FEUP Universidade do Porto
Faculdade de Engenharia

ASPECTOS SOCIAIS DA INFORMÁTICA

CRIMINALIDADE INFORMÁTICA – DESAFIOS DE UMA NOVA GERAÇÃO

17 DE MAIO DE 2006

Trabalho elaborado por: Belmiro Sotto-Mayor (ei01049)
Paulo Ferreira (ei02005)
e André Lessa (ei02017)

Aspectos Sociais da Informática

Criminalidade Informática – Desafios de uma nova Geração

Paulo Ferreira (ei02005)

Aluno do quarto ano do curso de Engenharia Informática e Computação da Faculdade de Engenharia da Universidade do Porto

Belmiro Sotto-Mayor (ei01049)

Aluno do quinto ano do curso de Engenharia Informática e Computação da Faculdade de Engenharia da Universidade do Porto

André Lessa (ei02017)

Aluno do quarto ano do curso de Engenharia Informática e Computação da Faculdade de Engenharia da Universidade do Porto

Trabalho realizado no âmbito da disciplina de Aspectos Sociais da Informática, do 2º semestre, 4º ano, da Licenciatura em Eng. Informática e de Computação da Faculdade de Engenharia da Universidade do Porto, leccionada por Manuel Veiga de Faria.

Faculdade de Engenharia da Universidade do Porto

Rua Roberto Frias, s/n, 4200-465 Porto, Portugal

Maio de 2006

Resumo

Numa altura em que a Informática tem cada vez mais peso, não podemos ir a algum lado sem ver um computador ou algo controlado por um computador, torna-se mais significativo saber lidar com esses novos meios, pois como sabemos a cada avanço tecnológico também correspondem avanços nos métodos de praticar crimes e atentar contra as pessoas.

Por isso vamos analisar ao longo deste documento estes novos crimes que assim aparecem quais as suas consequências, pois não se encaixam na topologia padrão mas representam novos desafios para as nossas forças de segurança.

Índice

INTRODUÇÃO 1

Enquadramento 1

Evolução da Legislação 1

Objectivos 3

Panorama dos crimes informáticos em Portugal 3

Mas porquê que o problema da segurança é assim tão importante na sociedade portuguesa? Será que existem assim tantos "piratas informáticos" em Portugal? 3

Mas afinal qual é o perfil de um criminoso informático? 4

Mas afinal quais são os riscos associados à utilização das novas tecnologias? 5

Mas sendo a Internet global a que legislação estamos vinculados? Que problemas pode criar a Internet em termos legais? 6

CRIMES INFORMÁTICOS 8

Legislação Aplicável 8

BBS 9

Sniffing 11

Hacking 12

Cracking 13

Phreaking 15

Carding 16

Spam 17

Abuso Sexual de Crianças – Pedofilia 18

Uso e Reprodução Ilegítima de Software 19

JURISPRUDÊNCIA EM PORTUGAL NO ÂMBITO DA CRIMINALIDADE INFORMÁTICA 21

MEIOS DE COMBATE À CRIMINALIDADE INFORMÁTICA EM PORTUGAL 24

CONCLUSÃO 25

BIBLIOGRAFIA 26

ANEXOS 27

1.INTRODUÇÃO

1.1.ENQUADRAMENTO

Este documento visa discutir o direito informático incidindo-se sobre a criminalidade informática em Portugal.

Nesse sentido vai ser apresentada as imposições a nível legislativo que irão culminar no direito informático, a evolução da legislação a nível do direito informático, os crimes informáticos previstos na legislação, crimes mais cometidos em Portugal e instrumentos de combate e medida a estes crimes.

1.2.EVOLUÇÃO DA LEGISLAÇÃO

O uso da informática pelas massas, na sociedade portuguesa, foi um fenómeno que surgiu no final do século XX. Com este fenómeno surgiu um vácuo na legislação portuguesa que obviamente têm vindo a ser preenchido desde á 30 anos para trás.

Por volta dos anos 70, a primeira legislação começou a ser desenvolvida. Esta primeira versão incidiu sobre a protecção das vidas privadas na recolha e armazenamento, transferência e inter conexão de dados pessoais, potenciados pela informática.

À medida que a tecnologia progredia, um maior desenvolvimento da legislação era requerido e assim, nos primórdios dos anos 80, esta sofreu uma nova evolução, contendo legislação relativa a combater a delinquência económica específica da informática (delinquência esta que será assunto de capítulos posteriores).

Obviamente com o avançar da década de 80, nova evolução da legislação era requerida. Os direitos de propriedade intelectual e sua salvaguarda necessitavam de ser melhorados, introduzindo-se assim emendas legislativas nesse sentido.

Em Agosto de 1991, foi criada uma nova lei denominada por **Lei da Criminalidade Informática**.

Actualmente a evolução na nossa legislação, em relação ao direito informático, têm sido no direito processual.

Mesmo com esta grande evolução a nível legislativo existe ainda actualmente uma grande deficiência de instrumentos de medida deste tipo de criminalidade. Estima-se que apenas 1% de todos os delitos informáticos praticados são descobertos.

Também existem ainda várias lacunas actualmente na legislação como foi defendido no seminário *"Leis Portuguesas na Sociedade da Informação"* ocorrido no ano passado em Lisboa (6 de Dezembro de 2005).

Uma das lacunas apresentadas foi o caso da descoordenação entre o regime que estabelece a lei e o regime que estabelece a lei que lhe é mais directamente conexa, o Código Penal. Existem, por exemplo, crimes que agora se associam aos computadores, que não estão contemplados na norma legislativa, como é o caso dos crimes referentes à protecção de dados pessoais, os crimes contra o meio informático e os crimes de conteúdo, apontados por Pedro Verdelho.

Para além destas ultimas também foram apresentadas discrepâncias em relação à severidade das penas, às diferenças entre a classificação da natureza dos crimes e a responsabilidade das pessoas colectivas, assim como, "um conjunto de novas actividades criativas" que também não cabem na actual Lei da Criminalidade Informática, e onde se integram o *spam*, a mistificação da interface e a mistificação da identidade, mas também o desbloqueio de telemóveis e, eventualmente, a alteração das caixas de recepção de televisão por cabo.

Uma outra adição à legislação actual tem vindo a ser pedido pela polícia e por muitos juristas, alegando ter grande pertinência ao combate à criminalidade informática, que é a instituição da Prova Digital. Esta engloba a disponibilização de dados de tráfego do sistema, incluindo localização de base e de conteúdo. Isto facilitaria em muito a acção da Policia e daria mais consistência à acusação do Ministério Público. Esta instituição da prova digital ainda está em estudo actualmente e ainda não faz parte da nossa legislação.

A evolução legislativa em termos do direito informático cresceu bastante, mas continua ainda com bastantes lacunas. Obviamente que isto deve-se ao grande avanço tecnológico que esta área têm vindo a sofrer, que faz com que seja praticamente impossível manter a legislação actualizada.

1.3.PANORAMA DOS CRIMES INFORMÁTICOS EM PORTUGAL

Nos dias de hoje o que mais se ouve falar é da segurança dos sistemas de informação e das redes. Os problemas, neste campo sucedem-se e há que encontrar soluções eficazes para resolver essas situações.

1.3.1. MAS PORQUÊ QUE O PROBLEMA DA SEGURANÇA É ASSIM TÃO IMPORTANTE NA SOCIEDADE PORTUGUESA? SERÁ QUE EXISTEM ASSIM TANTOS "PIRATAS INFORMÁTICOS" EM PORTUGAL?

A resposta a estas perguntas vem de um inspector da Polícia Judiciária, João Duque. Segundo ele, este tipo de crime em Portugal têm vindo a crescer a passos largos. Acessos ilegítimos, burlas informáticas e divulgação de imagens de pedofilia são três tipos de crimes que crescem exponencialmente.

Segundo informações divulgadas na imprensa, em 2004 as duas brigadas da Secção de Investigação de Criminalidade Informática e de Telecomunicações da Polícia Judiciária investigaram cerca de 572 casos, contra 338 em 2003 e 230 em 2002. Isto representa um crescimento de cerca de 69 por cento em relação ao ano anterior.

Dos 572 casos, 154 correspondem aos acessos ilegítimos, 148 a burlas informáticas e 70 casos correspondem a pedofilia.

Para além destes últimos três crimes um que têm notado um crescimento relativo é a devassa da vida privada, com 27 casos registados. Estes crimes estão maioritariamente relacionados com utilização abusiva ou difamação de imagem de figuras públicas. Outro crime que também têm tido um crescimento significativo a nível mundial e que foi a pouco tempo bastante denunciado pela média é o ataque de engenharia social conhecido por *phishing.* Por fim outro crime que têm tido um aumento significativo é o crime de cópias ilegais e pirataria de boxes de televisão por cabo com 22 queixas. (obviamente que estas são as percentagens de crimes apreendidos pela policia judiciária, deve-se relembrar o que já foi dito anteriormente que estima-se que apenas 1% dos crimes informáticos são descobertos).

1.3.2.MAS AFINAL QUAL É O PERFIL DE UM CRIMINOSO INFORMÁTICO?

Esta resposta também é fácil de obter podendo-se até ordenar a tipologia dos delinquentes da seguinte maneira:

- **Amadores:** colocados em lugares de confiança (normalmente pessoas com cargos de gestão ou administração em empresas) e com um certo nível de conhecimentos técnicos de informática. Na maioria dos casos cometem o crime por razões financeiras.

- **Perturbados**: desequilibrados psicologicamente, normalmente associados a crimes sexuais (ex: Pedofilia)

- **Espiões**: Pessoas que tentam furar a segurança informática das empresas com o fim de adquirir (furtar) segredos industriais/económicos.

- **Membros do crime organizado:** explorando potenciais ganhos em contrapartida de riscos comparativamente menores;

- ***Hackers*:** utilizando as falhas de procedimentos e de segurança no acesso aos sistemas, agindo com um objectivo mais virado para o simples prazer de entrar nos sistemas, do que com objectivos fraudulentos ou prejudicativos (ex.: estudantes).

E ordenar as suas motivações da seguinte forma:

- **Utilitaristas:** são determinados por ganhos financeiros;

- **Empreendedores:** agem por jogo ou desafio

- **Agressivos:** são guiados pelo propósito de compensar uma frustração ou agravo profissional

- **Destruidores:** a sua intenção é a destruição das empresas ou organizações através da sabotagem ou terrorismo.

Em Portugal o criminoso informático está normalmente compreendido entre 15 a 40 anos. Caso seja estudante, é tido normalmente como introvertido e filho de pais divorciados, frequentando normalmente o ensino superior numa vertente tecnológica, tirando notas medianos e sem antecedentes criminais. No caso de estar já envolvido no mundo de trabalho, são tidos normalmente como bons trabalhadores, sendo bastante dedicados ao seu trabalho sem se importarem em fazer horas extraordinárias.

1.3.2. MAS AFINAL QUAIS SÃO OS RISCOS ASSOCIADOS À UTILIZAÇÃO DAS NOVAS TECNOLOGIAS?

Para um utilizador comum da Internet os riscos de serem vítimas de um crime informático são bastante grandes. Um dos crimes usuais é o que já foi referido em cima o de *phishing*. Um exemplo deste tipo de crime é o utilizador receber um mail que se faz passar por uma qualquer entidade credível (normalmente entidade bancária) com um link para uma pagina web(bastante parecida com a original), pedindo ao utilizador que recebeu o mail para voltar a inserir os seus dados. Se o utilizador "cair" nesta armadilha poderá ver as suas contas bancárias a serem esvaziadas muito rapidamente.

Este tipo de crime normalmente é realizado em conjunto com outro, o spam. O spam é a emissão simultânea de uma mensagem de e-mail para vários utilizadores ao mesmo tempo sem serem solicitadas pelo utilizador, com identificação falsa do remetente e usando a maquina servidora de correio electrónico de uma qualquer vitima.

Qual é o perigo do spam (para além do *phishing*) para o utilizador? Bem imaginemos que o leitor é um utilizador da Internet, vai ver o seu mail e vê uma mensagem de e-mail com um ficheiro lá dentro com o endereço de mail de uma pessoa de confiança sua. Obviamente sendo de sua confiança, provavelmente iria abrir esse ficheiro. E aqui começa o problema do spam, dado que quem lhe enviou o ficheiro estava identificado como um amigo de sua confiança, o mais provável é o ficheiro ser ou um vírus ou um *trojan* ou qualquer outro tipo de código maléfico que poderá desde destruir completamente o seu sistema informático, a dar acesso ao seu computador a um desconhecido ou até mesmo enviando passwords suas pela internet para um desconhecido.

Basicamente os riscos que corremos ao navegar pela Internet de sermos vítimas de um crime, são muito possivelmente maiores daqueles que correrrmos ao passear na rua. O maior problema dos crimes informáticos é que a grande maioria das vezes que se é vítima de um crime não nos apercebemos de nada. Pode mesmo acontecer situações anormais de o leitor por exemplo ter a policia a bater à sua porta a dizer que foi feito um acesso ilegítimo do seu computador pessoal, por exemplo, a um banco. Quando na verdade o que aconteceu foi alguém que se ligou ilegalmente ao seu computador e através dele fez o tal acesso ilegal ao banco.

A legislação informática é importantíssima para que as liberdades, leis e direitos conhecidas na nossa sociedade e vida quotidiana sejam também

cumpridas e aplicadas no mundo virtual. Pois os crimes informáticos mesmo sendo virtuais, podem ter implicações e prejuízos reais bastante sérios.

1.3.2. MAS SENDO A INTERNET GLOBAL A QUE LEGISLAÇÃO ESTAMOS VINCULADOS? QUE PROBLEMAS PODE CRIAR A INTERNET EM TERMOS LEGAIS?

Este é um problema bastante interessante. É verdade que a Internet é global, não têm fronteiras e ninguém é dono dela. Basicamente, á primeira vista é um meio de transmissão de dados completamente anarquista. É praticamente impossível a uma qualquer nação impor qualquer tipo de legislação sobre ela. Imaginemos que três quaisquer países proíbem publicidade a tabaco on-line. Estes só vão poder fiscalizar o cumprimento dessas regras em relação aos servidores e utilizadores que se encontram fisicamente no seu pais. Quaisquer outros utilizadores/servidores que não se encontrem fisicamente dentro das fronteiras destes países podem colocar publicidade a tabaco disponível a toda a gente. A rede passa fronteiras e um estado é apenas soberano para legislar apenas no seu território. O local onde ocorre o crime acontece apenas no espaço em que essa acção realmente seja considerada um delito.

