VII REVISÃO CONSTITUCIONAL [2005]

TÍTULO II

Direitos, liberdades e garantias

CAPÍTULO I

Direitos, liberdades e garantias pessoais

[**Artigo 35o Constituição**](#_sxs1bdup2m0h) **2**

[Artigo 35.o no. 1](#_qbq5vzsbg9u8) 2

[Utilização da informática](#_2nrvktcbptq9) 2

[Artigo 35.o no. 2](#_4owpk3seatdw) 2

[Artigo 35.o no. 3](#_791k36z7zifj) 2

[Artigo 35.o no. 4](#_nb3rficif9ez) 2

[Artigo 35.o no. 5](#_65zymf791p21) 2

[Artigo 35.o no. 6](#_4j6lvewnalh0) 2

[Artigo 35.o no. 7](#_md1j11ldotya) 2

[**Módulo II - Cibercrime**](#_a2o797ul811c) **2**

[Criminalidade Informática](#_3rzukz63kl91) 2

[Responsabilidade criminal](#_ueuadm5k8fzy) 2

[Cibercrime Definição:](#_o1h9b3iarljv) 3

[Cibercrime Características:](#_ho8uudfx5i) 3

[Tipificação:](#_u1dlhihmm6rr) 3

[Cibercrime Legislação Nacional:](#_qx7e2zxkl6e7) 4

[Exemplos de Crimes clássicos](#_evpn1kfgii8z) 4

[Exemplos Novos crimes específicos](#_ekj5ltpvung) 4

[Objectivo Criminoso](#_gpzlvo6gdxl4) 4

[Como?](#_s9u5o4rzvfn3) 4

[Crime de falsidade informática](#_lzvybuf5py0u) 5

[Crime de dano relativo a programas ou outros dados informáticos](#_ih2yyxjo05ip) 5

[Crime de Sabotagem Informática](#_k7e37f5jool4) 5

[Crime de reprodução ilegítima de programa protegido](#_2d97g07x66m) 7

[Exemplo de vários crimes de 1 x só](#_llcq5cfg3e2v) 7

[Crime de devassa por meio de informática](#_pvmup1pd7rg9) 8

[Crime de burla informática e nas comunicações](#_130x1f36p55x) 8

[Principais métodos de ataque Engenharia Social](#_848lt0c6hq4g) 9

[Principais métodos de ataque Engenharia Social](#_4rk49rtbv28z) 9

# Artigo 35o Constituição

## Artigo 35.o no. 1

### Utilização da informática

Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.

### Artigo 35.o no. 2

A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente.

### Artigo 35.o no. 3

A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas,

filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.

### Artigo 35.o no. 4

É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei.

### Artigo 35.o no. 5

É proibida a atribuição de um número nacional único aos cidadãos.

### Artigo 35.o no. 6

A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.

### Artigo 35.o no. 7

Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei.

# Módulo II - Cibercrime

## Criminalidade Informática

### Responsabilidade criminal

* Tipificação
* Ilicitude
* Imputação / Causalidade
* Intenção / Culpa
* Punibilidade

### Cibercrime Definição:

* Recorre a tecnologias de informação e comunicação
* Dirigido contra tecnologias de informação e comunicação
* E ainda pode usar tecnologias de informação e comunicação
* para a prática de outros crimes
* Todos os crimes praticados com recurso a meios informáticos

### Cibercrime Características:

* Afetam gravemente a economia nacional
* Facilitam direta ou indiretamente outras atividades criminosas
* Apresentam dificuldades de recolha de prova - Principio da Territorialidade
* Relevância da localização: onde os dados estão armazenados e como acedemos?

#### Tipificação:

* Crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos
* Acesso ilegítimo
* Interceção ilegítima
* Sabotagem informática
* Devassa por meio de Informática
* Crimes relacionados com sistemas informáticos
* Falsidade informática
* Burla informática
* Burla nas telecomunicações
* Crimes relacionados com o conteúdo
  + Difusão de pornografia infantil
  + Falsidade informática
* Crimes praticados contra os direitos de autor e direitos conexos
  + Cópia/Reprodução ilícita/Pirata de
  + Programas/filmes/musica/obras literárias

### 

### Cibercrime Legislação Nacional:

* Lei 109/09, 15/09 –Lei do Cibercrime
* Código Penal
* Lei 67/98, 26/10 –Proteção dos Dados Pessoais
* Lei 12/05, 26/01 –Dados pessoais na Saúde
* DLei252/94, 20/10 –Proteção de Software
* Dlei63/85, 14/03 (L82/13, 6/12) –Cód. Direitos Autor e Direitos Conexos
* Lei 41/04, 18/08 –Lei Proteção Dados Pessoais nas Telecomunicações
* Lei 32/08, 17/07 –Dados de Tráfego
* Dlei7/04, 7/01 –at.o 22 “Comunicações não solicitadas”
* Dlei63/09, 10/03 ( Lei 177/99, 21/05), -Audiotexto
* Dlei290-D/99, 02/08 (Dlei88/09, 9/04)–Assinatura Digital
* Dlei143/01, 06/04, ( Dlei57/08, Dlei82/08, Dlei317/09 e Dlei24/14, 14/02) –Fraudecom cartão de crédito
* Lei 5/04, 10/02 (Lei 35/08, 28/07), Lei das Comunicações Eletrónicas

