

compilações doutrinais

VERBOJURIDICO

BREVE INTRODUÇÃO DA QUESTÃO DA
INVESTIGAÇÃO E MEIOS DE PROVA
NA CRIMINALIDADE INFORMÁTICA

DR. PEDRO DIAS VENÂNCIO

ADVOGADO

DOCENTE CONVIDADO DO INSTITUTO POLITÉCNICO DO CÁVADO E DO AVE



verbojuridico[®]

DEZEMBRO 2006

Título: **INVESTIGAÇÃO E MEIOS DE PROVA NA CRIMINALIDADE INFORMÁTICA**

Autor: Dr. PEDRO DIAS VENÂNCIO
Advogado e Docente Convidado do Instituto Politécnico do Cávado e do Ave

Data de Publicação: Dezembro de 2006

Classificação: Direito Penal
Direito das Novas Tecnologias. Informática e Internet.

Edição: Verbo Jurídico © - www.verbojuridico.pt | .eu | .net | .org | .com.

Nota Legal: Respeite os direitos de autor. É permitida a reprodução exclusivamente para fins pessoais ou académicos. É proibida a reprodução ou difusão com efeitos comerciais, assim como a eliminação da formatação, das referências à autoria e publicação. Exceptua-se a transcrição de curtas passagens, desde que mencionado o título da obra, o nome do autor e da referência de publicação.



Ficheiro formatado para ser amigo do ambiente. Se precisar de imprimir este documento, sugerimos que o efective frente e verso, assim reduzindo a metade o número de folhas, com benefício para o ambiente. Imprima em primeiro as páginas pares invertendo a ordem de impressão (do fim para o princípio). Após, insira novamente as folhas impressas na impressora e imprima as páginas ímpares pela ordem normal (princípio para o fim).

SUMÁRIO

	Pág.
- Introdução	5
- Capítulo I (Direito Penal da Informática)	7
- Secção I (Introdução)	7
- Secção II (Critérios de aplicabilidade)	8
- Secção III (Crimes informáticos previstos no Código Penal)	9
- Subsecção I (Devassa por meio informático)	9
- Subsecção II (Violação de correspondência ou de telecomunicações)	10
- Subsecção III (Burla informática e nas telecomunicações)	11
- Secção IV (Crimes informáticos previstos na Lei da Criminalidade Informática)	11
- Subsecção I (Falsidade informática)	11
- Subsecção II (Dano relativo a dados ou programas informáticos)	12
- Subsecção III (Sabotagem informática)	12
- Subsecção IV (Acesso ilegítimo)	13
- Subsecção V (Intercepção ilegítima)	14
- Subsecção VI (Reprodução ilegítima de programa protegido)	15
- Capítulo II (Convenção sobre cibercriminalidade)	15
- Secção I (Introdução)	15
- Secção II (Medidas a tomar a nível nacional)	16
- Subsecção I (Medidas ao nível do direito penal processual)	17
- Secção III (Cooperação internacional)	19
- Subsecção I (Disposições específicas)	19
- Capítulo III (Meios de prova em ambiente digital no ordenamento português) .	20
- Secção I (Inexistência de um regime próprio)	20
- Secção II (Aplicação das regras gerais do processo penal)	21
- Subsecção I (A prova pericial)	21
- Subsecção II (Intercepção de comunicações)	22
- Subsecção III (Apreensão de correspondência)	23
- Subsecção IV (Outras disposições)	24
- Conclusão	24
- Fontes e bibliografia	27
- Anexos	28

**BREVE INTRODUÇÃO À QUESTÃO DA
INVESTIGAÇÃO E MEIOS DE PROVA
NA CRIMINALIDADE INFORMÁTICA**

Dr. Pedro Dias Venâncio
ADVOGADO
DOCENTE CONVIDADO DO IPCA ^(*)

Introdução

O presente artigo insere-se no interesse do autor pela interacção entre o “Direito” e a “Sociedade da Informação”, e resulta da investigação desenvolvida no âmbito da disciplina de «Investigação e meios de prova na Criminalidade informática» do Curso de Mestrado e Doutoramento em Direito Comercial da Faculdade de Direito da Universidade Católica Portuguesa – Centro Regional do Porto.

A sociedade da informação, nomeadamente a “Internet” ¹, surgiu como um campo de liberdade à margem do direito. No entanto, a crescente importância social, cultural e económica que rapidamente assumiu a nível mundial não podia deixar o Direito alheado desta realidade.

A primeira questão que obviamente se colocou era a da aplicabilidade do direito aos actos electrónicos, o que desde sempre levantou diversos problemas de competência territorial, de ausência de previsão legal dos seus mecanismos, de novas realidades dificilmente enquadráveis nos mecanismos legais existentes.

(*) O Autor, Dr. Pedro Dias Venâncio é Advogado com a cédula 7332p e escritório na Comarca da Maia e Docente convidado do Instituto Politécnico do Cávado e do Ave.
Contactos do Autor: pvenancio@ipca.pt / pdvenancio@advogadosportugal.com.pt

¹ **Internet:** Teve início em meados de 1969 pelo Departamento de Defesa dos EUA. É a interligação de computadores das mais variadas regiões geográficas numa mesma rede, possibilitando a comunicação em tempo real entre estes. A Internet é agora um conjunto em permanente expansão de redes de computadores, ao nível mundial, formada por servidores ou hosts, interligados por uma rede remota e utilizando um protocolo comum de comunicação (TCP/IP – transmission control protocol/Internet protocol) que lhes permite a disponibilização de toda a panóplia de serviços comuns – email, ftp, newsgroups, chat, etc...

Mais relevante se torna a questão quando os meios electrónicos são utilizados para a prática de actos criminosos, atentas as especificidades que esta realidade tecnológica, em permanente evolução e expansão, levantam ao direito penal e processual penal.

Desde logo, as práticas e potencialidades informáticas, quer pela utilização da “Internet” quer através de “Intranet”², potenciam exponencialmente a internacionalização da criminalidade informática, tornando mais difícil a reconstituição do percurso das informações entre o ponto emissor e o ponto receptor, permitindo a dissimulação dos intervenientes.

Estas “facilidades” têm gerado, por um lado, uma deslocação criminosa para a Internet, fazendo com que cada vez mais pessoas se sintam tentadas a utilizar a Internet para as suas práticas criminosas, ou mesmo a arriscar-se na consumação de crimes que por outros meios não praticariam. Por outro, uma deslocação criminosa na Internet, ou seja, detectado um ponto emissor de práticas criminosas, ainda que as autoridades encerrem esse ponto (site ou e-mail³) é extremamente simples transferir a informação para outro ponto na Internet, eventualmente noutro país, fugindo à competência “territorial” da lei e ao “braço” das autoridades.

Por outro lado, dia para dia, apuram-se novas técnicas de dissimulação ou ocultação em meios digitais que dificultam a identificação do agente das actividades criminosas por parte das autoridades.

Toda esta nova tecnologia, e a dificuldade da pesada máquina estatal em acompanhar esta evolução, têm gerado uma generalizada desadequação do direito e processo penais ao combate eficaz da criminalidade informática, não só em Portugal, como na generalidade dos países ocidentais. Desde logo, porque as normas substantivas assentam na territorialidade e materialidade da prática dos crimes, não se coadunando com o carácter transfronteiriço e virtual dos actos praticados na Internet.