Isto realmente é um problema grande, mas é de possível resolução. Para isso "bastam acordos" internacionais e uma estandardização das legislações a nível global em certos aspectos (obviamente que quando é dito "bastam acordos" não sequer dar a ideia que este tipo de acção seja fácil…antes pelo contrário, este tipo de acordos não são nada fáceis de obter…)

Outro problema grande está em provar realmente os crimes. Para alguém ser acusado e condenado de ter cometido uma acção ilícita é necessário provar três coisas básicas: a ocorrência do ilícito, se realmente o ilícito foi praticado pelo sujeito em questão e obviamente se o ilícito que se está a acusar é realmente um ilícito. Qual é a grande dificuldade então? Bem as dificuldades surgem devido á efemeridade da Internet e à facilidade com que as provas podem desaparecer e omitidas e devido a ser uma área que pode entrar em campos demasiado tecnicistas, é possível levantar linhas de defesa em aspectos técnicos que podem de facto levar a uma absolvição. Temos um caso minimamente recente que se passou na Grã-Bretanha em que Aaron Caffrey foi acusado de atacar o servidor de uma empresa. Este apresentou como defesa uma invasão do seu computador por um trojan que possibilitou um acesso remoto por um outro utilizador que cometeu o crime utilizando a sua ligação. Dado que os peritos não encontraram qualquer vestígio desse ficheiro, ele alegou que ao cumprir a missão dele (o ficheiro trojan) o ficheiro se auto destruiu.

Realmente isto é possível acontecer e com tais alegações as provas perderam consistência e o arguido foi ilibado. No nosso sistema judicial tal não seria possível, pois tal alegação do arguido teria de ser provado pelo mesmo. Obviamente que isso pode ser bom, mas também pode ser mau, pois se tal realmente acontece-se a alguém a Portugal e devido ao trojan se auto destruir o arguido seria inocente mas não teria meios para poder provar a sua inocência. Claro que o contrário também deixa de ser possível, se alguém entrar ilicitamente num sistema, não poderia usar a mesma alegação que foi usada na Grã-Bretanha para ser ilibado.

Tal como foi explicado em cima o problema da Internet ser global pode mesmo violar direitos básicos, como o direito de autor. Basta haver um país que tenha uma politica em relação a copyrights um bocado mais permissiva, que permita em certas condições a partilha de documentos, aplicações media etc… de um modo menos restrito, o que implica que as pessoas nesse país possam partilhar na web esses mesmos documentos, aplicações, media, etc… de um noutro país tenham leis de copyright mais restritas e protectoras do autor. Saindo assim o autor delas lesado em relação à legislação do seu país e sem ferramentas legais para garantir os seus direitos (dado que como explicado em cima essa partilha não é ilícita no pais em que está a ser partilhada mas apenas ilícita no país de origem do autor).

Estes problemas são bastante complicados de resolver e a solução mais eficaz e possível será como já referido por acordos internacionais e de uma convergência de legislações em relação a este tipo de problemas.

2.CRIMES INFORMÁTICOS

2.1. LEGISLAÇÃO APLICÁVEL

Como ja foi referido em Portugal já existe, desde há algum, espaço na lei portuguesa para o tratamento do crime informático, mais especificamente a Lei 109/91, de 17 de Agosto, mas também infracções previstas e punidas na Lei 67/98, de 26 de Outubro, bem como algumas infracções previstas no Código Penal.

Mas quais são em concreto os chamados crimes informáticos?

Os previstos e punidos na Lei 109/91:

- Falsidade informática
- Dano relativo a dados ou programas informáticos
- Sabotagem informática
- Acesso ilegítimo
- Intercepção ilegítima
- Reprodução ilegítima de programas protegidos e de topografia

Os previstos e punidos na Lei 67/98:

- Não cumprimento de obrigações relativas a protecção de dados
- Acesso indevido
- Viciação ou destruição de dados pessoais
- Desobediência qualificada
- Violação do dever de sigilo

Os previstos no Código Penal:

- Devassa por meio de Informática
- Burla informática e nas telecomunicações

A entidade responsável em Portugal para a investigação destes crimes é a Secção de Investigação de Criminalidade Informática e de Telecomunicações, vulgarmente designada por SICIT, não vamos aprofundar aqui o seu âmbito, história e competências, pois isso será tratado mais à frente.

Estes vários crimes podem ser atribuídos a vários grupos distintos, reconhecidos pela SICIT, podendo desta maneira ser categorizados e identificados alguns dos comportamentos e áreas onde são mais vulgarmente praticados.

Os grupos identificados como tendo comportamentos desviantes na Internet pela SICIT são, os BBS, BlackBoxing, BlueBoxing, carding, cracking, hacking, NUI, pedofilia, phreaking, sniffing, software, spam e VUI.

De seguida vamos analisar mais concretamente cada um destes grupos, o que são, para que servem e que leis potencialmente podem ser violadas por cada um desses grupos, sendo que essa violação não é exclusiva de um só grupo.

2.2. BBS

Os BBS (Bulletin Board System) são uma das mais antigas formas de aceder a Internet precedendo a actual WWW (World Wide Web) eram usados pelas pessoas para múltiplas funções, sendo um fenómeno altamente social, eram usados para encontrar e conhecer pessoas, discussões acerca de qualquer tópico, bem como para publicar artigos, fazer o *download* de *software* e jogar jogos, isto tudo usando apenas uma única aplicação.

O seu uso era feito através de uma ligação telefónica para um servidor usando um programa específico, no entanto com o surgimento da WWW o uso dos BBS caiu em completo declínio, mas estes serviram de base para o que agora se chama de *Newsgroups,* apesar disto o termo usado pela SICIT ainda continua a ser BBS podendo ser aplicado aos dois serviços.

Segundo a lei portuguesa os BBS e os *Newsgroups* não são proibidos nem regulamentados, tendo que estar apenas em conformidade com o preconizado pela ANACOM (Autoridade Nacional de Comunicações) no tocante aos meios técnicos empregues.

No entanto, o que esta ao abrigo da lei portuguesa é o seu conteúdo, pois este não pode de maneira alguma contribuir com informações que contrariem a Lei ou que constituam um risco de segurança, quer seja pessoal, nacional ou internacional, quer seja so um simples incitamento ou a disponibilização de dados para tal.

Por isso, e atendendo a alguns casos, é crime disponibilizar, quer seja apenas uma parte ou na sua totalidade, dados relativos a explosivos, números de cartões de crédito, descrever como se pode cometer crimes, *software* protegido por *copyright*, mesmo que este esteja comprimido por outros programas ou seja distribuído incompleto ou por partes.

Por estas definições verifica-se que a Reprodução ilegítima de programa protegido e de topografia é das mais facilmente quebradas, sendo tanto os BBS como os *Newsgroups* povoados por muitos utilizadores a publicarem de maneira ilegítima programas de computador. Por isso e de acordo com o artigo 9º da Lei 109/91 quem efectua tal publicação pode ser punido com uma pena de prisão até três anos ou com uma pena de multa, sendo que a própria tentativa também é punida.

Na parte relativa à Lei da Protecção de Dados Pessoais, verificamos que as infracções podem ser várias, desde a violação do dever de sigilo ao não cumprimento de obrigações relativas a protecção de dados, sendo no caso da violação do dever de sigilo em caso de incumprimento, segundo o artigo 47º da Lei 67/98, punido com prisão até dois anos ou multa ate 240 dias, no caso específico de negligência é punido com prisão até seis meses ou multa até 120 dias.

Nestes casos a acção depende de uma queixa.

Há um agravamento de metade dos limites da pena em caso excepcionais, tais como se o agente for funcionário público ou equiparado, nos termos da lei penal, for determinado pela intenção de obter qualquer vantagem patrimonial ou outro benefício ilegítimo ou puser em perigo a reputação, a honra e consideração ou a intimidade da vida privada de outrem.

Pelo artigo 46º da mesma lei podem ser punidos com a pena correspondente ao crime de desobediência qualificada, se após uma notificação não houver uma

mudança de comportamento e continuarem em incumprimento, no caso do não cumprimento de obrigações relativas a protecção de dados, é aplicada uma punição com pena de prisão até um ano ou uma multa ate 120 dias, sendo esta pena agravada para o dobro dos seus limites caso os dados pessoais forem aqueles a que se referem os artigos 7º e 8º da Lei 67/98, mais concretamente os dados considerados sensíveis e dados referentes a suspeitas de actividades ilícitas, infracções penais e contra-ordenações.

Por fim como um meio que possibilita a fácil distribuição de conteúdos, e de acordo com o artigo 172º do Código Penal é punível com pena de prisão até três anos quem exibir, ceder a qualquer título ou por qualquer meio, fotografias, filmes ou gravações pornográficas de menores de 14 anos. Sendo que para este artigo conta a posse, mera troca ou afixação, a venda destas imagens constitui uma agravante da pena de prisão de seis meses a cinco anos.

2.3. SNIFFING

Sniffing implica o uso de um *packet sniffer* para a "escuta" da informação passada entre dois pontos. O seu funcionamento, será tal como uma escuta telafónica, com a diferença que neste caso a conversa escutada será toda a informação passada entre dois computadores ou entre a rede e um computador, pode assim ser gravada toda a informação passada para esse computador alvo, seja voz, dados, imagens, sons.

Ao contrário de uma conversa telefónica, os dados passados entre computadores são aparentemente apenas dados binários aleatórios, só uns e zeros, por isso esses *packet sniffers* descodificam essa informação podendo assim saber o que se passa e que tipo de informação está a ser enviada.

Na França por exemplo o caso de Tareg Al Baho o ministério público Francês condenou os Directores da Escola Superior de Física e Química Industrial de Paris por violação do segredo de correspondência, pois eles tinham suspeitado que Tareg estava a usar o e-mail para uso pessoal e assim invadido a sua privacidade pois a Justiça Francesa entende que as contas de e-mail estão protegidas pelo segredo da correspondência.

Por isso neste caso alguém que sem autorização efectue *sniffing* incorre no crime de intercepção ilegítima que através do artigo 8º da Lei 109/91 pode ser punido com pena de prisão até três anos ou com pena de multa, mesmo para quem apenas tente sem qualquer resultado interceptar a transmissão de informação.

2.4. HACKING

Possivelmente o termo mais conhecido de todos, bem como termo usado para identificar os seus praticantes *hackers*.

Este termo surge do inglês, tendo o seu significado evoluído consideravelmente, considera-se que originou do verbo *to hack* em que *hack* representa o acto de alterar algo que já se encontra pronto ou em desenvolvimento, deixando-a melhor. O termo era usado então no MIT (Massachusetts Institute of Technology) para designar os primeiros interessados pela, então, nascente área da informática, sendo que por esta definição um *hacker* seriam todos aqueles que criaram coisas tão distintas como a Internet, o Linux, entre outros e vários especialistas em segurança de grandes empresas.

O termo teve a sua adopção alargada devido ao uso em vários filmes de Hollywood sendo dando ênfase principal no filme Wargames e apesar de toda esta conotação com o mundo informático, na sua origem poderia ser também indicativo de qualquer pessoa que fosse um especialista na sua area.

Actualmente tem um sentido mais pejorativo, apesar de ainda centrar-se em pessoas com fortes conhecimentos em programação, administração de sistemas e segurança informática, designa geralmente as pessoas que usam esses conhecimentos para aceder a sistemas informáticos de uma maneira indevida.

A personalidade do *hacker* designa alguém que tradicionalmente invade um sistema alheio, não para qualquer ganho pessoal, mas apenas pelo desafio que isso representa, no possuem assim motivações monetárias ou maliciosas. A grande maioria dos genuínos *hackers* invadem um sistema, deixam a sua marca e saem sem qualquer prejuízo para o mesmo. Havendo no entanto também aqueles que o fazem, por maldade e ganho pessoal, sendo que geralmente esses são excluídos da própria comunidade *hacker*. Muitas vezes os *hackers* são também confundidos com os *crackers* que na comunidade *hacker* são designados por *Black Hat*. Isto é algo que não deveria acontecer, mas acontece muitas vezes na comunicação social. Possivelmete devido à sua própria desinformação, ou devido ao termo hacker ser mais sensasionalista, o que acaba por levar a um uso indevido da palavra *hacker*.

No entanto diversos *hackers* estão, ou acabam por passar para o lado cumpridor da lei. Isto acontece principalmente na área de segurança informática, trabalhando para ajudar as empresas a manterem os seus sistemas seguros. Estes são geralmente denominados de *White Hat,* pois quando invadem

um sistema avisam apenas o responsável do mesmo para que este o corrija e evite novos ataques. Estes acabam, muitas vezes também, por trabalhar para essas mesmas empresas como consultores de segurança, fazendo esses ataques com o seu consentimento.

Podemos encontrar um exemplo muito conhecido de um *White Hat* na pessoa de Tsutomu Shimomura, um *hacker* que a trabalhar com o FBI ajudou a capturar o possivelmente mais famoso *hacker* de sempre Kevin Mitnick em 1994. Mitnick foi condenado por fraude e invasão dos sistemas da Fujitsu, Motorola, Nokia e Sun Microsystems. Apesar de muitos o considerarem como um especialista, a maior parte dos seus ataques foi feita usando principalmente técnicas de engenharia social. Mas até Mitnick acabou por se converter num *hacker* do bom lado da lei, dando, hoje em dia, conferências sobre segurança por todo o mundo.

Em termos da lei portuguesa, e através do artigo 7º da Lei 109/91 *hackar* um sistema constitui um crime de acesso ilegítimo, e por isso punido com pena de prisão até um ano, agravado até três anos ou multa se o acesso for conseguido através de violação de regras de segurança.

Se com tal acesso, no entanto, se tiver tomado conhecimento de segredo comercial ou industrial ou dados confidenciais, protegidos por lei, ou obtiver benefício ou vantagem patrimonial de valor consideravelmente elevado a pena será a de prisão de um a cinco anos.

Nesta área está contemplada também o uso de *default accounts* e de *passwords* que não lhe pertençam e não tenha obtido autorização prévia, sendo um exemplo disso o uso de contas de terceiros para o acesso a Internet.

A pena é agravada até cinco anos se o valor da vantagem obtida for elevado ou se tomarem conhecimento de dados confidenciais protegidos por lei ou de segredos industriais ou comerciais.

