I. Introdução

A presente obra pretende de forma simples permitir o acesso directo a temas importantes relacionados com o Direito Digital ou Ciberdireito, no fundo, o conjunto de normas que regulam os novíssimos direitos da que surgiram com os Computadores Pessoais e a Internet.

O primeiro computador pessoal surgiu há quarenta anos, a 12 de Agosto de 1981, tendo a norte-americana IBM sido pioneira ao apresentar o seu Modelo 5150, com o processador 8088 da Intel e sistema operativo licenciado pela Microsoft.

Iniciava-se uma nova era. Uma novíssima Era Digital.

O 5051 da IBM – que sem disco rígido se apresentava como o conjunto de monitor monocromático de cor verde, teclado, unidade central, impressora e unidade externa de disquetes – inovava pelo seu tamanho físico, já que até aí os computadores, para além de terem valores que ascendiam a cerca de $20.000,00 (vinte mil dólares), ocupavam áreas que os impediam de ser adquiridos para uso doméstico.

Também o valor do novo 5051 veio garantir a abertura do mercado residencial e de pequenas e médias empresas à IBM com o valor de venda ao público do primeiro computador pessoal fixado em cerca de €1.300,00 (mil e trezentos euros), o que equivaleria hoje a cerca de €3.375,00 (três mil trezentos e setenta e cinco euros) sendo distribuído com software que incluía a folha de cálculo *VisiCalc*, processamento de texto através do programa *Easywriter* 1.0 e, ainda, o primeiro jogo da *Microsoft – Adventure*.

Estavam lançados os dados para uma nova era.

Foi com este equipamento que o computador da IBM marcou o início de uma nova era no uso digital, daí ser considerado o "Pai" dos computadores modernos, que veio revolucionar todo o sector.

Actualmente, o confinamento e o redireccionamento para o teletrabalho vieram contrariar a tendência de queda nas vendas, sendo que segundo a norte-americana *IDC Corporate USA* as fabricantes fecharam 2020 com números superiores a 302 milhões de PC vendidos (incluindo computadores de secretária,

portáveis e workstations) com a Lenovo, HP Inc e Dell Technologies no topo da tabela.

Mas, já antes da chegada às nossas casas dos computadores pessoais, se tinha iniciado a pesquisa sobre a comutação de pacotes de dados e redes de comutação de pacotes, com recurso a vários protocolos.

Entre a década de 60 e o início da década de 70, sistemas *Telenet, Cyclades, Merit Network* ou *Tymnet* foram desenvolvidos e permitiam a transmissão de dados.

Em especial, *a Arpanet (Advanced Research Projects Agency Network*) – financiada pelo Departamento de Defesa dos Estados Unidos através da sua Agência de Projectos de Pesquisa Avançada (ARPA) de onde herdaria o nome – veio lançar as bases da actual internet (*Lievrouw, L. A.; Livingstone, S. M. (2006). Handbook of New Media: Student Edition. EUA: SAGE. p. 253. 475 páginas. ISBN 1412918731*), permitindo desenvolver protocolos de comunicação entre várias redes separadas no espaço físico, tendo sido a primeira rede a implementar o conjunto de protocolos TCP/IP.

Também em 1981, com o financiamento da Rede de Ciência da Computação (CSNET) pela Fundação Nacional da Ciência norte-americana (NSF) se aumentou o acesso à ARPANET. Em 1982, o conjunto de protocolos de Internet (TCP/ /IP) foi introduzido como o protocolo de rede padrão na ARPANET, tendo, no início dos anos 80, a NSF financiado o estabelecimento de diversos centros nacionais de supercomputação nas diversas universidades, proporcionando uma interconectividade em 1986 com o projecto NSFNET, que também criou acesso aos sítios electrónicos por supercomputadores nos Estados Unidos a partir de organizações de pesquisa e educação. A ARPANET viria a ser desactivada em 1990. [*G. Schneider; J. Evans; K. Pinard (2009). The Internet – Illustrated. EUA: Cengage Learning. ISBN 0538750987*]