² **Intranet:** Rede interna e privativa de informações baseada na tecnologia da Internet. É usada por qualquer tipo de organizações (empresa, entidade ou órgão público) que deseje compartilhar informações apenas entre os seus utilizadores registados, sem permitir o acesso de outras pessoas.

³ **Endereço electrónico:** identificação de um equipamento informático adequado para receber e arquivar documentos electrónicos (artigo 2º do Decreto-Lei n.º 290-D/99, de 2 de Agosto).

Garcia Marques e Lourenço Martins⁴, falam em Criminalidade Informática como “*todo o acto em que o computador serve de meio para atingir um objectivo criminoso ou em que o computador é o alvo desse acto*”.

O tema é vasto, pelo que nos atenderemos neste trabalho apenas à “criminalidade informática propriamente dita”, entendendo esta como aquela em que a utilização dos meios electrónicos não é apenas um meio distinto para a prática que um crime comum, mas um elemento próprio do tipo de crime.

A legislação internacional, comunitária e nacional tem já, no essencial, caracterizado os tipos de crimes específicos do ambiente digital. A questão que continua por resolver é a investigação e obtenção de prova da prática destes crimes.

CAPÍTULO I

Direito Penal da Informática

Secção I - Introdução

O código penal desde cedo previu a possibilidade de crimes especificamente praticados por meios informáticos, no entanto, só com a publicação da Lei da Criminalidade Informática (Lei 109/91 de 17 de Agosto) se veio completar de modo abrangente o leque de crimes informáticos em sentido estrito.

Assim, é no próprio Código Penal que encontraremos os critérios essenciais de aplicabilidade do direito penal português aos actos informáticos, encontrando aí também a tipificação dos crimes de «Devassa por meio informático», «Violação de correspondência e telecomunicações», e «Burla informática e nas telecomunicações».

Na Lei 109/91, de 17 de Agosto, tipificam-se mais cinco crimes informáticos em sentido estrito: «Falsidade informática», «Sabotagem informática», «Acesso ilegítimo», «Intercepção ilegítima» e «Reprodução ilegítima de programa protegido».

⁴ - MARTINS, A. G. Lourenço, “Criminalidade Informática”, artigo publicado em Direito da Sociedade da Informação, Volume IV, APDI, Coimbra Editora, 2003;

Faremos então, seguidamente, uma análise sucinta destes critérios de aplicabilidade e dos tipos legais supra referenciados.

Secção II - Critérios de aplicabilidade

Começemos por verificar em que circunstâncias podemos considerar que determinado crime informático é punível em Portugal.

O artigo 4º do Código Penal estabelece como regra geral o princípio da territorialidade: «*Salvo tratado ou convenção internacional em contrário, a lei penal portuguesa é aplicável aos factos praticados: a) em território português, seja qual for a nacionalidade do agente; ou b) a bordo de navios ou aeronaves portuguesas.*»

Vemos facilmente aqui a dificuldade de aplicação deste conceito puro de territorialidade aos crimes praticados através da Internet. Desde logo, coloca-se a dúvida de saber se o local do crime é o país onde está instalado o servidor⁵ que contém a informação, ou o país onde reside o agente que coloca a informação naquele servidor, no caso de divergir.

O artigo 7º do Código Penal ajuda-nos a resolver esta questão, pois vem estabelecer que: «o facto considera-se praticado tanto no lugar em que total ou parcialmente, e sob qualquer forma de participação, o agente actuou, ou no caso de omissão, devia ter actuado, como naquele em que o resultado típico se tiver produzido.»

Assim, no caso referido, aplicar-se-ia o direito penal português, quer o agente estivesse em Portugal, quer o servidor estivesse em Portugal!

Acresce que o artigo 5º do Código Penal prevê ainda excepções ao princípio da territorialidade (artigo 4º), prevendo um conjunto de crimes e situações, em que a lei penal portuguesa se aplicará a situações não praticadas em território português. Entre estes estão desde logo o crime de Burla Informática (artigo 221º do Código penal), para além da generalidade dos crimes contra a Soberania Nacional, contra o Estado de Direito, falsificação de moeda, títulos ou valores selados, ou ainda terrorismo, entre outras

⁵ **Servidor (SERVER):** Computador ligado à Internet que detém e fornece serviços.

situações especiais. De certa maneira, todos estes crimes que podem ser praticados ou participados através da Internet.

Secção III - Crimes informáticos previstos no Código Penal

Subsecção I - Devassa por meio de informática ⁶

A criminalização destas práticas é decorrente do disposto no artigo 35º n.º 3 da Constituição da República Portuguesa, e visa proteger a reserva da vida privada contra possíveis actos de discriminação que a utilização de meios informáticos torna exponencialmente perigosos.

Razão pela qual o procedimento criminal relativamente ao crime previsto neste artigo 193º não depende de queixa. É assim, um crime público, sobre o qual o Estado terá sempre interesse e dever de agir.

No tipo legal da “devassa por meio de informática” encontramos não só os actos de criação de ficheiros violadores do “Bem” protegido, mas também os meros actos de conservação e utilização desse ficheiro, ainda que sem qualquer participação na sua criação. O tipo legal é assim bastante abrangente quanto às condutas penalizadas, o que pretende ser um facto dissuasor face à dificuldade de prova do “autor” material do ficheiro. No mesmo sentido se penaliza a mera tentativa.

⁶ Artigo 193º Código Penal – Devassa por meio de informática

1 - Quem criar, manter ou utilizar ficheiro automatizado de dados individualmente identificáveis e referentes a convicções políticas, religiosas ou filosóficas, à filiação partidária ou sindical, à vida privada, ou a origem étnica, é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias.

2 - A tentativa é punível.

Subsecção II - Violação de correspondência ou de telecomunicações ⁷

Este artigo é directamente aplicável à correspondência electrónica - via e-mail -, que é modernamente perfeitamente equiparável à correspondência postal fechada. O bem que se protege é aqui não só a privacidade mas também a confiança da comunidade na integridade dos meios de comunicação, nomeadamente das telecomunicações.

Coloca-se a questão de saber se este crime não se encontra absorvido pelo crime de “intercepção ilegítima”, previsto pelo artigo 8º da Lei 109/91. Parece-nos que embora possa existir sobreposição quando a intercepção da mensagem se dá durante a sua transmissão, já não haverá quando o acesso à mensagem se dá depois de esta ter sido já recepcionada pelo seu destinatário, encontrando-se guardada na sua caixa de correio electrónico. Embora, neste último caso, também se pudesse afirmar que estamos perante um crime de “acesso ilegítimo” previsto pelo artigo 6º da Lei 109/91, entendemos não ser o caso, desde logo porque este crime exige uma especial intenção: “e com a intenção de alcançar, para si ou para outrem, um benefício ou vantagem ilegítimos”, que o crime de “violação de correspondência ou de telecomunicações” não exige. Não se justificaria, assim, que uma correspondência fechada electrónica, depois de recepcionada, ficasse menos protegida que a correspondência em papel. Entendemos por isso que este crime se aplica ainda à correspondência electrónica.

⁷ Artigo 194º Código Penal - Violação de correspondência ou de telecomunicações

1 - Quem, sem consentimento, abrir encomenda, carta ou qualquer outro escrito que se encontre fechado e lhe não seja dirigido, ou tomar conhecimento, por processos técnicos, do seu conteúdo, ou impedir, por qualquer modo, que seja recebido pelo destinatário, é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias.