Deve-se salientar que não é só o proprio acesso que é considerado crime. A simples tentativa de acesso ilegal a um sistema também constitui um ilicito, caso seja provada.

2.5. CRACKING

Há aqui bastantes semelhanças com *hacking,* no entanto, e mesmo pelos prórprios *hackers*, os *crackers* têm uma conotação mais negativa. Estes são movidos por motivos "menos nobres" se assim o podermos dizer, qualquer ataque por parte deles tem como objectivo tirar algum partido pessoal, alguma vantagem dai, quer seja monetária ou informativa.

Neste caso e ultimamente cada vez mais a designação de *cracker* indica mais concretamente um *software cracker* (alguém que modifica *software* para retirar alguma protecção de cópia existente). Estes estão geralmente organizados em grandes organizações para a distribuição desse *software* pirateado, designado entre eles por *warez.* Distribuem também pequenos *patches* que permitem contornar a protecção existente em programas de computador, sendo neste caso mais uma violação de *copyright* e de direitos de autor.

O que reporta a um dos problemas que está mais na actualidade, a tão falada pirataria informática. As várias organizações estimam que as perdas originadas são astronómicas, havendo no entanto também que reconhecer os efeitos positivos que trouxe para algumas companhias. Por exemplo a Adobe e a Microsoft, que devido à sua posição, deixam que as pessoas individuais usem os seus programas de maneira ilicita, apenas consciencializando-as sem proceder a acções judiciais. Isto permitiu que nos anos 80 um sem número de estudantes, na altura sem possibilidade de pagar as licenças necessárias, usasse esses programas pirateados. Estes quando passaram para o mundo de trabalho devido à sua familiaridade com esses programas continuaram a usá-los. Obviamente aqui estas duas empresas já obrigavam judicialmente ao pagamento das suas licenças. Isto acabou por dar um contributo para o aumento de popularidade dos mesmos programas que um dia piratearam, assim como a um grande aumento de vendas a nivel empresarial.

No âmbito dos *crackers* há que referir os *phreakers* que vamos falar aprofundadamente, mais à frente, bem como dos *Script Kiddies*.

Estes últimos não são mais que, *crackers* inexperientes que usam *scripts* e programas desenvolvidos por outros, sem conhecimento real do que estão a fazer, usando apenas as ferramentas que outros fizeram. Tradicionalmente, e ao contrário da maior parte dos *crackers*, não atacam um alvo específico, mas sim analisam um número alargado de sistemas à procura de um que esteja vulnerável ao ataque. O potencial mais negativo advém da ajuda que eles podem dar a *crackers* mais experientes que os podem manipular e encorajar para

serem mais destrutivos, sendo assim uma força muito poderosa. Sendo considerados praticamente os *gangs* da Internet.

Actualmente, principalmente nos EUA os programas de computador, entre outros produtos digitais estão protegidos pela agressiva e bastante proibitiva DMCA (Digital Millennium Copyright Act) sendo que a União Europeia em 2001 passou a EUCD (EU Copyright Directive) sendo que ambas implementam o WIPO Copyright Treaty, Portugal já tem implementada a sua versão da EUCD.

É no entanto difícil condenar alguém pelo próprio acto de *crackar* um programa ou um jogo de computador. Isto acontece devido a ser bastante complicado provar que alguém é responsável por isso. Sendo assim a grande parte das acções judiciais existentes por todo mundo visam principalmente apanhar a distribuição desse *software*. Como exemplos práticos temos os casos contra a rede P2P Kazaa detida pela Sherman Networks, sendo principalmente atacada por violação de *copyright* e distribuição desse material.

Pela lei portuguesa estas actividades incorrem em vários crimes, sendo que a descompilação de programas é prevista e punida pelo artigo 7º do Decreto-Lei 252/94 (Protecção Jurídica dos Programas de Computador) e pelo artigo 9º da Lei 109/91. Esta legislação abrange os programas residentes em memória, que permitem a utilização de software utilitário e de jogos violando assim os direitos de autor. A própria tentativa deste ilícito é punível judicialmente.

No entanto se analisarmos pelo prisma dos *Script Kiddies* e mesmo pelos *crackers* como *hackers*, podem incorrer noutros crimes, como os definidos pelos artigos 7º, 6º e 5º da Lei 109/91.

2.6. PHREAKING

Como foi referido no ponto anterior na categoria dos *crackers* podemos individualizar um grupo que tem bastante importância e foi também dos primeiros grupos a praticarem este tipo de crimes informáticos, os *phreakers*.

O termo *phreaking* (geralmente reconhecido como a junção das palavras inglesas *phone* e *freak*) é usado para descrever uma subcultura de pessoas que se dedicam ao estudo, experiência e abuso dos telefones e das suas redes.

No seu inicio e com a introdução de automatizações nas redes telefónicas, era possível tirar partido dessas automatizações para efectuar chamadas sem pagar as taxas necessárias. Para isso, era emulado os sinais que a rede usava

para certas funções, sendo assim contornada a propria companhia, usando os mesmos sinais e frequências que existiam para propósitos internos.

Ultimamente todo o movimento deu origem ao que foi chamado de *Blue Box*, pequenos aparelhos com a capacidade de reproduzir esses tons, facilmente permitindo a qualquer pessoa com um fácil acesso à rede, cometer este crime. O nome surgiu pelo facto de o primeiro aparelho confiscado pela *Bell System Security* têr sido construído com uma caixa de plástico azul.

Daqui advém o termo usado pela SICIT de *blackboxing* e *blueboxing*, sendo que representam qualquer forma de perturbação na rede de telecomunicações, por injecção de frequências nas linhas ou por ligar dispositivos electrónicos cujo efeito, seja o impedimento total ou a diminuição da taxação devida à operadora de telecomunicações.

Ao longo dos tempos *phreaking* sempre manteve esta componente de mexer através da rede telefónica e os seus sinais e frequências. No entanto e com as novas tecnologias, derivado ao advento do VoIP (*voice over internet protocol*), os muitos *phreakers* existentes estão a ficar com novos interesses.

Um dos *phreakers* mais conhecidos é John Draper, mais conhecido online pelo seu *nickname* Captain Crunch, derivado à mascote de uns cereais. Estes cereais continham um assobio dado como prémio, que podia ser modificado para ter a mesma frequência que as rede telefónicas usavam para indicar que a rede estava disponível para efectuar uma nova chamada, a partir desse local. Isto permitia efectuar chamadas sem pagar as taxas, o que levou à construção de várias *blue boxes* para efectuar um mesmo efeito. Em 1972 foi preso e condenado por fraude e teve como sentença cinco anos de pena suspensa. A meio da década de 70 ensinou os seus conhecimentos de *phreaking* a Steve Jobs e Steve Wozniak, mais conhecidos como fundadores da Apple Computer, Inc.. Em 1977 Draper foi novamente preso e condenado tendo desta vez uma sentença de prisão efectiva de quatro meses.

Uma das histórias mais conhecidas de Draper, conta que num telefone público começou a "enviar" a sua chamada pelo mundo fora, sem pagar, passando por países como Japão, Russia e Inglaterra, após passar por dezenas de países diferentes marcou o número correspondente ao telefone público ao seu lado, passado alguns minutos o telefone começou a tocar, Draper falou ao primeiro telefone e após alguns segundos ouviu a sua própria voz, de maneira bastante ténue, no outro telefone.

Neste caso e pela lei portuguesa estas actividades constituem o crime de burla nas comunicações, punido pelo artigo 221 n.º 2 do Código Penal até 3 anos de prisão.

Bem como ainda a utilização de redes de comunicações com base na manipulação de centrais telefónicas acedidas sem autorização para o efeito, constitui o crime de acesso ilegítimo, contemplado no artigo 7º da Lei 109/91.

Há ainda o caso da utilização indevida dos chamados NUI's e VUI's para acesso a redes x.25, constituem crime de acesso ilegítimo, punido pelo mesmo artigo 7º da Lei 109/91.

2.7. CARDING

Este representa o abuso que pode surgir dos dados contidos por exemplo nos nossos cartões de crédito, através do uso indevido dos dados para uso malicioso. Em termos actuais pode-se considerar o *phishing* como uma forma de *carding* na tentativa de usurpação dos dados pessoais para posteriormente os usar com proveito pessoal.

O *phishing* é designado por ser uma forma de engenharia social, usando a ingenuidade das pessoas contra elas. Geralmente caracteriza-se por um e-mail ou uma mensagem instantânea. Traduz-se geralmente pelo envio de um e-mail que nos leva a uma *website* em tudo idêntico ao *website* do banco da pessoa em questão, tentando fazer com que o utilizador reescreva os seus dados pessoais (*username* e *password*) de modo a serem usados posteriormente de uma maneira ílicita.

Em Janeiro de 2004 nos EUA foi apresentado o primeiro processo contra um suposto *phisher*, este processo foi entreposto pela FCT (*Federal Trade Commission*) norte-americana, contra um jovem Californiano com menos de vinte anos, que alegadamente terá criado uma página desenhada para parecer o *website* da *America Online* de modo a poder roubar números de cartões de crédito, desde essa data por todo o mundo ocidental têm sido redobrados os esforços no sentido de apanhar os responsáveis por esta nova forma de burla, tendo sido apreendidos *phishers* no Brasil, Estonia e Reino Unido por exemplo.

Todas as formas de manipulação de dados ou de elementos de identificação quer na face quer contidos em bandas magnéticas de cartões de crédito, de débito ou de telecomunicações, bem como a implantação de dados ou de elementos de identificação noutros suportes técnicos, constituem um crime de falsificação, punido com pena de prisão até 3 anos.

A utilização em mail orders de elementos de identificação ou de dados bancários de terceiros, constitui um crime de burla, punido com a pena de prisão até 3 anos e é agravada se o montante em causa for elevado ou se mantiverem essa conduta mais que uma vez.

O abuso da possibilidade conferida pela posse de cartão de crédito ou de garantia, mesmo que só pela forma tentada, é punível com pena de prisão até 3 anos, podendo ser agravado até 5 anos ou de 2 a 8 anos, caso o valor seja elevado ou consideravelmente elevado.

2.8. SPAM

Por *spam* entende-se que representa situações em que se verifica a emissão simultânea de uma mensagem de e-mail para vários utilizadores ao mesmo tempo.

Para muita gente *spam* representa apenas os e-mails que são de alguma forma anúncios a produtos ou empresas, tendo assim um cariz comercial, no entanto outros tipo de *spam* não comercial também são comuns.

Tem características muito demarcadas, tais como, não ser solicitado pelo receptor, a identificação do remetente ser falsa e ser usado o servidor de correio electrónico da vítima, seja de um ISP ou de uma entidade pública ou privada.

O *spam* torna-se aliciante e atractivo em termos de mercado, em virtude do seu baixo custo. Como referido as mensagens tanto podem ser de cariz comercial, como de cariz não comercial. Ambos os casos são importantes, pois tanto perturba o utilizador receber uma mensagem a publicitar um produto, como uma que lhe pede para participar num abaixo-assinado, ou para difundir informações sobre novos vírus.

Em casos específicos pessoas individuais tentam lutar contra os chamados *spammers,* sendo que o primeiro caso conhecido e com sucesso foi o caso de Nigel Roberts, das Ilhas do Canal pertencentes ao Reino Unido. Este ganhou £270 contra a Media Logistics UK que lhe tinha enviado e-mails de *spam* para a sua conta de e-mail pessoal.

Segundo a lei portuguesa é o uso do servidor de correio electrónico da vítima que lhe dá o grau criminoso ao envio de *spam.* Isto acontece pois, quem naqueles termos usar um servidor de e-mail de terceiros, pode ser acusado da prática do crime de acesso ilegítimo, ou seja o artigo 7º da Lei 109/91.

Pode ainda coexistir o crime de falsificação se a identificação de endereço falsificada for a de alguém em concreto.

Se o intuito do "spam" é interferir no normal funcionamento de um sistema informático poderá ser considerado crime de sabotagem informática, artigo 6º da Lei 109/91, punido com pena de prisão de cinco anos, ou com pena de multa.

2.9. ABUSO SEXUAL DE CRIANÇAS – PEDOFILIA

A pornografia infantil é um dos maiores problemas que assolam a Internet nos dias de hoje, pois pode ser encontrada em virtualmente todos os serviços que por ela são fornecidos.

A sua produção e venda é ilegal na maior parte dos países desenvolvidos, apesar de as regulamentações variarem profundamente de país para país, alguns países tais como Portugal, o Reino Unido e o Canada, proíbem a simples posse, enquanto países como a Russia não têm legislação específica acerta pornografia infantil, sendo vista como abuso de crianças.

Outro factor diferenciador entre os vários países é a chamada idade de consentimento, sendo que nos EUA esta idade é de 18 anos e na Islândia por exemplo é de 14 anos. Havendo assim distinções dependendo do país em questão. Devido a este facto, a União Europeia recomenda uma harmonização deste limite para os 18 anos.

Ainda este ano, um politico de Long Island nos EUA, processou o Google por alegar que o motor de busca está a lucrar com pornografia infantil por mostrar links pagos para sites com conteúdo ilegal com menores.

Como referido atrás o art. 172º do Código Penal pune com prisão até três anos quem exibir, ceder a qualquer título ou por qualquer meio, fotografias, filmes ou gravações pornográficas de menores de 14 anos.

A Internet é um meio por excelência onde existe uma facilidade incrível para a publicação e partilha deste tipo de documentos. Quer em BBS, IRC, ou *Newsgroups* sendo que este artigo abrange tanto a posse, como a partilha e afixação de tais imagens, a venda constitui um agravamento da pena de prisão de seis meses a cinco anos.

2.10. USO E REPRODUÇÃO ILEGÍTIMA DE *SOFTWARE*

Aquilo que é vulgarmente conhecido como pirataria informática, como também já foi referido atrás, fazendo parte do comportamento dos *crackers*, está principalmente protegido em Portugal através do *copyright* e do Código de Direitos de Autor e Direitos Conexos, não havendo lugar em Portugal para patentes no âmbito da informática.

Sendo no entanto os seus direitos salvaguardados, por isso a cópia e a distribuição a terceiros de programas informáticos protegidos por lei são proibidos e punidos por lei até três anos de prisão, a própria tentativa também é punível.