### Exemplos de Crimes clássicos

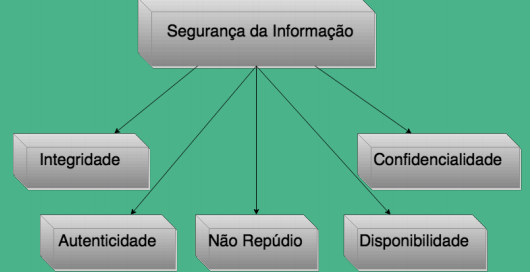
* Burlas, ameaças, injúrias e difamações

### Exemplos Novos crimes específicos

* Obtenção fraudulenta da identidade digital
* Ataques contra a segurança, confidencialidade e fiabilidade dos sistemas

### Objectivo Criminoso

Objetivo direto do “criminoso” é atingir o seu objetivo atacando um ou mais elementos dos 5 pilares da segurança informática



#### Como?

* **Revelação da informação** – Em casos de espionagem coletiva (NSA Prism);
* **Fraude** – Não reconhecimento da origem da informação, alteração da informação;
* **Interrupção** – Constrangimento na informação e modificações da informação;
* **Usurpação** – Modificação da informação e negação de serviço;
* **Modificação** – Alteração da mensagem em trânsito;
* **Repetição** – Repetição de operações já realizadas, sem autorização, de modo a obter o mesmo resultado;
* **Disfarce** – Apresentação de identidades falsas perante um determinado interlocutor;
* **Negação de serviço** – Ações que visam dificultar o normal funcionamento de um sistema;
* **Interceção** – Acesso não autorizado a uma mensagem, que, contudo, não é passível de ser alterada;
* **Repúdio** – Negação de participação numa determinada comunicação ou operação,

**Resumo:**

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.**

### Crime de falsidade informática

* Crime de falsificação no mundo digital
  + Falsificação de cartões
  + cartões bancários de pagamento (débito / crédito)
  + cartões acesso a sistemas de comunicações (SIM)
  + cartões de acesso a serviços condicionados (cartões ou box de televisão por cabo)
* Difusão de dispositivos para praticar estes crimes

### Crime de dano relativo a programas ou outros dados informáticos

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.

A tentativa é punível.

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.

### Crime de Sabotagem Informática

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.

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

Nos casos previstos no número anterior, a tentativa não é punível.

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

• O dano emergente da perturbação for de valor elevado /consideravelmente elevado;

• 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.

Crime de Acesso ilegítimo

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.

Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as acções não autorizadas

descritas no número anterior.

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:

• a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou

• b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.

• A tentativa é punível, salvo nos casos previstos no n.º 2.

• Nos casos previstos nos nos 1, 3 e 5 o procedimento penal depende de queixa.

Violação de confidencialidade de sistemas informáticos, acedendo sem autorização, Intrusão, hacking, break-in

• Difusão de dispositivos para praticar estes crimes (ex. roubo de identidade, senhas passwords de acesso vendas de dump’s)

Ac. Trib. Relação de Coimbra, de 17 de fevereiro de 2016: -

Comete o crime de acesso ilegítimo (Artigo 6º, nºs 1 e 4, al a, da Lei nº 109/2009), o inspetor tributário que, por motivos estritamente pessoais, acede ao sistema informático da Autoridade Tributária, consultando declarações de IRS de outrem. O tipo subjetivo daquele ilícito penal não exige qualquer intenção específica (como seja o prejuízo ou a obtenção de benefício ilegítimo), ficando preenchido com o dolo genérico de intenção de aceder a sistema).

Na sua essência, o crime de acesso ilegítimo é um crime em que alguém consegue penetrar – não há que ter dúvida na terminologia, trata-se de um universalmente designado acto de break-in – num sistema informático ou numa rede informática (dependendo das soluções de política legislativa adoptadas pelos diversos ordenamentos jurídicos, os tipos criminais conterão ou não elementos subjectivos específicos, o que permitirá punir ou não as condutas de hacking em sentido estrito).

Crime de Interceção ilegítima

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.

• A tentativa é punível.

• Incorre na mesma pena prevista no 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 no mesmo número.

### Crime de reprodução ilegítima de programa protegido

• 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.

• Na mesma pena incorre quem ilegitimamente reproduzir topografia de um produto semicondutor ou a explorar comercialmente ou importar, para estes fins, uma topografia ou um produto semicondutor fabricado a partir dessa topografia.

• A tentativa é punível.