2 - Na mesma pena incorre quem, sem consentimento, se intrometer no conteúdo de telecomunicação ou dele tomar conhecimento.

3 - Quem, sem consentimento, divulgar o conteúdo de cartas, encomendas, escritos fechados, ou telecomunicações a que se referem os números anteriores, é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias»

Subsecção III - Burla informática e nas telecomunicações⁸

A burla informática prevista no artigo 221º do Código Penal surge no desenvolvimento da disciplina geral da burla, comungando dos mesmos elementos delimitadores do tipo do artigo 217º do Código penal: a intenção de obter para si ou para terceiro enriquecimento ilegítimo e o requisito de causar a terceiro prejuízo patrimonial. Tal como no tipo geral da burla, a tentativa é punível e o procedimento penal depende de queixa.

A especificidade deste tipo legal está no processo utilizado: a utilização de meios informáticos, ou seja, a utilização de meios informáticos de forma ardilosa para manipulação de dados ou de resultados.

Secção IV - Crimes informáticos previstos na Lei da Criminalidade Informática

Subsecção I - Falsidade Informática⁹

Este crime visa proteger a segurança das relações jurídicas, enquanto interesse público essencial que ao próprio Estado de Direito compete assegurar. Nessa medida a lei não

⁸ Artigo 221º do Código Penal - Burla informática e nas comunicações

1 - Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorrecta de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até 3 anos ou com pena de multa.

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

3 - A tentativa é punível.

4 - O procedimento criminal depende de queixa.

5 - Se o prejuízo for:

a) De valor elevado, o agente é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias;

b) De valor consideravelmente elevado, o agente é punido com pena de prisão de 2 a 8 anos.

6 - É correspondentemente aplicável o disposto no artigo 206º.

(Redacção da Lei nº 65/98, de 2 de Setembro)

⁹ Artigo 4º da Lei 109/91 - 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.

prevê a necessidade de queixa crime para o prosseguimento do procedimento criminal. Estamos assim perante um crime público.

No tipo legal equipara-se a adulteração de dado ou programa informático ao crime de “falsificação de documento” sempre que dessa adulteração poder resultar igual efeito de adulteração de meio de prova. Trata-se de um crime que inclui um elemento subjectivo - “intenção de provocar engano nas relações jurídicas” – na medida em que se entendeu que a adulteração de ficheiro informático apenas será aqui relevante quando for susceptível de criar insegurança nas relações jurídicas electrónicas.

Subsecção II - Dano relativo a dados ou programas informáticos¹⁰

Neste caso o bem jurídico protegido é o património do lesado. Nessa medida este crime dependerá de queixa, sendo um crime semi-público. Excepto no caso de o dano ser de «valor consideravelmente elevado», caso em que se dispensa a necessidade de queixa-crime para o procedimento criminal, sendo então um crime público (n.º 4 e 5). Neste caso, considera-se que, se o dano atingir determinados valores há um risco de perturbação da paz social e da confiança das pessoas na segurança jurídica e, no caso, na fiabilidade dos meios electrónicos, motivo pelo qual se considera haver um interesse público essencial em agir criminalmente.

Subsecção III - Sabotagem Informática¹¹

No caso, o bem jurídico protegido é a segurança dos sistemas e comunicações electrónicas, havendo por isso, um interesse essencial do Estado em agir criminalmente. Razão pela qual

¹⁰ Artigo 5º da Lei 109/91

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 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 n.os 1, 2 e 3 o procedimento penal depende da queixa.

¹¹ Artigo 6º da Lei 109/91 - 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 entrar 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.

este crime não depende de queixa para o prosseguimento do procedimento criminal, sendo um crime público.

Entre o tipo legal previsto neste artigo 6º da Lei 109/91 e o previsto no artigo 5º do mesmo diploma subsistem duas distinções essenciais:

Por um lado, o elemento objectivo do “Dano relativo a dados ou programas informáticos” é mais restrito que o protegido pela “Sabotagem informática” que para além da protecção de “dados e programa informáticos” visa proteger o «funcionamento de um sistema informático ou de comunicação de dados à distância».

Por outro lado, o elemento subjectivo do artigo 5º exige que o agente actue «com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo para si ou para terceiros», enquanto no crime de “Sabotagem informática” para a tipificação legal basta que agente actue «com intenção de entrar ou perturbar o funcionamento», não se exigindo a específica intenção de prejuízo ou benefício ilegítimos. Sendo por isso mais abrangente.

Subsecção IV - Acesso ilegítimo ¹²

O termo “acesso ilegítimo” abrange basicamente a infracção relativa às ameaças à segurança (confidencialidade, integridade e disponibilidade) dos sistemas informáticos. O meio mais viável de prevenção do acesso não autorizado é, indubitavelmente, a introdução e o desenvolvimento de medidas de segurança eficazes.

Neste caso, o bem jurídico protegido é o património do lesado e a segurança dos sistemas informáticos. Nessa medida este crime dependerá de queixa, sendo um crime semi-público.

Excepto nos casos em que através do acesso ilegítimo, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei¹³ ou «o

12 Artigo 7º da Lei 109/91 - 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 n.os 1, 2 e 4 o procedimento penal depende de queixa.

benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado», em que se dispensa a necessidade de queixa-crime para o procedimento criminal, sendo então um crime público. Nestes casos, outros valores públicos se levantam que justificam o interesse do Estado em agir criminalmente: a defesa da “concorrência” e da liberdade de comércio, a protecção um “Direito, Liberdade e Garantia”, ou ainda a protecção da segurança jurídica quando estão em causa valores elevados.

Subsecção V - Intercepção ilegítima ¹⁴

A intercepção ilegítima (Artigo 8º) tem o intuito de proteger o direito à privacidade na comunicação de dados. Esta infracção é aplicada a todas as formas de transferência electrónica de dados, quer se trate de uma transferência por telefone, fax, correio electrónico (e-mail) ou ficheiro. A infracção aplica-se a transmissões “não-públicas” de dados informatizados. O termo “não-públicas” delimita a natureza da comunicação e não a natureza dos dados transmitidos. Os dados comunicados poderão constituir informação disponível ao público, mas as partes desejarem comunicar confidencialmente. Ou os dados poderão ser mantidos em sigilo, para fins comerciais, até que o serviço seja remunerado. Desta forma, o termo “não-públicas” não exclui as redes públicas.

Aqui o bem jurídico protegido é a segurança e privacidade das comunicações electrónicas, havendo por isso, um interesse essencial do Estado em agir criminalmente. Por isso, este crime não depende de queixa para o prosseguimento do procedimento criminal, sendo um crime público.

¹³ Falamos aqui da protecção de dados pessoais e sensíveis nos termos do artigo 35º da Constituição da república Portuguesa e do Decreto-Lei 67/98 de 27 de Outubro.

¹⁴ Artigo 8º da Lei 109/91 - 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.

Subsecção VI - Reprodução ilegítima de programa protegido ¹⁵

O artigo 14º do DL 252/94, de 20/10, que regula a protecção jurídica de programas de computador, dispõe expressamente que quanto à tutela penal dos programas de computador lhes é aplicável o disposto no n.º 1 do artigo 9º da Lei 109/91.

Embora o bem protegido seja um direito privado, entendeu-se que existe um interesse essencial do Estado em proteger os criadores intelectuais e se justificava o interesse do Estado em agir criminalmente contra a violação de direitos desta natureza. Assim, este crime não depende de queixa, sendo um crime público.