Com o desmantelamento da NSFNET (*National Science Foundation Network*) e a remoção das últimas restrições sobre o uso da internet para transportar o tráfego comercial, a internet foi definitivamente liberalizada em 1995, tornando-se o seu uso comercial (*Harris, Susan R.; Gerich, Elise «Retiring the NSFNET Backbone Service: Chronicling the End of an Era». ConneXions. 10*) iniciando, no final da década de 80, uma rápida expansão para a Europa, Ásia e Austrália.

A partir do início da década de 1990 a internet passou a ter um impacto crescente sobre a cultura e o comércio mundiais, nomeadamente com o surgimento de sistemas de comunicação instantânea com programas como o *mIRC* (cliente de chat através do protocolo de *Internet Relay Chat*) mas também softwares como o ICQ cuja notificação de nova mensagem ficou gravada para todos os seus utilizadores.

Do protocolo IRC à facilidade de envio de mensagens de correio electrónico, chamadas VoIP (*Voice over* IP), chamadas de vídeo, fóruns de discussão, páginas

web institucionais, redes sociais, sítios de compras em linha, o mundo Digital evoluiu a uma velocidade imbatível.

Ao mesmo tempo as operadoras de comunicação – conscientes da necessidade de assegurar a transmissão cada vez mais elevada de dados – aumentaram a oferta que nos anos 90 era maioritariamente disponibilizado com recurso a modems que ocupavam as linhas telefónicas, e cuja velocidade era naturalmente incompatível com o que a sociedade impunha com o aumento da curiosidade desta nova Era.

Hoje, à velocidade da fibra óptica, a oferta de conteúdos e aplicações permitem considerar a internet como uma extensão da nossa vida pessoal e laboral, como espaço familiar, de trabalho ou de entretenimento. Quantos almoços de família se fizeram com recurso às novas tecnologias, com recurso a programas como Zoom ou *WhatsApp*. Quantas reuniões com clientes ou com colegas de trabalho. Quantos julgamentos terão já sido feitos através da aplicação *Webex*. É, pois, deste mundo digital que trataremos na presente obra que apenas pretende abrir a porta para o que já existe e cuja regulamentação não é, ainda, suficiente para o que já existe.

Ao legislador espera-o um trabalho árduo de seleccionar todas as matérias cujo actual estado das artes permite que se verifiquem em ambientes digitais (transmissão de dados pessoais, comércio electrónico, investimento em cripto-activos, desde a sua oferta inicial de distribuição até à celebração de contratos por diferença – CDF) e regula-los para que a fuga para o mundo virtual não implique uma perda de competência territorial e consequente inviabilização da segurança jurídica cuja base estará, espera-se, na norma a criar.

II. Resenha Histórica

Em Portugal, Lei da criminalidade informática (Lei nº 109/91, de 17 de Agosto), que entrou em vigor em Dezembro daquele ano, apresentava já definições para rede informática, sistema informático, programa informático, topografia, produto semicondutor e intercepção, prevendo já níveis de valores (elevado aquele que excedesse 50 unidades de conta e consideravelmente elevado aquele que excedesse as 200 unidades de conta no momento da prática do facto).

A Lei da Criminalidade Informática previa já a responsabilidade penal das pessoas colectivas ou equiparadas, as quais respondiam penal e civilmente (de forma solidária), pelo pagamento de multas, indemnizações e outras prestações em que fossem condenados os agentes das respectivas infracções.

Subsidiariamente aplicável a legislação penal (ex vi do art. 1º) a Lei nº 109/91 de 17 de Agosto previa no seu elenco de crimes ligados à informática a Falsidade informática (art. 4º) Dano relativo a dados ou programas informáticos (art. 5º), Sabotagem informática (art. 6º), Acesso ilegítimo (art. 7º), Intercepção ilegítima (art. 8º) e Reprodução ilegítima de programa protegido (art. 9º), prevendo-se a aplicação de penas às pessoas colectivas e equiparadas pelos crimes ali previstos, nomeadamente a admoestação, multa ou dissolução.