Mesmo que tais programas estejam comprimidos por outros programas ou sejam distribuídos apenas parcialmente, em vários serviços, *Newsgroups*, IRC, *websites*, FTP, etc.

O uso ilegítimo de programas de computador é punido pelo Código de Direitos de Autor e Direitos Conexos, com prisão até três anos e multa.

3. JURISPRUDÊNCIA EM PORTUGAL NO ÂMBITO DA CRIMINALIDADE INFORMÁTICA

Os Tribunais Portugueses têm proferido poucas decisões em matéria de criminalidade informática, sendo certo que grande parte das decisões proferidas em Portugal nesta matéria são decisões de primeira instância, as quais não são de acesso fácil pelo facto de não se encontrarem organizadas em bases de dados.

Em matéria de criminalidade informática, é aqui apresentada uma decisão proferida pelo Tribunal da Relação do Porto, relativa à questão de saber se uma busca e apreensão de material informático levada a cabo pelo IGAE foi ou não legítima (no âmbito de uma acção de inspecção destinada a detectar crimes de reprodução ilegítima de programas protegidos), e uma decisão do Tribunal Judicial de Coruche que condenou dois arguidos pela prática do crime de falsidade informática.

Acórdão do Tribunal da Relação do Porto de 01/05/2002

Realizada uma acção de inspecção pela IGAE, num gabinete de arquitectura, no âmbito das respectivas acções de fiscalização sobre "pirataria informática", os respectivos inspectores procederam à apreensão, nos termos do n.º 1 do artigo 178.º do CPP, de dois computadores nos quais se encontravam instalados programas que teriam sido reproduzidos ilegitimamente.

Inconformado com a busca e apreensão levadas a cabo, o arguido requereu ao Ministério Público que fosse declarada nula a busca efectuada por entender que (i) a IGAE carece de competência para proceder à investigação e instauração de processos crime bem como às buscas no âmbito destes processos apenas tendo competência para a investigação e instrução de processos por contra-ordenações cuja competência lhe esteja legalmente atribuída (sendo que a única entidade com competência para fiscalizar os actos ilícitos decorrentes do Decreto-Lei n.º 252/94 é o Ministério Público), que (ii) o local onde foi realizada a inspecção não era de livre acesso ao público pelo que, não tendo a busca sido autorizada por entidade competente, estaria também por essa via ferida de nulidade, e que (iii) os computadores apreendidos deveriam ser devolvidos

porquanto artigo 12.º da Lei 109/91 perda de bens a favor do Estado – não tem aplicação no âmbito da Lei de Protecção de Software.

A pretensão foi indeferida pelo Juiz de Instrução Criminal, o que motivou o recurso interposto pelo arguido para o Tribunal da Relação Porto.

O Tribunal da Relação do Porto confirmou o despacho recorrido por entender que: (i) a IGAE é um órgão de polícia criminal, tendo competência para proceder à investigação e instauração de processos crime; (ii) a busca efectuada ao gabinete de arquitectura do arguido, aquando de detenção em flagrante por crime a que corresponde pena de prisão, cai na previsão do artigo 174.º n.º 4 c) do CPP, não necessitando de autorização prévia da autoridade judiciária competente; (iii) o local em que a busca teve lugar, embora não fosse de livre acesso ao público, não assume as características de uma casa habitada ou de uma sua dependência fechada, pelo que não se encontra protegido pela norma contida no artigo 177.º do CPP, que define as regras sobre a busca domiciliária; e (iv) os computadores não deviam ser devolvidos, porquanto, por um lado, a sua apreensão foi validamente efectuada pelos inspectores da IGAE, como resulta das disposições conjugadas dos artigos 178.º n.º 1, 55.º n.º 2 e 249.º n.º 2 c), todos do CPP, e, por outro lado, o artigo 12.º da Lei 109/91 é plenamente aplicável no âmbito da Lei de Protecção de Software.

Sentença do Tribunal Judicial de Coruche

O Tribunal Judicial de Coruche condenou dois arguidos pela prática do crime de falsidade informática e crime de burla.

Ficou provado que um dos arguidos forjava cartões destinados a obter o benefício fiscal do gasóleo agrícola, substituindo os respectivos chips por chips por si modificados, nos quais introduzia os dados de entidades que sabia terem um elevado *plafond* de utilização de gasóleo agrícola, dados esses que subtraía dos cartões utilizados no posto de abastecimento por si explorado.

Ficou também provado que o referido arguido utilizava esses cartões simulando abastecimentos que não tinham lugar, por forma a obter por parte do Estado, em conluio com um cúmplice e com outros postos de abastecimento, o pagamento do aludido benefício fiscal (o qual era, posteriormente, dividido entre todos).

O Tribunal entendeu que a modificação de dados não incidia exactamente sobre o chip do cartão original, pelo que não seria adequada a incriminação dos arguidos pelo crime de falsificação de documento previsto no artigo 256.º do Código Penal.

Contudo, o Tribunal acabou por condenar os arguidos pela prática dos crimes de falsidade informática e burla, tendo entendido, relativamente ao primeiro, previsto no artigo 4.º da Lei da Criminalidade Informática, que a prática levada a cabo pelo arguido interferiu no tratamento informático dos dados com base nos quais era feita a gestão e controle da concessão do benefício fiscal do gasóleo agrícola, sendo certo que os dados em causa eram susceptíveis de servir como meio de prova, designadamente da legitimidade do portador e do *plafond* de gasóleo disponível (refira-se que, para que seja preenchido o tipo penal previsto no artigo 4.º da Lei da Criminalidade Informática, é necessário que os dados objecto de interferência ou modificação ilícita sejam susceptíveis de servir como meio de prova, de tal modo que a sua visualização produza os mesmos efeitos de um documento falsificado).

Através destes dois exemplos pode-se verificar que hoje em dia a criminalidade informática, a nível dos tribunais constitui uma, se podemos designar, nova matéria, quer a nível jurisprudencial, quer a nível doutrinal. Com a nova era informática que se aproxima, esta questão adquire uma nova relevância. A segurança e protecção dos utilizadores poderá sair reforçada com uma mais eficaz admoestação e com a descoberta cada vez mais precisa deste tipo de crime.

4.MEIOS DE COMBATE À CRIMINALIDADE INFORMÁTICA EM PORTUGAL

Em Portugal, foi criada em Janeiro de 1995, a Brigada de Investigação de Criminalidade Informática – BICI, que tinha competência nacional para a investigação da criminalidade informática e alguns dos crimes praticados com recursos e meios informáticos.

Em Setembro de 1998, foi substituída pela SICIT, *Secção de Investigação de Criminalidade Informática e de Telecomunicações*, constituída por duas Brigadas de Investigação. Estes órgãos, no âmbito das suas funções, estão especialmente empenhados em actos de prevenção criminal na sua órbita de investigação. Entre os seus objectivos, pretendem contribuir para o aumento da cultura de segurança informática.

De acordo com a Lei Orgânica da Polícia Judiciária – LOPJ, presume-se deferida à Polícia Judiciária em todo o território a competência exclusiva para a investigação de determinados crimes de maior gravidade e complexidade. E é justamente nessa área que a SICIT detém a competência nacional para a investigação da chamada criminalidade informática, a qual compreende a generalidade das infracções penais previstas e punidas pela Lei 109/91, que são: *Falsidade informática; Dano relativo a dados ou programas informáticos; Sabotagem informática; Acesso ilegítimo, Intercepção ilegítima; Reprodução ilegítima de programa protegido e de topografia*, bem como as infracções penais previstas e punidas pela Lei 67/98, designadamente: *Não cumprimento de obrigações relativas a protecção de dados; Acesso indevido; Viciação ou destruição de dados pessoais; Desobediência qualificada; Violação do dever de sigilo*, e ainda de algumas infracções penais previstas no Código Penal: *Devassa por meio de informática; Burla informática e nas Telecomunicações*.

5. CONCLUSÃO

A já longínqua lei portuguesa da criminalidade informática, com quase 16 anos de existência, tomou na altura da sua elaboração posições particularmente veementes nesse domínio quando, paradoxalmente, nem sequer os programas de computador eram objecto de protecção legal, tendo o legislador tido por base trabalhos preparatórios de convenções internacionais não correspondentes a textos que tivessem permanecido em vigor.

A sua evolução permaneceu estagnada, no remoto ano de 1991, o mesmo em que foi concebida. Assim se pode entender, tantas são as mudanças que ocorrem, face extraordinário aceleramento das actividades de investigação e desenvolvimento, produção, comercialização e utilização da informática e, no entanto, a LCI permanece inalterada.

Ao longo do trabalho referimos, estarmos a caminhar a um passo de um sistema onde, inevitavelmente, a criminalidade informática se torna num flagelo cada vez maior na proporção inversa que são os meios para a combater ou dissuadir.

As cifras negras da criminalidade informática, de dimensão incomparavelmente maior à de outros ilícitos penais, continua a reger-se mais por mecanismos de auto regulação que regras de comércio e da concorrência, da propriedade intelectual e dos direitos de autor, dos direitos e garantias da privacidade, da protecção da pessoa e da convivência civilizacional e cultura dos povos e dos países do que pelas normas específicas deste novo tipo de ilícitos que têm como objecto e meio a informática e todas as realidades da vida humana que crescentemente se lhe associam.

Certamente, que um novo corpo de normas se constituirá que mais coerentemente e prospectivamente responderá à protecção dos bens informáticos na sua expressão mais extensa de Hardware, Software, dados, informação, conhecimento, poder, vida, direito, moral e ética e um mundo novo com todas estas realidades em crescente transformação.

6. BIBLIOGRAFIA

- http://www.apdsi.pt/Peritos_defendem_actualizacao_da_Lei_do_Crime_Informatico.pdf
- http://216.239.59.104/search?q=cache:ur50P3gGkrwJ:seguranet.min-edu.pt/media/2005_Artigo_criminalidade%2520informatica_revista_comunicacoes.doc+criminalidade+inform%C3%A1tica&hl=pt-PT&gl=pt&ct=clnk&cd=8&client=firefox-a
- http://www.policiajudiciaria.pt/htm/noticias/criminalidade_informatica.htm
- http://www.miudossegurosna.net/artigos/2005-03-18-acapital.html
- http://diariodigital.sapo.pt/news_history.asp?section_id=44&id_news=162241
- http://news.bbc.co.uk/1/hi/technology/3202116.stm
- http://en.wikipedia.org/wiki/Hacker
- http://en.wikipedia.org/wiki/Phreaking
- http://en.wikipedia.org/wiki/Phishing
- http://en.wikipedia.org/wiki/Spam_%28electronic%29
- http://en.wikipedia.org/wiki/Software_cracking
- http://en.wikipedia.org/wiki/Bbs
- http://en.wikipedia.org/wiki/Child_pornography
- http://en.wikipedia.org/wiki/WIPO_Copyright_Treaty
- http://en.wikipedia.org/wiki/Script_kiddie
- http://en.wikipedia.org/wiki/Packet_sniffer
- http://en.wikipedia.org/wiki/Kazaa
- http://en.wikipedia.org/wiki/Kevin_Mitnick
- http://en.wikipedia.org/wiki/John_Draper
- http://en.wikipedia.org/wiki/Digital_Millennium_Copyright_Act
- http://en.wikipedia.org/wiki/EU_Copyright_Directive

A N E X O S :

Anexo A - Lei nº 109/91 - Sobre a criminalidade informática

A Assembleia da República decreta, nos termos dos artigos 164º, alínea d), 168º, nº 1, alínea c), e 169º, nº 3, da Constituição, o seguinte:

CAPÍTULO I

Princípios gerais

Artigo 1º – Legislação penal

Aos crimes previstos na presente lei são subsidiariamente aplicáveis as disposições do Código Penal.

Artigo 2º – Definições

Para efeitos da presente lei, considera-se:

a) Rede informática – um conjunto de dois ou mais computadores interconectados;

b) Sistema informático – um conjunto constituído por um ou mais computadores, equipamento periférico e suporte lógico que assegura o processamento de dados;

c) Programa informático – um conjunto de instruções capazes, quando inseridas num suporte explorável em máquina, de permitir à máquina que tem por funções o tratamento de informações indicar, executar ou produzir determinada função, tarefa ou resultado;

d) Topografia – uma série de imagens entre si ligadas, independentemente do modo como são fixadas ou codificadas, que representam a configuração tridimensional das camadas que compõem um produto semicondutor e na qual cada imagem reproduz o desenho ou parte dele de uma superfície do produto semicondutor, independentemente da fase do respectivo fabrico;

e) Produto semicondutor – a forma final ou intermédia de qualquer produto, composto por um substrato que inclua uma camada de material semicondutor e constituído por uma ou várias camadas de matérias condutoras, isolantes ou semicondutoras, segundo uma disposição conforme a uma configuração tridimensional e destinada a cumprir, exclusivamente ou não, uma função electrónica;

f) Intercepção – o acto destinado a captar informações contidas num sistema automatizado de dados, através de dispositivos electromagnéticos, acústicos, mecânicos ou outros;

g) Valor elevado – aquele que exceder 50 unidades de conta processual penal avaliadas no momento da prática do facto;

h) Valor consideravelmente elevado – aquele que exceder 200 unidades de conta processual penal avaliadas no momento da prática do facto.

Artigo 3º – Responsabilidade penal das pessoas colectivas e equiparadas

1– As pessoas colectivas, sociedades e meras associações de facto são penalmente responsáveis pelos crimes previstos na lei, quando cometidos em seu nome e no interesse colectivo pelos seus órgãos ou representantes.

2– A responsabilidade é excluída quando o agente tiver actuado contra ordens ou instruções expressas de quem de direito.

3– A responsabilidade das entidades referidas no nº 1 não exclui a responsabilidade individual dos respectivos agentes.

4– As entidades referidas no nº 1 respondem solidariamente, nos termos da lei civil, pelo pagamento das multas, indemnizações e outras prestações em que forem condenados os agentes das infracções previstas na presente lei.

CAPÍTULO II

Dos crimes ligados à informática

Artigo 4º .– Falsidade informática

1– Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados ou programas informáticos ou, por qualquer outra forma, interferir num tratamento informático de dados, quando esses dados ou programas sejam susceptíveis de servirem como meio

de prova, de tal modo que a sua visualização produza os mesmos efeitos de um documento falsificado, ou, bem assim, os utilize para os fins descritos, será punido com pena de prisão até cinco anos ou multa de 120 a 600 dias.