CAPÍTULO II

Convenção sobre cibercriminalidade

Secção I - Introdução

A Convenção sobre o Cibercrime do Conselho da Europa é o primeiro trabalho internacional de relevo sobre o crime no ciberespaço, tendo participado na sua elaboração peritos internacionais de todo o mundo.

A Convenção sobre a Cibercriminalidade foi aberta para assinatura em 23 de Novembro de 2001. Até à data, esta convenção foi assinada por 42 países, dos quais 4 não se encontram entre os Estados-membros (Canadá, Japão, África do Sul e E.U.A), e ratificada por 10.

Assim, a Convenção já se encontra em vigor uma vez que o requisito para esse efeito, o de ser ratificado por, pelo menos, cinco Estados, três dos quais teriam que ser Estados-membros, foi cumprido em doze de Maio de 2003, aquando da ratificação da Convenção sobre o Cibercrime por parte da Estónia, juntando-se assim à Croácia e à Albânia. Portugal já assinou esta convenção mas ainda não a ratificou.

¹⁵ Artigo 9º da Lei 109/91 - 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.

Este Tratado prevê a maior parte dos crimes informáticos. No entanto, não foi contemplada inicialmente a utilização da Internet na propagação de conteúdos racistas que foi alvo de protocolo adicional em 28 de Janeiro de 2003, devido à oposição dos EUA por considerarem que essa medida poderia ser incompatível com a Primeira Emenda, que garante a liberdade de expressão.

A Convenção sobre o Cibercrime tem por objectivo principal a harmonização dos elementos relativos a infracções no contexto do direito penal substantivo de âmbito nacional e das disposições conexas na área da cibercriminalidade, a definição ao abrigo do código de processo penal interno dos poderes necessários para investigar e intentar acções penais relativamente a tais infracções, assim como a outras infracções cometidas por meio de um sistema informático¹⁶ ou às provas com elas relacionadas e existentes sob a forma electrónica, e a implementação de um regime rápido e eficaz de cooperação internacional.

A Convenção encontra-se dividida em quatro capítulos: (I) Utilização de terminologia; (II) Medidas a empreender a nível nacional – direito substantivo e direito processual; (III) Cooperação Internacional; (IV) Disposições Finais.

Analisemos sumariamente estes capítulos naquilo que interessa ao estudo que aqui desenvolvemos.

Secção II - Medidas a tomar a nível nacional

A convenção apresenta medidas a tomar pelos países aderentes em três níveis distintos: no direito penal material (artigos 2º ao 13º), no direito processual penal (artigos 14º ao 21º) e na competência (artigo 22º).

Ao nível do direito penal material, e no particular âmbito dos crimes informáticos propriamente ditos, verificamos que a maioria (acesso ilegítimo, interceptação ilegítima, interferência em dados, interferência em sistemas) estão já previstos em Portugal na Lei da Criminalidade Informática (Lei 109/91). Na legislação interna portuguesa apenas não se

¹⁶ **Sistema informático:** é um equipamento composto por *hardware* e *software* desenvolvidos para o tratamento automático de dados digitais. Podendo incluir dispositivos de entrada, saída e armazenamento, funcionar independentemente ou estar ligado em rede com outros dispositivos semelhantes (artigo 1º da Convenção sobre Cibercrime do Conselho da Europa).

prevê a «utilização indevida de dispositivos» que estabelece como infracção penal distinta e independente a prática intencional de actos ilegais específicos relativamente a certos dispositivos ou dados de acesso, indevidamente utilizados para cometer as infracções referidas contra a confidencialidade, integridade e disponibilidade dos sistemas ou dados informáticos. Este artigo visa penalizar a produção, a venda, a importação e a obtenção para utilização deste tipo de dispositivos. Veja-se a título de exemplo: os aparelhos destinados descodificação não autorizada de comunicações electrónicas codificadas, como seja emissão de televisão por cabo ou satélite.

Analisemos, seguidamente, as medidas propostas ao nível processual com interesse para o estudo que agora desenvolvemos.

Subsecção I

Medidas ao nível do direito penal processual

Nos artigos 14º a 25º da Convenção prevêm-se 5 medidas essenciais que os Estados subscritores deverão adoptar com vista a agilizar a investigação e punição da criminalidade informática a nível internacional.

Os artigos incluídos no primeiro título desta secção dizem que cada parte será obrigada a adoptar as medidas de foro legislativo, e outras, que sejam necessárias para assim estipular poderes e procedimentos para fins de investigação criminal (artigo 15º). Contudo, a implementação e a aplicação dos poderes e procedimentos anteriormente referidos deverão ficar sujeitos às condições e salvaguardas previstas nos termos da legislação interna de cada Estado (artigo 16º).

O segundo título desta segunda secção diz respeito à conservação expedita de dados informáticos¹⁷ armazenados. As disposições previstas nos artigos 16º e 17º aplicam-se a dados armazenados que já foram recolhidos e arquivados. Referem-se ainda à preservação e não ao arquivo de dados. Neste título pretende-se assegurar que as autoridades competentes disponham das capacidades necessárias para emitir uma ordem, ou obter a

¹⁷ **Dados informatizados:** serão dados sob a forma electrónica ou outra forma directamente processável, ou seja, que tenham sido colocados de tal forma que podem ser processados pelo sistema informático. É este o sentido da expressão “adequado para tratamento” utilizada pela convenção. Esta definição assenta na definição de dados de acordo com a norma ISSO (artigo 1º da Convenção sobre Cibercrime do Conselho da Europa).

preservação expedita de dados informatizados armazenados. Definem-se ainda obrigações específicas relativamente à preservação de dados de tráfego.

O terceiro título diz respeito à “injunção” (artigo 18º). Com esta figura pretende-se que as partes invistam as suas autoridades competentes de poderes necessários para obrigar uma pessoa que se encontre no seu território a fornecer dados armazenados e específicos, ou um fornecedor de serviços que ofereça os seus serviços no território da parte a prestar informação relativa a subscritores.

O título 4 (artigo 19º), relativo à busca e apreensão de dados informáticos armazenados, visa a modernização e harmonização das legislações nacionais relativamente à busca e apreensão desses dados para obtenção de provas. Este artigo introduz uma medida coerciva cujo objectivo é o de facilitar a apreensão de dados informatizados.

Por último, no título 5 desta secção propõe-se a possibilidade de recolha de dados informatizados em tempo real (artigos 20º e 21º). Ou seja, criar mecanismos legais que permitam a recolha, em tempo real, de dados de tráfego e a intercepção, também em tempo real, de dados de conteúdos associados a comunicações específicas transmitidas por meio de um sistema informático. Esta recolha de dados, do conteúdo das telecomunicações, desde sempre se tem revelado uma ferramenta de investigação útil. No entanto, não é possível determinar, em tempo real (devido às grandes quantidades de informação transmitidas), a natureza ilegal e nociva destas comunicações sem que se proceda à intercepção do conteúdo da mensagem. Desta forma, a intercepção das comunicações informáticas é tão importante como a intercepção de telecomunicações.