• Visa exclusivamente programas de computador

• Decreto-Lei nº 252/94

• Não é aplicável à reprodução não autorizada de bases de dados

• Decreto-lei nº 122/2000

A instalação de um único programa informático licenciado em vários computadores traduz-se numa reprodução de programa não autorizada. O tipo de crime de reprodução de programa protegido não exige intenção de lucro.

O tipo de crime de reprodução ilegítima de programa protegido não exige que, cumulativamente, haja reprodução, divulgação e comunicação ao público, bastando-se, por exemplo, com a instalação não autorizada de um programa informático protegido.

### Exemplo de vários crimes de 1 x só

• Em Portugal, como é do conhecimento geral, é prática comum piratear o serviço TV paga. Considerado atualmente como crime, os piratas arriscam uma pena até cinco anos.

• De acordo com o JN, são pelo menos 200 mil os lares em Portugal equipados com sistemas pirata de televisão.

• As perdas para as operadoras variam entre 600 mil e um milhão de euros/mês.

Apesar das operadoras de televisão paga redobrarem a vigilância para travar a pirataria, a verdade é que continua a ser fácil contornar a lei para poder ver a TV de borla, ou quase. O fenómeno chama-se cardsharing e consiste na recepção de sinal de televisão por cabo ou satélite e posterior disponibilização ilegítima a outros utilizadores

(permitindo o acesso das box pirata oficial, para ler as chaves e assim, descodificar o sinal) os quais pagam uma quantia simbólica (comparativamente aos preços praticado pelos operadores).

Quem o faz, no entanto, comete pelo menos quatro crimes puníveis com penas que podem chegar aos cinco anos de cadeia e avultadas multas.

• Crime de Acesso Ilegítimo

• Intercetação ilegítima

• Reprodução ilegítima de programa protegido

• Falsidade informática

### Crime de devassa por meio de informática

Criação, manutenção ou utilização de ficheiro automatizado de dados individualmente identificáveis e referentes a convicções políticas, religiosas ou filosóficas, à filiação partidária ou sindical, à vida privada, ou a origem étnica.

• A pena prevista é de prisão até 2 anos ou multa até 240 dias.

• Em relação aos outros tipos de intromissão na vida privada, este tipo contém agravamentos substanciais:

• Tentativa é punível

• O procedimento criminal não depende de queixa ou participação (art.198º)

• Não se exige nenhum elemento subjectivo de ilicitude

• Este aspecto é reforçado pelo art.35º, 3 da CRP, que exclui o tratamento informático de dados referentes aos mesmos aspectos referidos no art.193º.

• O pirata informático que revelou a nudez da atriz Scarlett Johansson na internet foi condenado, esta terça-feira, a dez anos de prisão. Em Portugal, a ação não ficaria impune, mas a pena não passaria de dois anos.

• Mantinha um sitio na web com informação pessoal categorizada por celebridades, religião entre outros.

Uma proteção para prevenir várias tentativas no uso de uma API de autenticação estava sem limite de 3 tentativas, permitindo que fosse usado um dicionário para tentar chegar à password.

Artigo 139º CP

Esta técnica permite retirar informação catalogada de servidores que podem guardar informação sensível sobre um determinado grupo.

Um exemplo, informação sobre orientação sexual guardada no Ashley Madison

### Crime de burla informática e nas comunicações

Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorrecta de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até três anos ou com pena de multa.

• A mesma pena é aplicável a quem, com intenção de obter para si ou para terceiro um benefício ilegítimo, causar a outrem prejuízo patrimonial, usando programas, dispositivos electrónicos ou outros meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações.

• A tentativa é punível.

• O procedimento criminal depende de queixa.

**Isto significa:**

• Intenção de obter enriquecimento ilegítimo ou causar prejuízo patrimonial

• Interferir no tratamento de dados ou em programa informático

• Uso de programas ou dispositivos eletrónicos para diminuir, alterar ou impedir o normal funcionamento de serviços de telecomunicações

• Técnica pela qual o criminoso finge ser outra pessoa ou instituição

• Utilização de imagens que copiam imagens de instituições legítimas

• Construção de páginas web falsas com uso de imagens de instituições legitimas

### Principais métodos de ataque Engenharia Social

• A engenharia social, no contexto de segurança da informação, refere-se à manipulação psicológica de pessoas para a execução de ações ou divulgar informações confidenciais.

• Este é um termo que descreve um tipo psicotécnico de intrusão que depende fortemente de interação humana e envolve enganar outras pessoas para quebrar procedimentos de segurança

Um ataque clássico na engenharia social é quando uma pessoa se passa por um alto nível profissional dentro das organizações e diz que o mesmo possui problemas urgentes de acesso ao sistema, conseguindo assim o acesso a locais restritos.[1]

#### Principais métodos de ataque Engenharia Social

• O principal de meio de uso é o phishing

• O segundo é envio de email portadores de vírus

• O terceiro é não informático, consistente na observação (sholdersniffing)