2- Nas mesmas penas incorre quem use documento produzido a partir de dados ou programas informatizados que foram objecto dos actos referidos no número anterior, actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiros.

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

Artigo 5º - Dano relativo a dados ou programas informáticos

1- Quem, sem para tanto estar autorizado, e actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo para si ou para terceiros, apagar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis dados ou programas informáticos alheios ou, por qualquer forma, lhes afectar a capacidade de uso será punido com a pena de prisão até três anos ou pena de multa.

2- A tentativa é punível.

3- Se o dano causado for de valor elevado, a pena será a de prisão até 5 anos ou de multa até 600 dias.

4- Se o dano causado for de valor consideravelmente elevado, a pena será a de prisão de 1 a 10 anos.

5- Nos casos previstos nos nºs 1, 2 e 3 o procedimento penal depende da queixa.

Artigo 6º - Sabotagem informática

1- Quem introduzir, alterar, apagar ou suprimir dados ou programas informáticos ou, por qualquer outra forma, interferir em sistema informático, actuando com intenção de entravar ou perturbar o funcionamento de um sistema informático ou de comunicação de dados à distância, será punido com pena de prisão até 5 anos ou com pena de multa até 600 dias.

2- A pena será a de prisão de um a cinco anos se o dano emergente da perturbação for de valor elevado.

3- A pena será a de prisão de 1 a 10 anos se o dano emergente da perturbação for de valor consideravelmente elevado.

Artigo 7º - Acesso ilegítimo

1- Quem, não estando para tanto autorizado e com a intenção de alcançar, para si ou para outrem, um benefício ou vantagem ilegítimos, de qualquer modo aceder a um sistema ou rede informáticos será punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.

2- A pena será a de prisão até três anos ou multa se o acesso for conseguido através de violação de regras de segurança.

3- A pena será a de prisão de um a cinco anos quando:

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

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

4- A tentativa é punível.

5- Nos casos previstos nos nºs 1, 2 e 4 o procedimento penal depende de queixa.

Artigo 8º - Intercepção ilegítima

1- Quem, sem para tanto estar autorizado, e através de meios técnicos, interceptar comunicações que se processam no interior de um sistema ou rede informáticos, a eles destinadas ou deles provenientes, será punido com pena de prisão até três anos ou com pena de multa.

2- A tentativa é punível.

Artigo 9º - Reprodução ilegítima de programa protegido

1- Quem, não estando para tanto autorizado, reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei será punido com pena de prisão até três anos ou com pena de multa.

2- 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.

3- A tentativa é punível.

Artigo 10º - Penas aplicáveis às pessoas colectivas e equiparadas

1- Pelos crimes previstos na presente lei são aplicáveis às pessoas colectivas e equiparadas as seguintes penas principais:

a) Admoestação;

b) Multa;

c) Dissolução.

2- Aplica-se a pena de admoestação sempre que, nos termos gerais, tal pena possa ser aplicada à pessoa singular que, em representação e no interesse da pessoa colectiva ou equiparada, tiver praticado o facto.

3- Quando aplicar a pena de admoestação, o tribunal poderá aplicar cumulativamente a pena acessória de caução de boa conduta.

4- Cada dia de multa corresponde a uma quantia entre 10 000$ e 200 000$, que o tribunal fixará em função da situação económica e financeira da pessoa colectiva ou equiparada e dos seus encargos.

5- Se a multa for aplicada a uma entidade sem personalidade jurídica, responderá por ela o património comum e, na sua falta ou insuficiência, o património de cada um dos associados.

6- A pena de dissolução só será aplicada quando os titulares dos órgãos ou representantes da pessoa colectiva ou sociedade tenham agido com a intenção, exclusiva ou predominantemente, de, por meio dela, praticar os factos que integram os crimes previstos na presente lei ou quando a prática reiterada desses factos mostre que a pessoa colectiva ou sociedade está a ser utilizada para esse efeito, quer pelos seus membros, quer por quem exerça a respectiva administração.

CAPÍTULO III

Penas acessórias

Artigo 11º - Penas acessórias

Relativamente aos crimes previstos no presente diploma, podem ser aplicadas as seguintes penas acessórias:

a) Perda de bens;

b) Caução de boa conduta;

c) Interdição temporária do exercício de certas actividades ou profissões;

d) Encerramento temporário do estabelecimento;

e) Encerramento definitivo do estabelecimento;

f) Publicidade da decisão condenatória.

Artigo 12º – Perda de bens

1– O tribunal pode decretar a perda dos materiais, equipamentos ou dispositivos pertencentes à pessoa condenada que tiverem servido para a prática dos crimes previstos no presente diploma.

2– A perda de bens abrange o lucro ilícito obtido com a prática da infracção.

3– Se o tribunal apurar que o agente adquiriu determinados bens, empregando na sua aquisição dinheiro ou valores obtidos com a prática do crime, serão os mesmos também abrangidos pela decisão que decretar a perda.

Artigo 13º – Caução de boa conduta

1– A caução de boa conduta implica a obrigação de o agente depositar uma quantia em dinheiro, a fixar entre 10 000$ e 1 000 000$, à ordem do tribunal, pelo prazo fixado na decisão condenatória, por um período entre seis meses e dois anos.

2– A caução de boa conduta deve, em regra, ser aplicada sempre que o tribunal condene em pena cuja execução declare suspensa.

3– A caução será declarada perdida a favor do Estado se o agente praticar, por meio de informática, nova infracção no período fixado na sentença, pela qual venha a ser condenado, sendo-lhe restituída no caso contrário.

Artigo 14º – Interdição temporária do exercício de certas actividades ou profissões

1– A interdição temporária do exercício de certas actividades ou profissões pode ser decretada quando a infracção tiver sido cometida com flagrante e manifesto abuso da profissão ou no exercício de actividade que dependa de um título público ou de uma autorização ou homologação da autoridade pública.

2- A duração da interdição tem um mínimo de dois meses e um máximo de dois anos.

3- Incorre na pena do crime de desobediência qualificada quem, por si ou por interposta pessoa, exercer a profissão ou a actividade durante o período da interdição.

Artigo 15º - Encerramento temporário do estabelecimento

1- O encerramento temporário do estabelecimento pode ser decretado por um período mínimo de um mês e máximo de um ano, quando o agente tiver sido condenado em pena de prisão superior a 6 meses ou em pena de multa superior a 100 dias.

2- Não obstam à aplicação desta pena a transmissão do estabelecimento ou a cedência de direitos de qualquer natureza, relacionados com o exercício da profissão ou actividade, efectuados após a instauração do processo ou depois de cometida a infracção, salvo se, neste último caso, o adquirente se encontrar de boa fé.

3- O encerramento do estabelecimento nos termos do nº 1 não constitui justa causa para o despedimento de trabalhadores nem fundamento para a suspensão ou redução do pagamento das respectivas remunerações.

Artigo 16º - Encerramento definitivo do estabelecimento

1- O encerramento definitivo do estabelecimento pode ser decretado quando o agente:

a) Tiver sido anteriormente condenado por infracção prevista neste diploma em pena de prisão ou multa, se as circunstâncias mostrarem que a condenação ou condenações anteriores não constituíram suficiente prevenção contra o crime;

b) Tiver anteriormente sido condenado em pena de encerramento temporário;

c) For condenado em pena de prisão por infracção prevista neste diploma, que tenha determinado dano de valor consideravelmente elevado ou para um número avultado de pessoas.

2- Aplicam-se ao encerramento definitivo as disposições dos nºs 2 e 3 do artigo anterior.

Artigo 17º - Publicidade da decisão

1- Quando o tribunal aplicar a pena de publicidade, será esta efectivada, a expensas do condenado, em publicação periódica editada na área da comarca da prática da infracção ou, na sua falta, em publicação da área da comarca mais próxima, bem como através da afixação de edital, por período não inferior a 30 dias, no próprio estabelecimento ou no local do exercício da actividade, por forma bem visível pelo público.

2- Em casos particularmente graves, nomeadamente quando a infracção importe lesão de interesses não circunscritos a determinada área do território, o tribunal poderá ordenar, também a expensas do condenado, que a publicidade da decisão seja feita no Diário da República ou através de qualquer meio de comunicação social.

3- A publicidade da decisão condenatória é feita por extracto, do qual constem os elementos da infracção e as sanções aplicáveis, bem como a identificação dos agentes.

CAPÍTULO IV

Disposições finais

Artigo 18º - Processo de liquidação

1- Transitada em julgado a decisão que aplicar a pena de dissolução, o Ministério Público requer a liquidação do património, observando-se, com as necessárias adaptações, o processo previsto na lei para a liquidação de patrimónios.

2- O processo de liquidação corre no tribunal da condenação e por apenso ao processo principal.

3- Os liquidatários são sempre nomeados pelo juiz.

4- O Ministério Público requer as providências cautelares que se mostrem necessárias para garantir a liquidação.

Artigo 19º - Entrada em vigor

O presente diploma entra em vigor no prazo de 120 dias a contar da sua publicação.

Aprovada em 11 de Junho de 1991.

O Presidente da Assembleia da Republica, Vítor Pereira Crespo.

Promulgada em 26 de Julho de 1991.

Publique-se.

O Presidente da República, MÁRIO SOARES.

Referendada em 31 de Julho de 1991.

O Primeiro-Ministro, Aníbal António Cavaco Silva.

Anexo B - Lei nº 67/98 - Lei da Protecção de Dados Pessoais

Lei n.º 67/98 de 26 de Outubro

Lei da Protecção de Dados Pessoais (transpõe para a ordem jurídica portuguesa a Directiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados).

A Assembleia da República decreta, nos termos da alínea c) do artigo 161.º, das alíneas b) e c) do n.º 1 do artigo 165.º e do n.º 3 do artigo 166.º da Constituição, para valer como lei geral da República, o seguinte:

CAPÍTULO I

Disposições gerais

Artigo 1.º

Objecto

A presente lei transpõe para a ordem jurídica interna a Directiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Artigo 2.º

Princípio geral

O tratamento de dados pessoais deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais.

Artigo 3.º

Definições

Para efeitos da presente lei, entende-se por:

a) «Dados pessoais»: qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável a pessoa que possa ser identificada directa ou indirectamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social;

b) «Tratamento de dados pessoais» («tratamento»): qualquer operação ou conjunto de operações sobre dados pessoais, efectuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição;

c) «Ficheiro de dados pessoais» («ficheiro»): qualquer conjunto estruturado de dados pessoais, acessível segundo critérios determinados, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico;

d) «Responsável pelo tratamento»: a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais; sempre que as finalidades e os meios do tratamento sejam determinados por disposições legislativas ou regulamentares, o responsável pelo tratamento deve ser indicado na lei de organização e funcionamento ou no estatuto da entidade legal ou estatutariamente competente para tratar os dados pessoais em causa;

e) «Subcontratante»: a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que trate os dados pessoais por conta do responsável pelo tratamento;

f) «Terceiro»: a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que, não sendo o titular dos dados, o responsável pelo tratamento, o subcontratante ou outra pessoa sob autoridade directa do responsável pelo tratamento ou do subcontratante, esteja habilitado a tratar os dados;
g) «Destinatário»: a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo a quem sejam comunicados dados pessoais, independentemente de se tratar ou não de um terceiro, sem prejuízo de não serem consideradas destinatários as autoridades a quem sejam comunicados dados no âmbito de uma disposição legal;

h) «Consentimento do titular dos dados»: qualquer manifestação de vontade, livre, específica e informada, nos termos da qual o titular aceita que os seus dados pessoais sejam objecto de tratamento;

i) «Interconexão de dados»: forma de tratamento que consiste na possibilidade de relacionamento dos dados de um ficheiro com os dados de um ficheiro ou ficheiros mantidos por outro ou outros responsáveis, ou mantidos pelo mesmo responsável com outra finalidade.

Artigo 4.º

Âmbito de aplicação

1 – A presente lei aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros manuais ou a estes destinados.
2 – A presente lei não se aplica ao tratamento de dados pessoais efectuado por pessoa singular no exercício de actividades exclusivamente pessoais ou domésticas.
3 – A presente lei aplica-se ao tratamento de dados pessoais efectuado:
a) No âmbito das actividades de estabelecimento do responsável do tratamento situado em território português;

b) Fora do território nacional, em local onde a legislação portuguesa seja aplicável por força do direito internacional;

c) Por responsável que, não estando estabelecido no território da União Europeia, recorra, para tratamento de dados pessoais, a meios, automatizados ou não, situados no território português, salvo se esses meios só forem utilizados para trânsito através do território da União Europeia.

4 – A presente lei aplica-se à videovigilância e outras formas de captação, tratamento e difusão de sons e imagens que permitam identificar pessoas sempre que o responsável pelo tratamento esteja domiciliado ou sediado em Portugal ou utilize um fornecedor de acesso a redes informáticas e telemáticas estabelecido em território português.

5 – No caso referido na alínea c) do n.º 3, o responsável pelo tratamento deve designar, mediante comunicação à Comissão Nacional de Protecção de Dados (CNPD), um representante estabelecido em Portugal, que se lhe substitua em todos os seus direitos e obrigações, sem prejuízo da sua própria responsabilidade.

6 – O disposto no número anterior aplica-se no caso de o responsável pelo tratamento estar abrangido por estatuto de extraterritorialidade, de imunidade ou por qualquer outro que impeça o procedimento criminal.

7 – A presente lei aplica-se ao tratamento de dados pessoais que tenham por objectivo a segurança pública, a defesa nacional e a segurança do Estado, sem prejuízo do disposto em normas especiais constantes de instrumentos de direito internacional a que Portugal se vincule e de legislação específica atinente aos respectivos sectores.

CAPÍTULO II

Tratamento de dados pessoais

SECÇÃO I

Qualidade dos dados e legitimidade do seu tratamento

Artigo 5.º

Qualidade dos dados

1 – Os dados pessoais devem ser:

a) Tratados de forma lícita e com respeito pelo princípio da boa fé;

b) Recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser posteriormente tratados de forma incompatível com essas finalidades;

c) Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e posteriormente tratados;

d) Exactos e, se necessário, actualizados, devendo ser tomadas as medidas adequadas para assegurar que sejam apagados ou rectificados os dados inexactos ou incompletos, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente;

e) Conservados de forma a permitir a identificação dos seus titulares apenas durante o período necessário para a prossecução das finalidades da recolha ou do tratamento posterior.