A última secção deste segundo capítulo versa sobre as competências, isto é, o conjunto de critérios segundo os quais as Partes ficam obrigadas a estipular a sua jurisdição relativamente às infracções penais dos artigos 2º a 11º da Convenção. O artigo 22º obriga cada Parte a punir a prática dos crimes definidos pela Convenção, quando estes forem cometidos no seu território (princípio da territorialidade). É ainda determinado que cada parte deverá estipular uma jurisdição penal relativa a infracções cometidas a bordo de um navio que ostente a sua bandeira ou de um avião registado ao abrigo das suas respectivas leis.

Secção III - Cooperação Internacional

Finalmente a Convenção dedica ainda um capítulo a disposições relativas à assistência mútua em casos de crime tradicional e crime informático, bem como a normas de extradição.

O artigo 23º especifica que a cooperação internacional deverá ter lugar entre as Partes “no âmbito mais alargado possível”, estendendo-se a todas as infracções penais relacionadas com sistemas informáticos e dados informatizados, bem como à recolha de provas sob a forma electrónica de uma determinada infracção penal, naquilo que aqui nos interessa.

Subsecção I - Disposições específicas

As disposições específicas, previstas na secção 2, visam estabelecer, num plano internacional, mecanismos que permitam uma acção eficaz em relação a casos que envolvam infracções relacionadas com computadores e provas sob a forma electrónica. Esta secção divide-se em três títulos.

O primeiro título desta secção, da assistência mútua relativa a medidas provisórias, compreende os artigos 29º e 30º que instituem mecanismos de âmbito internacional similares aos consagrados nos artigos 16º e 17º para o plano nacional. Assim, o artigo 29º impõe que as Partes disponham da capacidade jurídica para obter de qualquer outra parte, mediante requerimento, a preservação expedita dos dados armazenados no território da Parte requerida através de um sistema informático, de modo a que os dados não sejam alterados, removidos ou eliminados durante o período de tempo necessário à preparação, transmissão e execução de um pedido de assistência mútua para fins de obtenção de dados. Segundo o artigo 30º, através de solicitação de uma Parte no território da qual foi cometida uma infracção, a Parte requerida irá proceder à preservação dos dados de tráfego relativos a uma comunicação transmitida através dos seus computadores, a fim de detectar a origem da comunicação e identificar o autor da infracção ou localizar provas decisivas.

O segundo título, da assistência mútua relativamente a poderes de investigação, engloba, os artigos 31º a 34. Onde é de realçar o artigo 32º que prevê mecanismos para evitar a dependência das investigações de sistemas de assistência mútua internacional, isto é, prevê uma forma de obtenção de prova no estrangeiro sem recurso à cooperação internacional.

Trata-se de, no decurso de uma investigação, obter de um computador localizado no estrangeiro, dados de livre acesso ou cujo acesso tenha sido autorizado pela pessoa com legitimidade para autorizar tal acesso.

O último título, respeitante à designada rede 24/7, cinge-se ao artigo 35º que obriga cada Parte a denominar um ponto de contacto permanente, ou seja, que esteja disponível 24 horas por dia, 7 dias por semana, com o intuito de assegurar uma assistência imediata ao nível das investigações e dos processos penais.

CAPÍTULO III

Meios de prova em ambiente digital no ordenamento português

Secção I - Inexistência de um regime próprio

Apesar de já ter assinado a Convenção sobre Cibercrime, Portugal ainda não a ratificou, pelo que esta ainda não se encontra em vigor em Portugal.

Assim, como dissemos, e ao contrário do que sucede com o direito penal material, Portugal ainda não dispõe no seu processo penal dos meios de prova promovidos pela Convenção citada, nem dos meios de colaboração internacional aí consignados o que, desde logo, inquina parcialmente as investigações criminais nesta área.

É certo que esteve já em discussão na Assembleia da República um projecto de lei promovido pelo grupo parlamentar do partido popular (projecto de lei n.º 217/IX, de 27 de Janeiro de 2003¹⁸), que se debruçava precisamente sobre a criação de um Regime Jurídico da obtenção de prova digital electrónica na Internet. No entanto, este projecto veio a caducar por vicissitudes relacionadas com crises governamentais alheias a esta matéria.

Na esteira deste projecto de Lei, também o Governo chegou a elaborar uma proposta de lei sobre a mesma matéria em 2004, mas o diploma não chegou a ser levado a conselho de Ministros, não tendo a matéria sido ainda regulamentada.

¹⁸ Ver anexo 1 – Projecto de lei n.º 217/IX, de 27 de Janeiro de 2003.

Não entraremos na análise deste diploma para não dispersarmos mais o objecto do presente trabalho, embora o anexemos dado o interesse que pode revestir no estudo de uma futura solução legal.

Secção II - Aplicação das regras gerais do processo penal

Pese embora a ausência de um regime próprio para a obtenção de prova em ambiente digital, ainda assim é possível encontrar novas aplicações para os instrumentos tradicionais do processo penal.

Analisaremos de seguida os que nos parecem mais relevantes.

Subsecção I - A prova pericial

O artigo 151º do Código de Processo Penal determina que a prova pericial “tem lugar quando a percepção ou apreciação dos factos exigir especiais conhecimentos técnicos, científicos ou artísticos”.

No ambiente digital, pela complexidade e especificidade das suas técnicas e linguagem a que apenas a compreensão de especialistas consegue aceder, o recurso a perícias tem duas virtualidades para a investigação e obtenção de prova.

Por um lado, a opinião dos técnicos e peritos especialistas permite a quem investiga compreender os factos em investigação e reconduzir esses factos técnicos à tipificação legal dos crimes informáticos e ao conhecimento dos respectivos autores.

Veja-se, a título de exemplo, o crime de «Dano relativo a dados ou programas informáticos» (artigo 5º da Lei 109/91) penaliza quem “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“. Poderá ser necessário, por exemplo, saber o que é “tornar um dado não utilizável” em termos electrónicos? E em que medida tal facto afecta a “capacidade de uso” de determinado programa informático? Bem como se tal dano poderá ter sido praticado por mera negligência, uso indevido, acto fortuito, ou se apenas um acto intencional poderia causar tal dano ao “dado electrónico”.

Por outro lado, a perícia facilita a produção da prova e a percepção desses mesmos factos pelos julgadores, também eles, provavelmente, sem conhecimentos técnicos suficientes para compreender plenamente a realidade digital. As perícias nesta matéria são tão mais importantes como tipo de prova quanto tem um valor reforçado no processo penal, já que as suas conclusões escapam à possibilidade de livre apreciação do julgador, pois “se a convicção do julgador divergir do juízo contido no parecer dos peritos, deve aquele fundamentar a divergência” (artigo 163º, n.º 1 CPP) já que “o juízo técnico, científico ou artístico inerente à prova pericial presume-se subtraído à livre apreciação do julgador” (artigo 171º n.º 1 do CPP).

Subsecção II - Intercepção de comunicações

Pedro Verdelho¹⁹ defende a plena aplicação às comunicações electrónicas do regime da intercepção de comunicações «por remissão para o regime de intercepção de conversações telefónicas». E, de facto, o artigo 190º do CPP dispõe que é aplicável “às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática” o regime previsto para a intercepção e gravação de conversações telefónicas.

Aplicar-se-ão a estas, nessa medida, os mesmos procedimentos e autorizações judiciais previstas para as “escutas telefónicas” (artigos 187º a 189º do CPP). Certo sendo que entendemos que as comunicações electrónicas não exigem uma tramitação processual distinta da consagrada para as demais comunicações, mormente no que concerne à salvaguarda do direito fundamental à inviolabilidade do domicílio e da correspondência (artigo 34º da CRP). Por esse motivo, abster-nos-emos de analisar estes procedimentos e autorizações judicial para não estendermos em demasia o objecto do presente trabalho.

