A PROPÓSITO DA *PROVA DIGITAL* NO PROCESSO PENAL(*)

Pelo Dr. Renato Lopes Militão

Sumário:

1. Sobretudo a partir da década de 1980, bastas vezes acriticamente, tem sido recorrente a afirmação de que a sociedade hodierna é uma *sociedade pós-industrial*, *da informação* ou *da comunicação*. Pretensamente, a informação seria hoje não só a

---

(*) Este texto corresponde, com ligeiras alterações, ao trabalho de projecto apresentado na disciplina de Direito da Comunicação, no âmbito de um curso de Mestrado leccionado pelas Faculdades de Direito e de Ciências Sociais e Humanas da Universidade Nova de Lisboa.

principal fonte de riqueza como a causa primeira das transformações económicas, sociais, políticas e culturais, enfim, o motor da evolução social.

Não cabe no âmbito deste trabalho o aprofundamento dessa perspectiva. Todavia, não deixará de dizer-se que a mesma surgiu enquadrada no processo de implementação da *globalização neoliberal*, serve em pleno a defesa deste modelo de sociedade e, do nosso ponto de vista, não passa de um mito radicalmente ideológico construído para o efeito.

Na verdade, o que tal perspectiva pretende afirmar e tem de facto proclamado é que as novas tecnologias da informação e da comunicação (NTIC) impuseram, objectivamente, no quadro global, uma *nova economia*, predominantemente de bens imateriais, pretensamente caracterizada por um elevado crescimento económico, pela expansão do emprego no domínio dos serviços relacionados com aquelas tecnologias, pela imperiosidade da flexibilização do trabalho e do mercado de trabalho, pela inevitabilidade de um mercado livre à escala mundial e por uma nova governança das empresas, que, obviamente, terão de ser, todas elas, privadas. Uma *nova economia* que inviabiliza a conflitualidade social e a própria acção política. Enfim, uma *nova economia* que impõe, inexoravelmente, o modelo do *capitalismo neoliberal global*.

Porém, ao contrário do que tem sido levianamente propagandeado pelos arautos da *nova economia*, desde o início da década de 1980, isto é, desde a introdução massiva das NTIC, a taxa de crescimento económico tem sido francamente reduzida, sobretudo se comparada com a que se registou nos decénios antecedentes. Os ganhos de produtividade decorrentes da utilização das NTIC são manifestamente inferiores aos que se têm verificado em sectores e actividades que não se servem dessas tecnologias, bem como àqueles que se registaram no tempo das *velhas tecnologias*. O número de empregos gerado pelas NTIC não se aproxima nem de perto àquele que se verifica em actividades alheias às mesmas (*v.g.*, Gadrey, 2001: 39 e ss.).

Com efeito, no actual modelo, que mais não é do que a reposição, no contexto do sistema capitalista, do paradigma do velho liberalismo, agora à escala global, em elevada medida *dirigida*

pelos Estados dos países capitalistas do centro e pelas suas organizações internacionais, tornou a intensificar-se a exploração do trabalho pelo capital(1), os salários têm diminuído, o desemprego e a precariedade laboral regressaram massivamente, voltaram as crises económicas cíclicas, agora globais e cada vez mais intensas, reacendeu-se a exploração do Sul pelo Norte(2) e, afinal, como se disse, regrediu o crescimento económico. Na verdade, o que se tem verificado nas últimas décadas é a ampliação colossal das desigualdades sociais e a *pauperização* de grande parte da população, com a consequente exclusão dos mais desfavorecidos(3).

Assim, ao contrário do que se propagandeia, a informação não substituiu o trabalho. E muito menos submeteu o capital. Ao invés, no actual modelo de sociedade, a informação, tal como, obviamente antes de mais, o trabalho, encontra-se profundamente subjugada pelo capital.

Como sublinhou Karl Marx (*apud* Chesnais, 1999: 552) no séc. XIX, conclusão que a actual crise económica tornou a demonstrar à saciedade, «[o] processo de produção capitalista aparece apenas como um intermediário inevitável, um mal necessário para fazer dinheiro. É por isso que todas as nações dedicadas ao

---

(1) É deveras curioso que, por exemplo na Grã-Bretanha, a pretensa *sociedade pós-industrial*, *da informação* ou *da comunicação* tenha elevado para 2 milhões o número de jovens entre os 6 e os 15 anos — dos quais 500 000 com menos de treze anos — com um emprego regular em sectores por vezes duríssimos. «Regresso ao século XIX». Aliás, nesse país, «em vinte anos, os 10% com rendimentos mais baixos perdiam 20% do seu poder de compra, ao passo que o poder de compra dos 10% com rendimentos mais elevados aumentava 65%» (Passet, 2002: 113-114). E nesse tal mundo pós-industrial, da informação ou da comunicação, «pelo menos 120 milhões de crianças de 5 a 14 anos trabalham a tempo inteiro, e pelo menos o dobro em actividades complementares» (Fontanel, 2007: 60).

(2) De facto, «o diferencial entre o Norte e Sul era (…) de trinta para um em 1965. Actualmente está por cima de setenta para um e continua a aumentar» (George, *apud* Lopes, 2008: 56).