2 – Mediante requerimento do responsável pelo tratamento, e caso haja interesse legítimo, a CNPD pode autorizar a conservação de dados para fins históricos, estatísticos ou científicos por período superior ao referido na alínea

e) do número anterior.

3 – Cabe ao responsável pelo tratamento assegurar a observância do disposto nos números anteriores.

Artigo 6.º

Condições de legitimidade do tratamento de dados
O tratamento de dados pessoais só pode ser efectuado se o seu titular tiver dado de forma inequívoca o seu consentimento ou se o tratamento for necessário para:

a) Execução de contrato ou contratos em que o titular dos dados seja parte ou de diligências prévias à formação do contrato ou declaração da vontade negocial efectuadas a seu pedido;

b) Cumprimento de obrigação legal a que o responsável pelo tratamento esteja sujeito;

c) Protecção de interesses vitais do titular dos dados, se este estiver física ou legalmente incapaz de dar o seu consentimento;

d) Execução de uma missão de interesse público ou no exercício de autoridade pública em que esteja investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados;

e) Prossecução de interesses legítimos do responsável pelo tratamento ou de terceiro a quem os dados sejam comunicados, desde que não devam prevalecer os interesses ou os direitos, liberdades e garantias do titular dos dados.

Artigo 7.º

Tratamento de dados sensíveis

1 – É proibido o tratamento de dados pessoais referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, bem como o tratamento de dados relativos à saúde e à vida sexual, incluindo os dados genéticos.

2 – Mediante disposição legal ou autorização da CNPD, pode ser permitido o tratamento dos dados referidos no número anterior quando por motivos de interesse público importante esse tratamento for indispensável ao exercício das atribuições legais ou estatutárias do seu responsável, ou quando o titular dos dados tiver dado o seu consentimento expresso para esse tratamento, em ambos os casos com garantias de não discriminação e com as medidas de segurança previstas no artigo 15.º

3 – O tratamento dos dados referidos no n.º 1 é ainda permitido quando se verificar uma das seguintes condições:

a) Ser necessário para proteger interesses vitais do titular dos dados ou de uma outra pessoa e o titular dos dados estiver física ou legalmente incapaz de dar o seu consentimento;

b) Ser efectuado, com o consentimento do titular, por fundação, associação ou organismo sem fins lucrativos de carácter político, filosófico, religioso ou sindical, no âmbito das suas actividades legítimas, sob condição de o tratamento respeitar apenas aos membros desse organismo ou às pessoas que com ele mantenham contactos periódicos ligados às suas finalidades, e de os dados não serem comunicados a terceiros sem consentimento dos seus titulares;

c) Dizer respeito a dados manifestamente tornados públicos pelo seu titular, desde que se possa legitimamente deduzir das suas declarações o consentimento para o tratamento dos mesmos;

d) Ser necessário à declaração, exercício ou defesa de um direito em processo judicial e for efectuado exclusivamente com essa finalidade.

4 – O tratamento dos dados referentes à saúde e à vida sexual, incluindo os dados genéticos, é permitido quando for necessário para efeitos de medicina preventiva, de diagnóstico médico, de prestação de cuidados ou tratamentos médicos ou de gestão de serviços de saúde, desde que o tratamento desses dados seja efectuado por um profissional de saúde obrigado a sigilo ou por outra pessoa sujeita igualmente a segredo profissional, seja notificado à CNPD,

nos termos do artigo 27.º, e sejam garantidas medidas adequadas de segurança da informação.

Artigo 8.º

Suspeitas de actividades ilícitas, infracções penais e contra-ordenações

1 – A criação e a manutenção de registos centrais relativos a pessoas suspeitas de actividades ilícitas, infracções penais, contra-ordenações e decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias só podem ser mantidas por serviços públicos com competência específica prevista na respectiva lei de organização e funcionamento, observando normas procedimentais e de protecção de dados previstas em diploma legal, com prévio parecer da CNPD.

2 – O tratamento de dados pessoais relativos a suspeitas de actividades ilícitas, infracções penais, contra-ordenações e decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias pode ser autorizado pela CNPD, observadas as normas de protecção de dados e de segurança da informação, quando tal tratamento for necessário à execução de finalidades legítimas do seu responsável, desde que não prevaleçam os direitos, liberdades e garantias do titular dos dados.

3 – O tratamento de dados pessoais para fins de investigação policial deve limitar-se ao necessário para a prevenção de um perigo concreto ou repressão de uma infracção determinada, para o exercício de competências previstas no respectivo estatuto orgânico ou noutra disposição legal e ainda nos termos de acordo ou convenção internacional de que Portugal seja parte.

Artigo 9.º

Interconexão de dados pessoais

1 – A interconexão de dados pessoais que não esteja prevista em disposição legal está sujeita a autorização da CNPD solicitada pelo responsável ou em conjunto pelos correspondentes responsáveis dos tratamentos, nos termos previstos no artigo 27.º

2 – A interconexão de dados pessoais deve ser adequada à prossecução das finalidades legais ou estatutárias e de interesses legítimos dos responsáveis dos tratamentos, não implicar discriminação ou diminuição dos direitos, liberdades e garantias dos titulares dos dados, ser rodeada de adequadas medidas de segurança e ter em conta o tipo de dados objecto de interconexão.

SECÇÃO II

Direitos do titular dos dados

Artigo 10.º

Direito de informação

1 – Quando recolher dados pessoais directamente do seu titular, o responsável pelo tratamento ou o seu representante deve prestar-lhe, salvo se já dele forem conhecidas, as seguintes informações:

a) Identidade do responsável pelo tratamento e, se for caso disso, do seu representante;

b) Finalidades do tratamento;

c) Outras informações, tais como:

Os destinatários ou categorias de destinatários dos dados;
O carácter obrigatório ou facultativo da resposta, bem como as possíveis consequências se não responder;

A existência e as condições do direito de acesso e de rectificação, desde que sejam necessárias, tendo em conta as circunstâncias específicas da recolha dos dados, para garantir ao seu titular um tratamento leal dos mesmos.

2 – Os documentos que sirvam de base à recolha de dados pessoais devem conter as informações constantes do número anterior.

3 – Se os dados não forem recolhidos junto do seu titular, e salvo se dele já forem conhecidas, o responsável pelo tratamento, ou o seu representante, deve prestar-lhe as informações previstas no n.º 1 no momento do registo dos dados ou, se estiver prevista a comunicação a terceiros, o mais tardar aquando da primeira comunicação desses dados.

4 – No caso de recolha de dados em redes abertas, o titular dos dados deve ser informado, salvo se disso já tiver conhecimento, de que os seus dados pessoais podem circular na rede sem condições de segurança, correndo o risco de serem vistos e utilizados por terceiros não autorizados.

5 – A obrigação de informação pode ser dispensada, mediante disposição legal ou deliberação da CNPD, por motivos de segurança do Estado e prevenção ou investigação criminal, e, bem assim, quando, nomeadamente no caso do

tratamento de dados com finalidades estatísticas, históricas ou de investigação científica, a informação do titular dos dados se revelar impossível ou implicar esforços desproporcionados ou ainda quando a lei determinar expressamente o registo dos dados ou a sua divulgação.

6 – A obrigação de informação, nos termos previstos no presente artigo, não se aplica ao tratamento de dados efectuado para fins exclusivamente jornalísticos ou de expressão artística ou literária.

Artigo 11.º

Direito de acesso

1 – O titular dos dados tem o direito de obter do responsável pelo tratamento, livremente e sem restrições, com periodicidade razoável e sem demoras ou custos excessivos:

a) A confirmação de serem ou não tratados dados que lhe digam respeito, bem como informação sobre as finalidades desse tratamento, as categorias de dados sobre que incide e os destinatários ou categorias de destinatários a quem são comunicados os dados;

b) A comunicação, sob forma inteligível, dos seus dados sujeitos a tratamento e de quaisquer informações disponíveis sobre a origem desses dados;

c) O conhecimento da lógica subjacente ao tratamento automatizado dos dados que lhe digam respeito;

d) A rectificação, o apagamento ou o bloqueio dos dados cujo tratamento não cumpra o disposto na presente lei, nomeadamente devido ao carácter incompleto ou inexacto desses dados;

e) A notificação aos terceiros a quem os dados tenham sido comunicados de qualquer rectificação, apagamento ou bloqueio efectuado nos termos da alínea d), salvo se isso for comprovadamente impossível.

2 – No caso de tratamento de dados pessoais relativos à segurança do Estado e à prevenção ou investigação criminal, o direito de acesso é exercido através da CNPD ou de outra autoridade independente a quem a lei atribua a verificação do cumprimento da legislação de protecção de dados pessoais.

3 – No caso previsto no n.º 6 do artigo anterior, o direito de acesso é exercido através da CNPD com salvaguarda das normas constitucionais aplicáveis, designadamente as que garantem a liberdade de expressão e informação, a liberdade de imprensa e a independência e sigilo profissionais dos jornalistas.

4 – Nos casos previstos nos n.os 2 e 3, se a comunicação dos dados ao seu titular puder prejudicar a segurança do Estado, a prevenção ou a investigação criminal ou ainda a liberdade de expressão e informação ou a liberdade de imprensa, a CNPD limita-se a informar o titular dos dados das diligências efectuadas.

5 – O direito de acesso à informação relativa a dados da saúde, incluindo os dados genéticos, é exercido por intermédio de médico escolhido pelo titular dos dados.

6 – No caso de os dados não serem utilizados para tomar medidas ou decisões em relação a pessoas determinadas, a lei pode restringir o direito de acesso nos casos em que manifestamente não exista qualquer perigo de violação dos direitos, liberdades e garantias do titular dos dados, designadamente do direito à vida privada, e os referidos dados forem exclusivamente utilizados para fins de investigação científica ou conservados sob forma de dados pessoais durante um período que não exceda o necessário à finalidade exclusiva de elaborar estatísticas.

Artigo 12.º

Direito de oposição do titular dos dados

O titular dos dados tem o direito de:

a) Salvo disposição legal em contrário, e pelo menos nos casos referidos nas alíneas d) e e) do artigo 6.º, se opor em qualquer altura, por razões ponderosas e legítimas relacionadas com a sua situação particular, a que os dados que lhe digam respeito sejam objecto de tratamento, devendo, em caso de oposição justificada, o tratamento efectuado pelo responsável deixar de poder incidir sobre esses dados;

b) Se opor, a seu pedido e gratuitamente, ao tratamento dos dados pessoais que lhe digam respeito previsto pelo responsável pelo tratamento para efeitos de marketing directo ou qualquer outra forma de prospecção, ou de ser informado, antes de os dados pessoais serem comunicados pela primeira vez a terceiros para fins de marketing directo ou utilizados por conta de terceiros, e de lhe ser expressamente facultado o direito de se opor, sem despesas, a tais comunicações ou utilizações.

Artigo 13.º

Decisões individuais automatizadas

1 – Qualquer pessoa tem o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afecte de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspectos da sua personalidade, designadamente a sua capacidade profissional, o seu crédito, a confiança de que é merecedora ou o seu comportamento.

2 – Sem prejuízo do cumprimento das restantes disposições da presente lei, uma pessoa pode ficar sujeita a uma decisão tomada nos termos do n.º 1, desde que tal ocorra no âmbito da celebração ou da execução de um contrato, e sob condição de o seu pedido de celebração ou execução do contrato ter sido satisfeito, ou de existirem medidas adequadas que garantam a defesa dos seus interesses legítimos, designadamente o seu direito de representação e expressão.

3 – Pode ainda ser permitida a tomada de uma decisão nos termos do n.º 1 quando a CNPD o autorize, definindo medidas de garantia da defesa dos interesses legítimos do titular dos dados.

SECÇÃO III

Segurança e confidencialidade do tratamento

Artigo 14.º

Segurança do tratamento

1 – O responsável pelo tratamento deve pôr em prática as medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito; estas medidas

devem assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger.
2 – O responsável pelo tratamento, em caso de tratamento por sua conta, deverá escolher um subcontratante que ofereça garantias suficientes em relação às medidas de segurança técnica e de organização do tratamento a efectuar, e deverá zelar pelo cumprimento dessas medidas.

3 – A realização de operações de tratamento em subcontratação deve ser regida por um contrato ou acto jurídico que vincule o subcontratante ao responsável pelo tratamento e que estipule, designadamente, que o subcontratante apenas actua mediante instruções do responsável pelo tratamento e que lhe incumbe igualmente o cumprimento das obrigações referidas no n.º 1.

4 – Os elementos de prova da declaração negocial, do contrato ou do acto jurídico relativos à protecção dos dados, bem como as exigências relativas às medidas referidas no n.º 1, são consignados por escrito em documento em suporte com valor probatório legalmente reconhecido.

Artigo 15.º

Medidas especiais de segurança

1 – Os responsáveis pelo tratamento dos dados referidos no n.º 2 do artigo 7.º e no n.º 1 do artigo 8.º devem tomar as medidas adequadas para:

a) Impedir o acesso de pessoa não autorizada às instalações utilizadas para o tratamento desses dados (controlo da entrada nas instalações);

b) Impedir que suportes de dados possam ser lidos, copiados, alterados ou retirados por pessoa não autorizada (controlo dos suportes de dados);

c) Impedir a introdução não autorizada, bem como a tomada de conhecimento, a alteração ou a eliminação não autorizadas de dados pessoais inseridos (controlo da inserção);

d) Impedir que sistemas de tratamento automatizados de dados possam ser utilizados por pessoas não autorizadas através de instalações de transmissão de dados (controlo da utilização);

e) Garantir que as pessoas autorizadas só possam ter acesso aos dados abrangidos pela autorização (controlo de acesso);

f) Garantir a verificação das entidades a quem possam ser transmitidos os dados pessoais através das instalações de transmissão de dados (controlo da transmissão);

g) Garantir que possa verificar-se a posteriori, em prazo adequado à natureza do tratamento, a fixar na regulamentação aplicável a cada sector, quais os dados pessoais introduzidos quando e por quem (controlo da introdução);

h) Impedir que, na transmissão de dados pessoais, bem como no transporte do seu suporte, os dados possam ser lidos, copiados, alterados ou eliminados de forma não autorizada (controlo do transporte).

2 – Tendo em conta a natureza das entidades responsáveis pelo tratamento e o tipo das instalações em que é efectuado, a CNPD pode dispensar a existência de certas medidas de segurança, garantido que se mostre o respeito pelos direitos, liberdades e garantias dos titulares dos dados.