A Lei da Criminalidade informática veio estabelecer os conceitos de rede informática, como o conjunto de dois ou mais computadores interconectados, sistema informático, como o conjunto constituído por um ou mais computadores, respectivos equipamentos periféricos e suporte lógico que assegurasse o processamento de dados.

A definição de programa informático consistia em "*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*".

Do ponto de vista físico, veio igualmente a ser definida "topografia" como a série de imagens ligadas entre si, 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 dese-

nho ou parte dele de uma superfície do produto semicondutor, independentemente da fase do respectivo fabrico e produto semicondutor, como "*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*";

Do ponto de vista da criminalidade informática, teve o legislador a necessidade de especificar o conceito de "Intercepção" (de dados informáticos) como o acto destinado a captar informações contidas num sistema automatizado de dados, através de dispositivos electromagnéticos, acústicos, mecânicos ou outros.

Também para efeitos de aplicação da moldura penal, e considerando que o valor do tipo de bem protegido pelo mesmo poderia variar fixou-se valor elevado como aquele que excedesse 50 unidades de conta processual penal avaliadas no momento da prática do facto e valor consideravelmente elevado como aquele que excedesse 200 unidades de conta processual penal avaliadas no momento da prática do facto.

Assim, a partir de 1991, passa a estar tipificado no ordenamento jurídico português o crime de *Falsidade informática*, o qual se verificaria sempre que alguém, com intenção de provocar engano nas relações jurídicas, introduzisse, modificasse, apagasse ou suprimisse dados ou programas informáticos ou, por qualquer outra forma, interferisse num tratamento informático de dados, quando esses dados ou programas fossem susceptíveis de servirem como meio de prova, de tal modo que a sua visualização produzisse os mesmos efeitos de um documento falsificado, ou, bem assim, os utilizasse para os fins descritos, seria punido com pena de prisão até cinco anos ou multa de 120 a 600 dias.

Nas mesmas penas incorreria quem use documento produzido a partir de dados ou programas informatizados que fossem objecto dos actos referidos, actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiros.

A referida moldura penal subiria para pena de prisão de um a cinco anos sempre que os factos referidos forem praticados por funcionário no exercício das suas funções.

Relativamente ao crime de *dano relativo a dados ou programas informáticos*, previa-se ali que 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, apagasse, destruísse, no todo ou em parte, danificasse, suprimisse ou tornasse não utilizáveis dados ou programas informáticos alheios ou, por qualquer forma, lhes afectasse a capacidade de uso seria punido com pena de prisão até três anos ou pena de multa, sendo a tentativa punível, dependendo de queixa

o procedimento criminal excepto se os danos causados fossem de valor consideravelmente elevados.

Quanto ao referido crime, caso o dano causado fosse de valor superior a 50 unidades de conta a pena seria a de prisão até 5 anos ou de multa até 600 dias, mas já se os danos causados fossem superiores a 200 unidades de conta, a pena fixar-se-ia em prisão de 1 a 10 anos.

O crime de *sabotagem informática*, previa que quem introduzisse, alterasse, apagasse ou suprimisse dados ou programas informáticos ou, por qualquer outra forma, interferisse em sistema informático, actuando com intenção de entravar ou perturbar o funcionamento de um sistema informático ou de comunicação de dados à distância, seria punido com pena de prisão até 5 anos ou com pena de multa até 600 dias, sendo que a pena seria a de prisão de um a cinco anos se o dano emergente da perturbação fosse de valor elevado ou, de 1 a 10 anos de prisão se o dano emergente da perturbação fosse de valor consideravelmente elevado.