Naturalmente que, neste caso, falamos da intercepção de mensagens de correio electrónico em tempo real, ou seja, no seu trajecto do computador do emissor para o computador do receptor a través da rede de servidores. Ou ainda à intercepção de mensagens trocadas através de processos de comunicação instantânea (usualmente designados por serviços de “Chat”, como são os casos do “IRC”, do “MSN Messenger”, ou do “ICQ”).

¹⁹ VERDELHO Pedro, “A obtenção de prova no ambiente digital”, Revista do Ministério Público, Ano 25, n.º 99, Julho/Setembro 2004, pp 117 a 136;

Atente-se ainda, com particular importância, que a aplicação do regime da interceptação de comunicações telefónicas às comunicações electrónicas abre também a possibilidade de interceptação de comunicações áudio realizadas através de “Voice Over IP”²⁰. Tanto mais que esta tecnologia, permitindo chamadas áudio, de qualidade similar às chamadas telefónicas, com possibilidade de ligação entre computadores ou de computadores para redes telefónicas fixas ou móveis, e com custos para o utilizador consideravelmente mais baixos que as comunicações telefónicas, está em exponencial crescimento a nível mundial.

Ainda quanto às mensagens de correio electrónico, há que considerar a hipótese de elas não serem interceptadas no seu trajecto, e ainda assim serem úteis à investigação ou como meio de prova. Falamos das mensagens que, após a sua recepção, ficam armazenadas na caixa de correio do destinatário, seja em servidor que preste serviço de armazenamento (Webmail) ou no próprio computador do destinatário que as descarrega do servidor.

Neste caso, o meio de obtenção destas provas terá de ser outro, por exemplo, a apreensão de correspondência.

Subsecção III - Apreensão de correspondência

Nos termos do artigo 179º do CPP “o juiz pode autorizar ou ordenar, por despacho, a apreensão, mesmo nas estações de correios e de telecomunicações, de cartas, encomendas, valores, telegramas ou qualquer outra correspondência”.

Não há motivos para que esta disposição não se aplique também à correspondência electrónica. Neste caso, como vimos supra, não falamos na interceptação da mensagem electrónica no seu trajecto na rede, mas na sua apreensão no local onde estiver armazenada.

Verifiquemos ainda que o artigo 179º do CPP permite a apreensão mesmo nas estações de correios e de telecomunicações”. Donde devemos admitir que a apreensão de correspondência electrónica possa ser feita quer directamente no disco duro do destinatário, quer no servidor onde estiver definitiva ou temporariamente armazenada.

²⁰ **Voice Over IP:** tecnologia que permite efectuar conversações áudio em tempo real, ou seja instantâneas como sucede nas comunicações telefónicas, utilizando o protocolo IP e a Internet. Esta tecnologia converte a voz em dados informáticos que são expedidos pela rede e depois de novo em voz no receptor da comunicação.

Naturalmente, e mais uma vez, terão que se respeitar os procedimentos previstos no CPP para a apreensão de correspondência em papel.

Pedro Verdelho²¹ coloca ainda a questão de saber se deve ser dado o mesmo tratamento garantístico a mensagens recebidas mas ainda não lidas e a mensagens recebidas e já efectivamente abertas e lidas, concluindo que “às primeiras parece fácil dar, analogicamente, o mesmo tratamento físico, dito tradicional, contido em envelopes ainda não abertos. Quanto às segundas, é de admitir a possibilidade de se considerarem meros documentos armazenados num computador, com o mesmo estatuto de uma carta recebida e guardada num arquivo pessoal ou de um texto escrito e guardado em suporte informático. A acolher-se esta perspectiva, as mensagens não abertas teriam um tratamento diferenciado das mensagens já abertas e lidas”.

Subsecção IV - Outras disposições

Naturalmente que será ainda passível de considerar a realização de exames (artigo 171º a 173º do CPP) e de revistas ou buscas (artigos 174º e 177º do CPP). Quanto a estas a única especificidade que se coloca é o “ambiente digital” em que estas se processam e as especiais habilitações que será necessário possuir para “examinar” ou “buscar” em meio electrónico.

CONCLUSÃO

Ao nível do direito penal material, e no particular âmbito dos crimes informáticos propriamente ditos, verificamos que, quer no Código penal quer na Lei da Criminalidade Informática (Lei 109/91), Portugal prevê já um leque capaz de abarcar os principais actos criminosos e que o uso de meios informáticos é elemento essencial. Em comparação com a Convenção sobre Cibercriminalidade não se prevê apenas a «utilização indevida de dispositivos» que estabelece como infracção penal distinta e independente a prática intencional de actos ilegais específicos relativamente a certos dispositivos ou dados de acesso, indevidamente utilizados para cometer as infracções referidas contra a confidencialidade, integridade e disponibilidade dos sistemas ou dados informáticos.

²¹ Obra citada.

Consideramos pois que a nível de direito penal material, Portugal encontra-se no bom caminho para a punição da Cibercriminalidade.

Verificamos ainda que os meios comuns de investigação e prova em processo penal têm relevantes aplicações no combate à criminalidade informática e na obtenção de prova em ambiente digital.

No entanto, estes meios de investigação e de prova, pela sua finalidade e pelos procedimentos que lhes estão associados, não são aptos a uma investigação eficaz e à obtenção de prova sustentável num ambiente virtual de mutação potencialmente instantânea.

É por demais evidente que a especificidade do ambiente digital e a potencial internacionalização inerente à Internet requerem outros meios de investigação e de prova adequados a estas realidades.

Reconhecendo a importância de uma harmonização da legislação e do desenvolvimento de meios eficazes para prevenir e combater a utilização abusiva das novas tecnologias foi elaborado o primeiro tratado internacional sobre crimes cometidos através da Internet e outras redes de computadores – A Convenção sobre o Cibercrime.

Esta convenção visa, basicamente, obter a cooperação, em sentido amplo, de todos os Estados Partes para que adoptem medidas legislativas locais, bem como outras acções preventivas e repressivas de toda a criminalidade, por forma a garantir a salvaguarda dos dados de tráfego, a sua retenção e a subsequente entrega de forma desburocratizada aos investigadores, sob pena de ineficácia. A cooperação prevista nesse instrumento de direito público internacional materializa-se através da adopção de uma política penal comum. A Convenção abrange um amplo campo de infracções relativas à criminalidade informática. Pretende-se que os Estados Partes na Convenção erijam estes actos em infracções penais e se dotem da legislação adequada.

Com vista a este fim, como vimos, o tratado prevê uma série de procedimentos legais que incluem a procura e a interceptação de computadores.

Portugal é um dos muitos países que apesar de já ter assinado a Convenção ainda não a ratificou. Esta ratificação implicará algumas mudanças na nossa lei, em várias vertentes, nomeadamente no âmbito das medidas de direito processual propostas e ainda não previstas na legislação processual penal portuguesa.

Pensamos assim que Portugal deverá retomar o mais rapidamente possível o processo legislativo de aprovação de um regime de meios de investigação e prova em ambiente digital, na senda das medidas propostas na Convenção sobre Cibercriminalidade, o que não só habilitaria os órgãos de investigação penal portugueses de meios processuais adequados ao combate à Cibercriminalidade em território português como potenciaria a cooperação internacional neste campo onde, como vimos, ela é particularmente relevante.