3 – Os sistemas devem garantir a separação lógica entre os dados referentes à saúde e à vida sexual, incluindo os genéticos, dos restantes dados pessoais.

4 – A CNPD pode determinar que, nos casos em que a circulação em rede de dados pessoais referidos nos artigos 7.º e 8.º possa pôr em risco direitos, liberdades e garantias dos respectivos titulares, a transmissão seja cifrada.

Artigo 16.º

Tratamento por subcontratante

Qualquer pessoa que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, bem como o próprio subcontratante, tenha acesso a dados pessoais não pode proceder ao seu tratamento sem instruções do responsável pelo tratamento, salvo por força de obrigações legais.

Artigo 17.º

Sigilo profissional

1 – Os responsáveis do tratamento de dados pessoais, bem como as pessoas que, no exercício das suas funções, tenham conhecimento dos dados pessoais tratados, ficam obrigados a sigilo profissional, mesmo após o termo das suas funções.

2 – Igual obrigação recai sobre os membros da CNPD, mesmo após o termo do mandato.

3 – O disposto nos números anteriores não exclui o dever do fornecimento das informações obrigatórias, nos termos legais, excepto quando constem de ficheiros organizados para fins estatísticos.

4 – Os funcionários, agentes ou técnicos que exerçam funções de assessoria à CNPD ou aos seus vogais estão sujeitos à mesma obrigação de sigilo profissional.

CAPÍTULO III

Transferência de dados pessoais

SECÇÃO I

Transferência de dados pessoais na União Europeia

Artigo 18.º

Princípio

É livre a circulação de dados pessoais entre Estados membros da União Europeia, sem prejuízo do disposto nos actos comunitários de natureza fiscal e aduaneira.

SECÇÃO II

Transferência de dados pessoais para fora da União Europeia

Artigo 19.º

Princípios

1 – Sem prejuízo do disposto no artigo seguinte, a transferência, para um Estado que não pertença à União Europeia, de dados pessoais que sejam objecto de tratamento ou que se destinem a sê-lo só pode realizar-se com o respeito das disposições da presente lei e se o Estado para onde são transferidos assegurar um nível de protecção adequado.

2 – A adequação do nível de protecção num Estado que não pertença à União Europeia é apreciada em função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados; em especial, devem ser tidas em consideração a natureza dos dados, a finalidade e a duração do tratamento ou tratamentos projectados, os países de origem e de destino final, as regras de direito, gerais ou sectoriais, em vigor no Estado em causa, bem

como as regras profissionais e as medidas de segurança que são respeitadas nesse Estado.

3 – Cabe à CNPD decidir se um Estado que não pertença à União Europeia assegura um nível de protecção adequado.

4 – A CNPD comunica, através do Ministério dos Negócios Estrangeiros, à Comissão Europeia os casos em que tenha considerado que um Estado não assegura um nível de protecção adequado.

5 – Não é permitida a transferência de dados pessoais de natureza idêntica aos que a Comissão Europeia tiver considerado que não gozam de protecção adequada no Estado a que se destinam.

Artigo 20.º

Derrogações

1 – A transferência de dados pessoais para um Estado que não assegure um nível de protecção adequado na acepção do n.º 2 do artigo 19.º pode ser permitida pela CNPD se o titular dos dados tiver dado de forma inequívoca o seu consentimento à transferência ou se essa transferência:

a) For necessária para a execução de um contrato entre o titular dos dados e o responsável pelo tratamento ou de diligências prévias à formação do contrato decididas a pedido do titular dos dados;

b) For necessária para a execução ou celebração de um contrato celebrado ou a celebrar, no interesse do titular dos dados, entre o responsável pelo tratamento e um terceiro; ou

c) For necessária ou legalmente exigida para a protecção de um interesse público importante, ou para a declaração, o exercício ou a defesa de um direito num processo judicial; ou

d) For necessária para proteger os interesses vitais do titular dos dados; ou

e) For realizada a partir de um registo público que, nos termos de disposições legislativas ou regulamentares, se destine à informação do público e se encontre aberto à consulta do público em geral ou de qualquer pessoa que possa provar um interesse legítimo, desde que as condições estabelecidas na lei para a consulta sejam cumpridas no caso concreto.

2 – Sem prejuízo do disposto no n.º 1, a CNPD pode autorizar uma transferência ou um conjunto de transferências de dados pessoais para um Estado que não assegure um nível de protecção adequado na acepção do n.º 2 do artigo 19.º desde que o responsável pelo tratamento assegure mecanismos suficientes de garantia de protecção da vida privada e dos direitos e liberdades fundamentais das pessoas, bem como do seu exercício, designadamente, mediante cláusulas contratuais adequadas.

3 – A CNPD informa a Comissão Europeia, através do Ministério dos Negócios Estrangeiros, bem como as autoridades competentes dos restantes Estados da União Europeia, das autorizações que conceder nos termos do n.º 2.

4 – A concessão ou derrogação das autorizações previstas no n.º 2 efectua-se pela CNPD nos termos de processo próprio e de acordo com as decisões da Comissão Europeia.

5 – Sempre que existam cláusulas contratuais tipo aprovadas pela Comissão Europeia, segundo procedimento próprio, por oferecerem as garantias suficientes referidas no n.º 2, a CNPD autoriza a transferência de dados pessoais que se efectue ao abrigo de tais cláusulas.

6 – A transferência de dados pessoais que constitua medida necessária à protecção da segurança do Estado, da defesa, da segurança pública e da prevenção, investigação e repressão das infracções penais é regida por disposições legais específicas ou pelas convenções e acordos internacionais em que Portugal é parte.

CAPÍTULO IV

Comissão Nacional de Protecção de Dados

SECÇÃO I

Natureza, atribuições e competências

Artigo 21.º

Natureza

1 – A CNPD é uma entidade administrativa independente, com poderes de autoridade, que funciona junto da Assembleia da República.

2 – A CNPD, independentemente do direito nacional aplicável a cada tratamento de dados em concreto, exerce as suas competências em todo o território nacional.

3 – A CNPD pode ser solicitada a exercer os seus poderes por uma autoridade de controlo de protecção de dados de outro Estado membro da União Europeia ou do Conselho da Europa.

4 – A CNPD coopera com as autoridades de controlo de protecção de dados de outros Estados na difusão do direito e das regulamentações nacionais em matéria de protecção de dados pessoais, bem como na defesa e no exercício dos direitos de pessoas residentes no estrangeiro.

Artigo 22.º

Atribuições

1 – A CNPD é a autoridade nacional que tem como atribuição controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de protecção de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei.

2 – A CNPD deve ser consultada sobre quaisquer disposições legais, bem como sobre instrumentos jurídicos em preparação em instituições comunitárias ou internacionais, relativos ao tratamento de dados pessoais.

3 – A CNPD dispõe:

a) De poderes de investigação e de inquérito, podendo aceder aos dados objecto de tratamento e recolher todas as informações necessárias ao desempenho das suas funções de controlo;

b) De poderes de autoridade, designadamente o de ordenar o bloqueio, apagamento ou destruição dos dados, bem como o de proibir, temporária ou definitivamente, o tratamento de dados pessoais, ainda que incluídos em redes abertas de transmissão de dados a partir de servidores situados em território português;

c) Do poder de emitir pareceres prévios ao tratamento de dados pessoais, assegurando a sua publicitação.

4 – Em caso de reiterado não cumprimento das disposições legais em matéria de dados pessoais, a CNPD pode advertir ou censurar publicamente o responsável pelo tratamento, bem como suscitar a questão, de acordo com as

respectivas competências, à Assembleia da República, ao Governo ou a outros órgãos ou autoridades.

5 – A CNPD tem legitimidade para intervir em processos judiciais no caso de violação das disposições da presente lei e deve denunciar ao Ministério Público as infracções penais de que tiver conhecimento, no exercício das suas funções e por causa delas, bem como praticar os actos cautelares necessários e urgentes para assegurar os meios de prova.

6 – A CNPD é representada em juízo pelo Ministério Público e está isenta de custas nos processos em que intervenha.

Artigo 23.º

Competências

1 – Compete em especial à CNPD:

a) Emitir parecer sobre disposições legais, bem como sobre instrumentos jurídicos em preparação em instituições comunitárias e internacionais, relativos ao tratamento de dados pessoais;

b) Autorizar ou registar, consoante os casos, os tratamentos de dados pessoais;

c) Autorizar excepcionalmente a utilização de dados pessoais para finalidades não determinantes da recolha, com respeito pelos princípios definidos no artigo 5.º;

d) Autorizar, nos casos previstos no artigo 9.º, a interconexão de tratamentos automatizados de dados pessoais;

e) Autorizar a transferência de dados pessoais nos casos previstos no artigo 20.º;

f) Fixar o tempo da conservação dos dados pessoais em função da finalidade, podendo emitir directivas para determinados sectores de actividade;

g) Fazer assegurar o direito de acesso à informação, bem como do exercício do direito de rectificação e actualização;

h) Autorizar a fixação de custos ou de periodicidade para o exercício do direito de acesso, bem como fixar os prazos máximos de cumprimento, em cada sector de actividade, das obrigações que, por força dos artigos 11.º a 13.º, incumbem aos responsáveis pelo tratamento de dados pessoais;

i) Dar seguimento ao pedido efectuado por qualquer pessoa, ou por associação que a represente, para protecção dos seus direitos e liberdades no que diz respeito ao tratamento de dados pessoais e informá-la do resultado;

j) Efectuar, a pedido de qualquer pessoa, a verificação de licitude de um tratamento de dados, sempre que esse tratamento esteja sujeito a restrições de acesso ou de informação, e informá-la da realização da verificação;

k) Apreciar as reclamações, queixas ou petições dos particulares;

l) Dispensar a execução de medidas de segurança, nos termos previstos no n.º 2 do artigo 15.º, podendo emitir directivas para determinados sectores de actividade;

m) Assegurar a representação junto de instâncias comuns de controlo e em reuniões comunitárias e internacionais de entidades independentes de controlo da protecção de dados pessoais, bem como participar em reuniões internacionais no âmbito das suas competências, designadamente exercer funções de representação e fiscalização no âmbito dos sistemas Schengen e Europol, nos termos das disposições aplicáveis;

n) Deliberar sobre a aplicação de coimas;

o) Promover e apreciar códigos de conduta;

p) Promover a divulgação e esclarecimento dos direitos relativos à protecção de dados e dar publicidade periódica à sua actividade, nomeadamente através da publicação de um relatório anual;

q) Exercer outras competências legalmente previstas.

2 – No exercício das suas competências de emissão de directivas ou de apreciação de códigos de conduta, a CNPD deve promover a audição das associações de defesa dos interesses em causa.

3 – No exercício das suas funções, a CNPD profere decisões com força obrigatória, passíveis de reclamação e de recurso para o Tribunal Central Administrativo.

4 – A CNPD pode sugerir à Assembleia da República as providências que entender úteis à prossecução das suas atribuições e ao exercício das suas competências.

Artigo 24.º

Dever de colaboração

1 – As entidades públicas e privadas devem prestar a sua colaboração à CNPD, facultando-lhe todas as informações que por esta, no exercício das suas competências, lhes forem solicitadas.

2 – O dever de colaboração é assegurado, designadamente, quando a CNPD tiver necessidade, para o cabal exercício das suas funções, de examinar o sistema informático e os ficheiros de dados pessoais, bem como toda a documentação relativa ao tratamento e transmissão de dados pessoais.

3 – A CNPD ou os seus vogais, bem como os técnicos por ela mandatados, têm direito de acesso aos sistemas informáticos que sirvam de suporte ao tratamento dos dados, bem como à documentação referida no número anterior, no âmbito das suas atribuições e competências.

SECÇÃO II

Composição e funcionamento

Artigo 25.º

Composição e mandato

1 – A CNPD é composta por sete membros de integridade e mérito reconhecidos, dos quais o presidente e dois dos vogais são eleitos pela Assembleia da República segundo o método da média mais alta de Hondt.

2 – Os restantes vogais são:

a) Dois magistrados com mais de 10 anos de carreira, sendo um magistrado judicial, designado pelo Conselho Superior da Magistratura, e um magistrado do Ministério Público, designado pelo Conselho Superior do Ministério Público;

b) Duas personalidades de reconhecida competência designadas pelo Governo.

3 – O mandato dos membros da CNPD é de cinco anos e cessa com a posse dos novos membros.

4 – Os membros da CNPD constam de lista publicada na 1.ª série do Diário da República.

5 – Os membros da CNPD tomam posse perante o Presidente da Assembleia da República nos 10 dias seguintes à publicação da lista referida no número anterior.

Artigo 26.º

Funcionamento

1 – São aprovados por lei da Assembleia da República:

a) A lei orgânica e o quadro de pessoal da CNPD;

b) O regime de incompatibilidades, de impedimentos, de suspeições e de perda de mandato, bem como o estatuto remuneratório dos membros da CNPD.

2 – O estatuto dos membros da CNPD garante a independência do exercício das suas funções.

3 – A Comissão dispõe de quadro próprio para apoio técnico e administrativo, beneficiando os seus funcionários e agentes do estatuto e regalias do pessoal da Assembleia da República.

SECÇÃO III

Notificação

Artigo 27.º

Obrigação de notificação à CNPD

1 – O responsável pelo tratamento ou, se for caso disso, o seu representante deve notificar a CNPD antes da realização de um tratamento ou conjunto de tratamentos, total ou parcialmente autorizados, destinados à prossecução de uma ou mais finalidades interligadas.

2 – A CNPD pode autorizar a simplificação ou a isenção da notificação para determinadas categorias de tratamentos que, tendendo aos dados a tratar, não sejam susceptíveis de pôr em causa os direitos e liberdades dos titulares dos dados e tenham em conta critérios de celeridade, economia e eficiência.

3 – A autorização, que está sujeita a publicação no Diário da República, deve especificar as finalidades do tratamento, os dados ou categorias de dados a tratar, a categoria ou categorias de titulares dos dados, os destinatários ou categorias de destinatários a quem podem ser comunicados os dados e o período de conservação dos dados.

4 – Estão isentos de notificação os tratamentos cuja única finalidade seja a manutenção de registos que, nos termos de disposições legislativas ou regulamentares, se destinem a informação do público e possam ser consultados pelo público em geral ou por qualquer pessoa que provar um interesse legítimo.