O crime de *acesso ilegítimo* verificar-se-ia sempre que alguém que, não estando para tanto autorizado e com a intenção de alcançar, para si ou para outrem, um benefício ou vantagem ilegítimos, de qualquer modo acedesse a um sistema ou rede informáticos seria punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.

A pena seria a de prisão até três anos ou multa se o acesso fosse conseguido através de violação de regras de segurança mas subiria para prisão de um a cinco anos quando através do acesso, o agente tivesse tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei ou, caso o benefício ou vantagem patrimonial obtidos fossem de valor consideravelmente elevado, sendo em qualquer caso a tentativa punível.

Praticaria o *crime de Intercepção ilegítima* todo aquele que, sem para tanto estar autorizado, e através de meios técnicos, interceptasse comunicações que se processassem no interior de um sistema ou rede informáticos, a eles destinadas ou deles provenientes, sendo nesses casos punida a prática do referido crime com pena de prisão até três anos ou com pena de multa e sendo a tentativa punível.

O crime de *Reprodução ilegítima de programa protegido* consistia em alguém, sem para tal estar autorizado, reproduzir, divulgar ou comunicar ao público programa informático protegido por lei, sendo nesses casos punido com pena de prisão até três anos ou com pena de multa.

Na mesma pena incorreria quem ilegitimamente reproduzisse topografia de um produto semicondutor ou a explorar comercialmente ou importasse, para esses fins, uma topografia ou um produto semicondutor fabricado a partir dessa topografia, sendo sempre a tentativa punível.

No caso penas aplicáveis às pessoas colectivas e equiparadas e pelos crimes previstos na referida lei previa-se a possibilidade de decretar a pena de disso-

lução, a qual seria aplicada quando os titulares dos órgãos ou representantes da pessoa colectiva ou sociedade tivessem agido com a intenção, exclusiva ou predominantemente, de, por meio dela, praticar os factos que integrassem os crimes ali previstos ou quando a prática reiterada desses factos revelasse que a pessoa colectiva ou sociedade estava a ser utilizada para esse efeito, quer pelos seus membros, quer por quem exercesse a respectiva administração.

A título de penas acessórias poderiam ser aplicadas a *perda de bens, a caução de boa conduta* (obrigação de o agente depositar uma quantia em dinheiro, entre cerca de €50,00 a €5.000,00 a fixar pelo tribunal e por período entre seis a dois anos e a qual seria perdida a favor do Estado caso o agente praticasse nova infracção), *interdição temporária do exercício de certas actividades ou profissões* (aplicada sempre que a infracção fosse cometida com flagrante e manifesto abuso da profissão ou no exercício de actividade que dependesse de um título público de uma autorização ou homologação da autoridade pública), *encerramento temporário ou definitivo de estabelecimento* (decretado por períodos mínimos de um mês a um ano no primeiro caso, sendo definitivo o encerramento em casos de anteriores condenações por infracções previstas na Lei da criminalidade informática, tiver sido já decretado o encerramento temporário e houver condenação anterior com pena de prisão por dano de valor consideravelmente elevado ou para um número avultado de pessoas) *e a publicidade da decisão condenatória* (sempre 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 editais, por período não inferior a 30 dias, no próprio estabelecimento ou no local do exercício da actividade, por forma bem visível pelo público).

Relativamente à conservação de prova, a Lei nº 32/2008, de 17 de Julho (Lei relativa a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações) viria estabelecer um regime processual privativo relativamente à conservação de dados, impondo aos fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações a conservação de diversas categorias de dados, nomeadamente de dados necessários para encontrar e identificar a fonte de uma comunicação, dados necessários para encontrar e identificar o destino de uma comunicação, dados necessários para identificar a data, a hora e a duração de uma comunicação, dados necessários para identificar o tipo de comunicação, dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento e dados necessários para identificar a localização do equipamento de comunicação móvel.