FONTES

- <http://www.verbojuridico.net> (site jurídico do Dr. Joel Timóteo Ramos Pereira)
- <http://www.anacom.pt> (site oficial da Autoridade Nacional de Comunicações)
- <http://www.dgrn.pt> (site oficial da Direcção Geral de Registos e Notariado)
- <http://www.pj.pt> – (site oficial da Polícia Judiciária)

BIBLIOGRAFIA

- SANTOS, Cristina Máximo dos, “As novas tecnologias da informação e o sigilo das telecomunicações”, Revista do Ministério Público, Ano 25, n.º 99, Julho/Setembro 2004, pp 89 a 116;
- VERDELHO Pedro, “A obtenção de prova no ambiente digital”, Revista do Ministério Público, Ano 25, n.º 99, Julho/Setembro 2004, pp 117 a 136;
- PEREIRA, Joel Timóteo Ramos, “Compêndio Jurídico da Sociedade da Informação”, Quid Júris, Lisboa, 2004;
- Vários, “Direito da Sociedade da Informação – Volume IV”, Associação portuguesa do Direito Itelectual, Coimbra Editora, 2003.
- VERDELHO, Pedro, BRAVO, Rogério, e LOPES ROCHA, Manuel, “ Leis do Cibercrime – volume 1”, Centro Atlântico, 2003.
- MARTINS, A. G. Lourenço, “Criminalidade Informática”, artigo publicado em Direito da Sociedade da Informação, Volume IV, APDI, Coimbra Editora, 2003;
- VERDELHO, Pedro, “Cibercrime”, artigo publicado em Direito da Sociedade da Informação, Volume IV, APDI, Coimbra Editora, 2003;
- MENDES, Paulo de Sousa, “ A responsabilidade das pessoas colectivas no âmbito da criminalidade informática em Portugal”, artigo publicado em Direito da Sociedade da Informação, Volume IV, APDI, Coimbra Editora, 2003;
- PEREIRA, Joel Timóteo Ramos; Direito da Internet e Comércio Electrónico, Quid Júris, Lisboa, 2001;
- ASCENÇÃO, José de Oliveira, «Estudos sobre Direito da Internet e da Sociedade da Informação», Livraria Almedina, Abril, 2001;
- SOUSA, Miguel Teixeira de, “O valor probatório dos documentos electrónicos”, in Direito da Sociedade da Informação – Volume II, FDUL / APDI, Coimbra Editora, 2001.
- MARQUES, Carlos e MARTINS, Lourenço, “Direito da Informática”, 2000, Almedina.
- COSTA; José F. de faria, “Direito Penal da Comunicação (alguns escritos)”, Coimbra Editora, Coimbra, 1998;
- ANDRADE, Manuel da Costa, “Sobre Proibições de prova em processo penal”, Coimbra Editora, 1992.

Anexo 1

PROJECTO DE LEI N.º 217/IX

**REGIME JURÍDICO DA OBTENÇÃO DE PROVA DIGITAL ELECTRÓNICA NA
INTERNET**

PROJECTO DE LEI N.º 217/IX

REGIME JURÍDICO DA OBTENÇÃO DE PROVA DIGITAL ELECTRÓNICA NA INTERNET

Exposição de motivos

1 — A utilização massiva e generalizada dos sistemas informáticos, potenciada pelo crescente aumento das capacidades de armazenamento e processamento dos computadores, pela fusão do processo de informação com as novas tecnologias de comunicação e pela fácil transmissão, em segundos ou minutos, dos dados criados, processados ou armazenados, não só permitiu a mutação das práticas tradicionais do crime, como também originou novos tipos de criminalidade (os chamados crimes virtuais puros e crimes virtuais mistos).

Seja da manipulação fraudulenta de dados com intuito lucrativo que estejamos a falar, seja da utilização indevida de informação contida em arquivos ou suportes informáticos alheios, designadamente a falsidade informática e acesso ilegítimo, seja de qualquer outra utilização possível das tecnologias de informação e comunicação como instrumento de trabalho ilícito e fonte inesgotável de mecanismos que facilitam as actividades criminosas, não é difícil chegar à conclusão que ainda há um longo caminho a percorrer, no sentido de se dotar a investigação criminal das condições necessárias a um combate profícuo a esta criminalidade que se dotou de novos meios.

Torna-se necessário, portanto, dotar as autoridades de novos métodos de investigação, proporcionando-lhes o acesso a informação relevante dentro dos parâmetros impostos pelo direito à reserva da intimidade da vida privada e familiar e pelo sigilo das telecomunicações.

2 — A Internet constitui, de facto um instrumento privilegiado de redes internacionais organizadas para a prática de crimes como o comércio de armas, o tráfico de droga, o terrorismo e o branqueamento de capitais, mas, também, de difusão de conteúdos que atingem outro tipo de valores, associados à subsistência e à liberdade da própria humanidade, como são os casos do incitamento ao ódio e à violência racial ou religiosa ou de exploração sexual de crianças e adolescentes.

Cada vez mais a Internet vem servindo de palco, meio e fonte de inspiração de desvios comportamentais especialmente danosos, como, por exemplo, a pedofilia, e, simultaneamente, de realização de um variado número de negócios relacionados com esses actos, tudo a coberto da ocultação da identidade dos diversos intervenientes.

É, pois, crucial o acesso urgente, por parte das autoridades, à informação necessária e suficiente para a investigação criminal, proporcionando-lhes a forma de acederem, em tempo útil, à

informação disponível nas operadoras de comunicações que permita a identificação dos autores e o registo dos actos ilícitos praticados através dos meios informáticos e de comunicações.

3 — A inexistência da obrigatoriedade das operadoras de comunicações de manterem e conservarem os dados que permitam a recolha de informação quanto à origem, percurso, destino e duração, entre outros dados (dados de tráfego), tem constituído uma dificuldade inultrapassável para a recolha da ora denominada prova digital.

Está em causa o tratamento de dados pessoais com vista à respectiva protecção, bem como a protecção da privacidade no sector das comunicações electrónicas. Mas o que importa não esquecer é que a reserva da intimidade da vida privada e familiar e o sigilo das comunicações não são os únicos valores que, nestes domínios, importa ao Estado de direito salvaguardar: a par deles, e porque contendem com os seus padrões éticos e com a liberdade e autodeterminação dos seres humanos, avultam outros tão ou mais importantes e que podem igualmente ser postergados pelo uso indevido das telecomunicações e pela falta de prevenção do uso ilícito dos meios electrónicos, tarefa da qual as operadoras devem partilhar por natureza e necessidade.

4 — Há, assim, que garantir:

— Que a informação relevante para a investigação seja preservada pelos operadores de telecomunicações e, simultaneamente,

— Que as autoridades a eles acedam em tempo útil.

Daí que se estabeleça a obrigação para os operadores de comunicações (ISP, GSM, Rede Fixa, SVA e outros) da manutenção e conservação dos registos durante um ano, período que se considerou adequado ao desenvolvimento da reacção da justiça, em caso de ilícito. Esta obrigação abrange não só os dados de tráfego, como também os chamados dados de base, estes igualmente por motivos de cooperação internacional. De igual modo, parece útil acautelar junto dos operadores a salvaguarda de determinadas comunicações, mediante solicitação das autoridades de polícia criminal, sem prejuízo da intervenção posterior da autoridade judiciária.