5 – Os tratamentos não automatizados dos dados pessoais previstos no n.º 1 do artigo 7.º estão sujeitos a notificação quando tratados ao abrigo da alínea a) do n.º 3 do mesmo artigo.

Artigo 28.º

Controlo prévio

1 – Carecem de autorização da CNPD:

a) O tratamento dos dados pessoais a que se referem o n.º 2 do artigo 7.º e o n.º 2 do artigo 8.º;

b) O tratamento dos dados pessoais relativos ao crédito e à solvabilidade dos seus titulares;

c) A interconexão de dados pessoais prevista no artigo 9.º;

d) A utilização de dados pessoais para fins não determinantes da recolha.

2 – Os tratamentos a que se refere o número anterior podem ser autorizados por diploma legal, não carecendo neste caso de autorização da CNPD.

Artigo 29.º

Conteúdo dos pedidos de parecer ou de autorização e da notificação
Os pedidos de parecer ou de autorização, bem como as notificações, remetidos à CNPD devem conter as seguintes informações:

a) Nome e endereço do responsável pelo tratamento e, se for o caso, do seu representante;

b) As finalidades do tratamento;

c) Descrição da ou das categorias de titulares dos dados e dos dados ou categorias de dados pessoais que lhes respeitem;

d) Destinatários ou categorias de destinatários a quem os dados podem ser comunicados e em que condições;

e) Entidade encarregada do processamento da informação, se não for o próprio responsável do tratamento;

f) Eventuais interconexões de tratamentos de dados pessoais;

g) Tempo de conservação dos dados pessoais;

h) Forma e condições como os titulares dos dados podem ter conhecimento ou fazer corrigir os dados pessoais que lhes respeitem;

i) Transferências de dados previstas para países terceiros;

j) Descrição geral que permita avaliar de forma preliminar a adequação das medidas tomadas para garantir a segurança do tratamento em aplicação dos artigos 14.º e 15.º

Artigo 30.º

Indicações obrigatórias

1 – Os diplomas legais referidos no n.º 2 do artigo 7.º e no n.º 1 do artigo 8.º, bem como as autorizações da CNPD e os registos de tratamentos de dados pessoais, devem, pelo menos, indicar:

a) O responsável do ficheiro e, se for caso disso, o seu representante;

b) As categorias de dados pessoais tratados;

c) As finalidades a que se destinam os dados e as categorias de entidades a quem podem ser transmitidos;

d) A forma de exercício do direito de acesso e de rectificação;

e) Eventuais interconexões de tratamentos de dados pessoais;

f) Transferências de dados previstas para países terceiros.

2 – Qualquer alteração das indicações constantes do n.º 1 está sujeita aos procedimentos previstos nos artigos 27.º e 28.º

Artigo 31.º

Publicidade dos tratamentos

1 – O tratamento dos dados pessoais, quando não for objecto de diploma legal e dever ser autorizado ou notificado, consta de registo na CNPD, aberto à consulta por qualquer pessoa.

2 – O registo contém as informações enumeradas nas alíneas a) a d) e i) do artigo 29.º

3 – O responsável por tratamento de dados não sujeito a notificação está obrigado a prestar, de forma adequada, a qualquer pessoa que lho solicite, pelo menos as informações referidas no n.º 1 do artigo 30.º

4 – O disposto no presente artigo não se aplica a tratamentos cuja única finalidade seja a manutenção de registos que, nos termos de disposições legislativas ou regulamentares, se destinem à informação do público e se encontrem abertos à consulta do público em geral ou de qualquer pessoa que possa provar um interesse legítimo.

5 – A CNPD deve publicar no seu relatório anual todos os pareceres e autorizações elaborados ou concedidas ao abrigo da presente lei, designadamente as autorizações previstas no n.º 2 do artigo 7.º e no n.º 2 do artigo 9.º

CAPÍTULO V

Códigos de conduta

Artigo 32.º

Códigos de conduta

1 – A CNPD apoia a elaboração de códigos de conduta destinados a contribuir, em função das características dos diferentes sectores, para a boa execução das disposições da presente lei.

2 – As associações profissionais e outras organizações representativas de categorias de responsáveis pelo tratamento de dados que tenham elaborado projectos de códigos de conduta podem submetê-los à apreciação da CNPD.

3 – A CNPD pode declarar a conformidade dos projectos com as disposições legais e regulamentares vigentes em matéria de protecção de dados pessoais.

CAPÍTULO VI

Tutela administrativa e jurisdicional

SECÇÃO I

Tutela administrativa e jurisdicional

Artigo 33.º

Tutela administrativa e jurisdicional

Sem prejuízo do direito de apresentação de queixa à CNPD, qualquer pessoa pode, nos termos da lei, recorrer a meios administrativos ou jurisdicionais para garantir o cumprimento das disposições legais em matéria de protecção de dados pessoais.

Artigo 34.º

Responsabilidade civil

1 – Qualquer pessoa que tiver sofrido um prejuízo devido ao tratamento ilícito de dados ou a qualquer outro acto que viole disposições legais em matéria de protecção de dados pessoais tem o direito de obter do responsável a reparação pelo prejuízo sofrido.

2 – O responsável pelo tratamento pode ser parcial ou totalmente exonerado desta responsabilidade se provar que o facto que causou o dano lhe não é imputável.

SECÇÃO II

Contra-ordenações

Artigo 35.º

Legislação subsidiária

Às infracções previstas na presente secção é subsidiariamente aplicável o regime geral das contra-ordenações, com as adaptações constantes dos artigos seguintes.

Artigo 36.º

Cumprimento do dever omitido

Sempre que a contra-ordenação resulte de omissão de um dever, a aplicação da sanção e o pagamento da coima não dispensam o infractor do seu cumprimento, se este ainda for possível.

Artigo 37.º

Omissão ou defeituoso cumprimento de obrigações

1 – As entidades que, por negligência, não cumpram a obrigação de notificação à CNPD do tratamento de dados pessoais a que se referem os n.os 1 e 5 do artigo 27.º, prestem falsas informações ou cumpram a obrigação de notificação com inobservância dos termos previstos no artigo 29.º, ou ainda quando, depois de notificadas pela CNPD, mantiverem o acesso às redes abertas de transmissão de dados a responsáveis por tratamento de dados pessoais que não cumpram as disposições da presente lei, praticam contra-ordenação punível com as seguintes coimas:

a) Tratando-se de pessoa singular, no mínimo de 50000$00 e no máximo de 500000$00;

b) Tratando-se de pessoa colectiva ou de entidade sem personalidade jurídica, no mínimo de 300000$00 e no máximo de 3000000$00.

2 – A coima é agravada para o dobro dos seus limites quando se trate de dados sujeitos a controlo prévio, nos termos do artigo 28.º

Artigo 38.º

Contra-ordenações

1 – Praticam contra-ordenação punível com a coima mínima de 100000$00 e máxima de 1000000$00, as entidades que não cumprirem alguma das seguintes disposições da presente lei:

a) Designar representante nos termos previstos no n.º 5 do artigo 4.º;

b) Observar as obrigações estabelecidas nos artigos 5.º, 10.º, 11.º, 12.º, 13.º, 15.º, 16.º e 31.º, n.º 3.

2 – A pena é agravada para o dobro dos seus limites quando não forem cumpridas as obrigações constantes dos artigos 6.º, 7.º, 8.º, 9.º, 19.º e 20.º

Artigo 39.º

Concurso de infracções

1 – Se o mesmo facto constituir, simultaneamente, crime e contra-ordenação, o agente é punido sempre a título de crime.

2 – As sanções aplicadas às contra-ordenações em concurso são sempre cumuladas materialmente.

Artigo 40.º

Punição de negligência e da tentativa

1 – A negligência é sempre punida nas contra-ordenações previstas no artigo 38.º

2 – A tentativa é sempre punível nas contra-ordenações previstas nos artigos 37.º e 38.º

Artigo 41.º

Aplicação das coimas

1 – A aplicação das coimas previstas na presente lei compete ao presidente da CNPD, sob prévia deliberação da Comissão.

2 – A deliberação da CNPD, depois de homologada pelo presidente, constitui título executivo, no caso de não ser impugnada no prazo legal.

Artigo 42.º

Destino das receitas cobradas

O montante das importâncias cobradas, em resultado da aplicação das coimas, reverte, em partes iguais, para o Estado e para a CNPD.

SECÇÃO III

Crimes

Artigo 43.º

Não cumprimento de obrigações relativas a protecção de dados

1 – É punido com prisão até um ano ou multa até 120 dias quem intencionalmente:

a) Omitir a notificação ou o pedido de autorização a que se referem os artigos 27.º e 28.º;

b) Fornecer falsas informações na notificação ou nos pedidos de autorização para o tratamento de dados pessoais ou neste proceder a modificações não consentidas pelo instrumento de legalização;

c) Desviar ou utilizar dados pessoais, de forma incompatível com a finalidade determinante da recolha ou com o instrumento de legalização;

d) Promover ou efectuar uma interconexão ilegal de dados pessoais;

e) Depois de ultrapassado o prazo que lhes tiver sido fixado pela CNPD para cumprimento das obrigações previstas na presente lei ou em outra legislação de protecção de dados, as não cumprir;

f) Depois de notificado pela CNPD para o não fazer, mantiver o acesso a redes abertas de transmissão de dados a responsáveis pelo tratamento de dados pessoais que não cumpram as disposições da presente lei.

2 – A pena é agravada para o dobro dos seus limites quando se tratar de dados pessoais a que se referem os artigos 7.º e 8.º

Artigo 44.º

Acesso indevido

1 – Quem, sem a devida autorização, por qualquer modo, aceder a dados pessoais cujo acesso lhe está vedado é punido com prisão até um ano ou multa até 120 dias.

2 – A pena é agravada para o dobro dos seus limites quando o acesso:

a) For conseguido através de violação de regras técnicas de segurança;

b) Tiver possibilitado ao agente ou a terceiros o conhecimento de dados pessoais;

c) Tiver proporcionado ao agente ou a terceiros benefício ou vantagem patrimonial.

3 – No caso do n.º 1 o procedimento criminal depende de queixa.

Artigo 45.º

Viciação ou destruição de dados pessoais

1 – Quem, sem a devida autorização, apagar, destruir, danificar, suprimir ou modificar dados pessoais, tornando-os inutilizáveis ou afectando a sua capacidade de uso, é punido com prisão até dois anos ou multa até 240 dias.

2 – A pena é agravada para o dobro nos seus limites se o dano produzido for particularmente grave.

3 – Se o agente actuar com negligência, a pena é, em ambos os casos, de prisão até um ano ou multa até 120 dias.

Artigo 46.º

Desobediência qualificada

1 – Quem, depois de notificado para o efeito, não interromper, cessar ou bloquear o tratamento de dados pessoais é punido com a pena correspondente ao crime de desobediência qualificada.

2 – Na mesma pena incorre quem, depois de notificado:

a) Recusar, sem justa causa, a colaboração que concretamente lhe for exigida nos termos do artigo 24.º;

b) Não proceder ao apagamento, destruição total ou parcial de dados pessoais;

c) Não proceder à destruição de dados pessoais, findo o prazo de conservação previsto no artigo 5.º

Artigo 47.º

Violação do dever de sigilo

1 – Quem, obrigado a sigilo profissional, nos termos da lei, sem justa causa e sem o devido consentimento, revelar ou divulgar no todo ou em parte dados pessoais é punido com prisão até dois anos ou multa até 240 dias.

2 – A pena é agravada de metade dos seus limites se o agente:

a) For funcionário público ou equiparado, nos termos da lei penal;

b) For determinado pela intenção de obter qualquer vantagem patrimonial ou outro benefício ilegítimo;

c) Puser em perigo a reputação, a honra e consideração ou a intimidade da vida privada de outrem.

3 – A negligência é punível com prisão até seis meses ou multa até 120 dias.

4 – Fora dos casos previstos no n.º 2, o procedimento criminal depende de queixa.

Artigo 48.º

Punição da tentativa

Nos crimes previstos nas disposições anteriores, a tentativa é sempre punível.

Artigo 49.º

Pena acessória

1 – Conjuntamente com as coimas e penas aplicadas pode, acessoriamente, ser ordenada:

a) A proibição temporária ou definitiva do tratamento, o bloqueio, o apagamento ou a destruição total ou parcial dos dados;

b) A publicidade da sentença condenatória;

c) A advertência ou censura públicas do responsável pelo tratamento, nos termos do n.º 4 do artigo 22.º

2 – A publicidade da decisão condenatória faz-se a expensas do condenado, na publicação periódica de maior expansão editada na área da comarca da prática da infracção ou, na sua falta, em publicação periódica da comarca mais próxima, bem como através da afixação de edital em suporte adequado, por período não inferior a 30 dias.

3 – A publicação é feita por extracto de que constem os elementos da infracção e as sanções aplicadas, bem como a identificação do agente.

CAPÍTULO VII

Disposições finais

Artigo 50.º

Disposição transitória

1 – Os tratamentos de dados existentes em ficheiros manuais à data da entrada em vigor da presente lei devem cumprir o disposto nos artigos 7.º, 8.º, 10.º e 11.º no prazo de cinco anos.

2 – Em qualquer caso, o titular dos dados pode obter, a seu pedido e, nomeadamente, aquando do exercício do direito de acesso, a rectificação, o apagamento ou o bloqueio dos dados incompletos, inexactos ou conservados de modo incompatível com os fins legítimos prosseguidos pelo responsável pelo tratamento.

3 – A CNPD pode autorizar que os dados existentes em ficheiros manuais e conservados unicamente com finalidades de investigação histórica não tenham que cumprir os artigos 7.º, 8.º e 9.º, desde que não sejam em nenhum caso reutilizados para finalidade diferente.

Artigo 51.º

Disposição revogatória

São revogadas as Leis n.os 10/91, de 29 de Abril, e 28/94, de 29 de Agosto.

Artigo 52.º

Entrada em vigor

A presente lei entra em vigor no dia seguinte ao da sua publicação. Aprovada em 24 de Setembro de 1998.

O Presidente da Assembleia da República, António de Almeida Santos. Promulgada em 7 de Outubro de 1998.

Publique-se.

O Presidente da República, JORGE SAMPAIO.

Referendada em 14 de Outubro de 1998.

O Primeiro-Ministro, António Manuel de Oliveira Guterres.