Relativamente a acessos à Internet, ao correio electrónico através da Internet e às comunicações telefónicas através da Internet estabeleceu-se a preservação dos códigos de identificação atribuídos ao utilizador, o código de identificação do utilizador e o número de telefone atribuídos a qualquer comunicação que entre na rede telefónica pública, o nome e o endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP, o código de identificação de utilizador ou o número de telefone estavam atribuídos no momento da comunicação sendo que se estipulava a preservação do código de identificação do utilizador ou o número de telefone do destinatário pretendido, ou de uma comunicação telefónica através da Internet, os nomes e os endereços dos subscritores, ou dos utilizadores registados, e o código de identificação de utilizador do destinatário pretendido da comunicação devendo sempre ser registada a data e a hora do início (*log in*) e do fim (*log off*) da ligação ao serviço de acesso à Internet com base em determinado fuso horário, juntamente com o endereço do protocolo IP, dinâmico ou estático, atribuído pelo fornecedor do serviço de acesso à Internet a uma comunicação, bem como o código de identificação de utilizador do subscritor ou do utilizador registado.

Estávamos ainda numa fase em que os acessos à internet eram feitos por via de modems cuja utilização implicava chamada telefónica para a operadora fornecedora de serviços de acesso à internet.

Por esse motivo, ficaria registado a data e a hora do início e do fim da ligação ao serviço de correio electrónico através da Internet ou de comunicações através da Internet, com base em determinado fuso horário, bem como o número de telefone que solicita o acesso por linha telefónica, a linha de assinante digital (*digital subscriber line*, ou DSL), ou qualquer outro identificador terminal do autor da comunicação.

A Lei da Criminalidade informática veio a ser revogada em 2009, com a publicação da Lei nº 109/2009 de 15 de Setembro que aprovou a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro nº 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adaptou o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

Com a entrada em vigor da referida lei foram estabelecidas as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico tendo em consideração o facto deste tipo de criminalidade estar habitualmente associado a práticas transfronteiriças que criavam obstáculos à aquisição de prova e à celeridade necessária para a cessação de actividades criminosas.

O Legislador mantém, grosso modo, as definições anteriormente estabelecidas na Lei da criminalidade informática, desenvolvendo-as no seu artigo 2º

onde refere na sua alínea a) «Sistema informático», como "*qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção*", uma definição, mais cuidada relativamente à anterior que definia como simples "*conjunto constituído por um ou mais computadores, respectivos equipamentos periféricos e suporte lógico que assegurasse o processamento de dados*."

Foi mantida igualmente a definição de "*Intercepção*" (de dados informáticos) como o acto destinado a captar informações contidas num sistema automatizado de dados, através de dispositivos electromagnéticos, acústicos, mecânicos ou outros, bem como a definição de "*Topografia*" (uma série de imagens ligadas entre si, 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 de "*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).

Surgem, contudo, as novas definições de "*Dados informáticos*" como qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função, "*Dados de tráfego*", como os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente e "*Fornecedor de serviço*" como qualquer entidade, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, bem como qualquer outra entidade que trate ou armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviço ou dos respectivos utilizadores.

O catálogo dos crimes tipificados na Lei 109/2009 de 15 de Setembro é idêntico ao que já constava da Lei de 1991, e inclui crime de *Falsidade informática* (art. 3º), *o crime de Dano relativo a programas ou outros dados informáticos* (Art. 4º), *o crime de Sabotagem informática* (Art. 5º), *o crime de acesso ilegítimo* (art. 6º), *o crime de*

intercepção ilegítima (art. 7º) *o crime de reprodução ilegítima de programa protegido* (art. 8º), mas passa agora a incluir um conjunto de disposições processuais os quais serão aplicáveis a processos relativos crimes que constem da Lei do Cibercrime, a crimes cometidos por meio de sistema informático e a quaisquer outros em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico.