Adoptou-se, nesta matéria, terminologia consensual e recentemente consagrada na Convenção sobre o Cibercrime, do Conselho da Europa, aberta à assinatura dos Estados a 23 de Novembro de 2001, em Budapeste).

Deste modo, a recolha de prova para efeitos de investigação criminal será feita:

— Pelas autoridades de polícia criminal (com o alcance previsto pela alínea d) do artigo 1.º do Código de Processo Penal) no que concerne à informação a colher junto das operadoras relativamente a dados de tráfego;

— Pelas autoridades de polícia criminal e (ou) pelas autoridades judiciárias competentes, e consoante o respectivo acesso seja ou não público, quanto à dos dados de base; e

— Com a aplicação do regime previsto nos artigos 188.º e 189.º do Código do Processo Penal, em relação aos dados de conteúdo.

Propugna-se igualmente a utilização dos mesmos meios de obtenção de prova quanto aos chamados crimes comuns cometidos com recurso a meios informáticos, dada a salvaguarda de apreciação judicial individualizada.

5 — Por fim, importa ainda estabelecer, em relação aos operadores em geral, um dever de colaboração que faça com que, sempre que estes detectem, no âmbito da sua actividade, condutas que possam indiciar a existência dos mencionados crimes, o comuniquem às autoridades competentes para efeitos de investigação criminal.

Nestes termos, os Deputados abaixo assinados apresentam o seguinte projecto de lei:

Artigo 1.º **(Definições)**

Para os efeitos da presente lei, considera-se:

- a) Dados de tráfego: os dados informáticos ou técnicos relacionados com uma comunicação efectuada por meio de tecnologias de informação e comunicação, por si gerados, indicando, designadamente, a origem da comunicação, o destino, os trajectos, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente;
- b) Dados de base: os dados pessoais relativos à conexão à rede de comunicações, designadamente número, identidade e morada de assinante, bem como a listagem de movimentos de comunicações, e que constituem elementos necessários ao estabelecimento de uma base para a comunicação;
- c) Dados de conteúdo: os dados relativos ao conteúdo da comunicação ou de uma mensagem.

Artigo 2.º **(Do acesso aos dados de tráfego)**

Para efeitos de prevenção e investigação criminal os operadores de comunicações devem facultar às autoridades de polícia criminal ou às autoridades judiciárias os dados de tráfego, sempre que estes lhes sejam por elas solicitados, no prazo máximo de cinco dias.

Artigo 3.º **(Do acesso aos dados de base)**

1 — O disposto no artigo anterior é aplicável aos dados de base, sempre que estes não estejam sujeitos ao regime de confidencialidade.

2 — Entende-se que se encontram sujeitos ao regime da confidencialidade os dados relativamente aos quais o utilizador tenha expressamente manifestado o desejo de não serem publicitados.

3 — No caso de dados de base sujeitos a esse regime, o pedido para o seu fornecimento incumbe a autoridade judiciária titular da direcção do processo, em despacho fundamentado, sem prejuízo da delegação genérica de competências de investigação criminal nos órgãos de polícia criminal, nos termos do Código de Processo Penal e do Decreto-Lei n.º 275-A/2000, de 29 de Novembro.

Artigo 4.º

(Da recusa injustificada de acesso aos dados de tráfego e de base)

A recusa injustificada de fornecimento dos dados solicitados nos termos dos artigos anteriores faz incorrer os operadores em crime de desobediência qualificada.

Artigo 5.º

(Do acesso aos dados de conteúdo)

Ao acesso aos dados de conteúdo é aplicável, independentemente da natureza e da gravidade da infracção, o preceituado nos artigos 188.º e 189.º do Código de Processo Penal.

Artigo 6.º

(Da obrigação de preservação de dados)

1 — Os operadores de comunicação são obrigados a preservar, pelo período mínimo de um ano, a informação relativa aos dados de tráfego e de base.

2 — Sem prejuízo do disposto no artigo 5.º, e até à intervenção judicial, impende sobre os operadores de comunicações o dever de preservação de uma comunicação, mediante solicitação concreta da autoridade de polícia criminal.

3 — O incumprimento dos deveres previstos nos n.ºs 1 e 2 constitui contra-ordenação punível com coima de 2 500 a 25 000 euros, no caso de pessoas singulares, e de 5 000 a 50 000 euros, no caso de pessoas colectivas.

4 — No caso de reincidência, a coima é elevada ao dobro nos seus limites mínimo e máximo.

Artigo 7.º

(Dos fornecedores de serviços de acesso às redes de comunicações)

1 — Os fornecedores de serviços de acesso às redes de comunicações, designadamente todas as que facultem aos utilizadores dos seus serviços a possibilidade de comunicar por meio de uma tecnologia de informação e comunicação, bem como qualquer outra entidade, pública ou privada, que processe ou armazene informação, devem identificar os respectivos utilizadores, através de documento legal de identificação, bem como registar o terminal e período de tempo utilizado.

2 — É aplicável o disposto nos n.ºs 1 a 4 do artigo anterior.

Artigo 8.º

(Dever especial de colaboração)

1 — Sempre que, no decurso da sua actividade, os operadores de comunicações constatem, através da utilização dos seus serviços, condutas que sejam passíveis de integrar a prática, com carácter de habitualidade, dos crimes previstos nos artigos 172.º, n.º 3, alíneas a) a d), e n.º 4, 173.º, n.º 2, e 240.º do Código Penal são obrigados a comunicá-las às autoridades de polícia criminal ou às autoridades judiciais, no prazo máximo de cinco dias.

2 — O dever de colaboração previsto no número anterior implica a obrigação de preservação de toda a informação adequada à identificação dos factos e dos seus autores.

3 — À prestação das informações previstas neste diploma é aplicável o disposto nos artigos 10.º, n.º 4, e 13.º do Decreto-Lei n.º 313/93, de 15 de Setembro.

4 — É aplicável o disposto nos n.ºs 3 e 4 do artigo 6.º.

Artigo 9.º

(Negligência e tentativa)

São puníveis a negligência e a tentativa na prática das contra-ordenações previstas no presente diploma.

Artigo 10.º

(Sanções acessórias)

Às contra-ordenações previstas nos artigos anteriores são aplicáveis, em função da sua gravidade e da culpa do agente, as sanções acessórias do artigo 21.º, alíneas b) c) f) e g), do Decreto-Lei n.º 433/82, de 27 de Outubro, sem prejuízo do disposto nos n.ºs 2 e 3 do mesmo artigo.

Artigo 11.º**(Processamento e aplicação das coimas e sanções acessórias)**

1 — A aplicação das coimas e sanções acessórias previstas na presente lei compete à Autoridade Nacional de Comunicações (ANC).

2 — A instauração e instrução do processo de contra-ordenação é da competência da mesma Autoridade.

3 — Do montante das coimas aplicadas, 70% revertem para o Estado e 30% para a ANC.

Palácio de São Bento, 27 de Janeiro de 2003. Os Deputados do CDS-PP: Telmo Correia — Nuno Teixeira de Melo — Diogo Feio — Álvaro Castello Branco — João Pinho de Almeida — Herculano Gonçalves — Miguel Paiva — Henrique Campos Cunha— Manuel Cambra.