãos de segurança** que detenham, a qualquer título e em qualquer suporte, informação classificada sob responsabilidade portuguesa, dentro e fora do território nacional;

f) **Avaliar, acreditar e certificar a segurança de produtos e sistemas de comunicações, de informática e de tecnologias de informação que sirvam de suporte ao tratamento, arquivo e transmissão de informação classificada e proceder à realização de limpezas eletrónicas**;

g) **Promover o estudo, a investigação e a difusão das normas e procedimentos** de segurança aplicáveis à proteção e salvaguarda da informação classificada, propondo a doutrina a adotar por Portugal e a formação de pessoal especializado nesta área da segurança;

h) **Credenciar as empresas** que pretendam exercer as atividades de comércio e indústria de bens e tecnologias militares, nos termos da Lei n.º 49/2009, de 5 de agosto;

i) **Credenciar entidades públicas e privadas** para o exercício de atividades industriais, tecnológicas e de investigação, quando tal seja exigido por disposição legal ou regulamentar;

j) Exercer as competências de autoridade credenciadora e de fiscalização de entidades que atuem no âmbito do SCEE, bem como no quadro do regime jurídico dos **documentos eletrónicos e da assinatura eletrónica**;

k) (...)

⋮

Nota: o conteúdo exposto na aula e aqui contido não é (nem deve ser considerado) suficiente para total entendimento do conteúdo programático desta unidade curricular e deve ser complementado com algum empenho e investigação pessoal.