E tal alteração veio a ter impacto, por exemplo, na alteração da jurisprudência que até aqui equiparava, por exemplo, as mensagens SMS às cartas de correio, distinguindo entre as situações em que ainda estariam fechadas ou aquelas em que já haviam sido abertas pelo destinatário, e que agora vê tal entendimento alterado, uma vez que a leitura de mensagens guardadas num cartão de telemóvel (ou equipamento) por um agente policial sem autorização do seu dono ou do JIC passa a ser prova proibida, em nada relevando que as mesmas tivessem sido ou não abertas e lidas pelo destinatário porquanto a lei não distingue entre essas duas situações.

A preservação expedita de dados passa a ser ordenada pela autoridade judiciária competente ou órgão de polícia criminal em caso de urgência ou perigo na demora, discriminando a natureza dos dados, origem e destino se conhecidos e período de tempo pelo qual deverão ser preservados, num máximo de três meses, deixando de se aplicar o regime processual das comunicações telefónicas previsto nos artigos 187º a 190º do Código de Processo Penal por extensão às «telecomunicações electrónicas», «crimes informáticos» e «recolha de prova electrónica (informática)»., sendo que tendo em vista assegurar a preservação dos dados de tráfego relativos a uma determinada comunicação, independentemente do número de fornecedores de serviço que nela participaram, o fornecedor de serviço a quem essa preservação tenha sido ordenada indica à autoridade judiciária ou ao órgão de polícia criminal, logo que o souber, outros fornecedores de serviço através dos quais aquela comunicação tenha sido efectuada, tendo em vista permitir identificar todos os fornecedores de serviço e a via através da qual aquela comunicação foi efectuada.

No decurso do processo, se se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência, será a injunção para apresentação ou concessão do acesso a dados, sendo igualmente possível a apreensão de dados informáticos (dados ou documentos informáticos necessários à produção de prova), quer do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à

respectiva leitura, quer através de realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo, quer ainda através da preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos ou ainda através de eliminação não reversível ou bloqueio do acesso aos dados.

Tal como supra referido, a apreensão de correio electrónico e registos de comunicações de natureza semelhante passa agora a ter tratamento específico, impondo-se que quando sejam encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, o juiz possa autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal, sendo igualmente admissível o recurso à intercepção de comunicações e o registo de transmissões de dados informáticos os quais apenas poderão ser autorizados durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público.

Passa a ser admissível o recurso às acções encobertas previstas na Lei nº 101/2001, de 25 de Agosto, nos termos aí previstos, no decurso de inquérito relativo aos crimes da lei do Cibercrime ou àqueles cometidos por meio de um sistema informático, quando lhes corresponda, em abstracto, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infracções económico-financeiras, bem como os crimes consagrados no título iv do Código do Direito de Autor e dos Direitos Conexos.

A Cooperação internacional é igualmente uma das apostas para efeitos de investigações ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos, bem como para efeitos de recolha de prova, em suporte electrónico, de um crime, de acordo com as normas sobre transferência de dados pessoais previstas na Lei nº 67/98, de 26 de Outubro sendo criado um ponto de contacto permanente para a cooperação internacional, tendo em vista a prestação de assistência imediata para os efeitos referidos no artigo anterior, assegurado pela Polícia Judiciária, vinte e quatro horas por dia, sete dias por semana.

Relativamente à aplicação no espaço da lei penal portuguesa e à competência dos tribunais portugueses, prevê-se que para além do disposto no Código

Penal em matéria de aplicação no espaço da lei penal portuguesa, e salvo tratado ou convenção internacional em contrário, a lei penal portuguesa será ainda aplicável a factos praticados por Portugueses, se aos mesmos não for aplicável a lei penal de nenhum outro Estado, cometidos em benefício de pessoas colectivas com sede em território português, fisicamente praticados em território português, ainda que visem sistemas informáticos localizados fora desse território ou que visem sistemas informáticos localizados em território português, independentemente do local onde esses factos forem fisicamente praticados.

ÍNDICE