(3) Sobre o crescimento da assimetria na repartição da riqueza em Portugal, *vd*. Rodrigues, 2007: sobretudo 140-193. Na verdade, o *capitalismo neoliberal global* tem gerado uma transferência da riqueza dos pobres para os ricos. De facto, «enquanto que a parcela dos 20% mais pobres no produto mundial baixava de 2,3% em 1969 para 1,5% em 1989 e para 1% em 1997, a dos 20% mais ricos subia de 69% para 82,5% e para 86%» (Passet, 2002: 102). *Sociedade pós-industrial*, *da informação* ou *da comunicação* ou capitalismo selvagem puro e duro?

modo de produção capitalista são periodicamente apanhadas pela vertigem de querer fazer dinheiro sem o intermediário do processo de produção». Ora, a disseminação da ideia de uma *sociedade pós-industrial*, *da informação* ou *do conhecimento*, conceitos, aliás, estes últimos, tautológicos e, de resto, todos, superficiais, para além de um mito ideológico, é em grande medida, justamente, o resultado dessa vertigem([4]).

2. O que se deixa dito de modo algum equivale a minimizar que, não obstante sob o enquadramento do modelo do *capitalismo neoliberal global* e em medidas substancialmente diferenciadas social e geograficamente, cada vez mais se assiste ao progresso científico, técnico e tecnológico no domínio das NTIC. Com efeito, as potencialidades, disponibilização, facilitação e, consequentemente, a utilização destas tecnologias vêm crescendo de dia para dia. O que tem ampliado enormemente os fluxos informacionais e comunicacionais na sociedade.

Estas realidades, seja pela sua dimensão, seja pelas próprias características e consequentes potencialidades das NTIC, têm naturalmente exigido a intervenção do Direito.

Porém, no actual contexto, os Estados e as organizações internacionais *neoliberais*, sempre radicalmente *dirigistas* no sentido da imposição do seu modelo de sociedade, têm-se servido do Direito justamente com vista a submeterem a informação e a comunicação ao modelo do *capitalismo neoliberal global*. De facto, um dos mais salientes aspectos da evolução do Direito da Informação nas últimas três décadas é sem dúvida a «consagração de formas de apropriação privada da informação ou dos produtos da informação», transferindo-se assim «em boa parte a questão da liberdade de informação das esferas política e pública para a esfera económica» e, nesta, para o domínio privado (Gonçalves, 2003: 40-43).

([4]) De resto, se não fosse preocupante, seria no mínimo caricato o facto de inúmeros adeptos da tese da chamada *sociedade pós-industrial* mostrarem logo de seguida profunda preocupação com a escalada da poluição no planeta. Afinal em que ficamos: vivemos num paraíso celestial da informação e do conhecimento ou antes num mundo radicalmente industrializado e, por isso, dramaticamente poluído?

Acresce que, sem aderirmos ao conceito *beckiano*, e não só, de *sociedade do risco*, o qual mais não é do que o desenvolvimento das ideias de *sociedade pós-industrial*, *da informação* ou *da comunicação*, sendo, no mínimo, tão superficial e radicalmente ideológico quanto estas([5]), o certo é que também aquelas realidades têm potenciado o desenvolvimento de riscos, perigos e danos nas esferas da vida individual e colectiva. Com efeito, para o que aqui mais interessa, é indiscutível que a disponibilização, a facilitação, as potencialidades e a utilização crescentes das NTIC são susceptíveis de levar e têm efectivamente levado ao seu uso como instrumentos privilegiados da prática de velhos e novos actos de elevada danosidade para os indivíduos, para as empresas, para as instâncias públicas e para a sociedade em geral.

([5]) Aliás, importa ter-se presente que, de um modo geral, o sentimento de risco e, consequentemente, de perigo, o qual surgiu no final da década de 1970 (*v.g.*, ROBERT, 2002: *maxime* 111 e ss.), é sobretudo um sentimento *subjectivo* e irracional (*v.g.*, MACHADO, 2004: 15 e ss.), resultando em primeira linha não de riscos e perigos concretos mas do desenvolvimento em crescendo da individualização, da instabilidade, da perda de expectativas quanto ao futuro, da exclusão social, da ampliação dos guetos periféricos às grandes cidades ou do crescimento das chamadas «incivilidades». É, de resto, precisamente por se tratar de um sentimento sobretudo *subjectivo* que é facilmente manipulável. E, de facto, tem-no sido à exaustão pelos ideólogos, políticos, *opinion makers* e demais actores do *sistema*. Com efeito, a exploração desse sentimento traz enormes vantagens ao *status quo*. Além do mais, inibe a intervenção social e política dos cidadãos, valida a subalternização de políticas económicas e sociais face a políticas de segurança e justifica a expansão colossal do aparelho de controlo social, que desse modo fica a dispor de todo o tipo de vigilância, informação e capacidade de reacção sobre a população, particularmente sobre os potenciais focos de revolta social, permitindo assim que o *establishment* económico, social e político não venha a ser beliscado. Na verdade, sem pretendermos subvalorizá-los, os riscos e perigos concretamente existentes nas sociedades contemporâneas, para além de decorrerem em grande medida do próprio modelo do *capitalismo neoliberal global* e de serem bastante diferenciados social e geograficamente, estão muito aquém da dimensão que grande parte dos autores pretende conferir-lhes. De resto, para utilizarmos uma expressão suave, é no mínimo anacrónico que um dos principais teóricos da chamada *sociedade do risco*, Anthony Giddens, haja sido um dos mais influentes conselheiros de Tony Blair e, portanto, tenha estado directamente ligado à invasão intencional e injustificada do Iraque, cujos riscos e perigos, esses sim *concretos*, bem como os danos causados têm sido incomensuráveis e dramáticos. Para além de tudo o mais, aproxima-se rapidamente de um milhão o número de vidas humanas que já se perdeu desde o início dessa invasão... Como qualificará Giddens um Estado que provoca directa e intencionalmente tamanhos riscos, perigos e danos?

Ora, tais fenómenos têm originado a progressão também neste domínio do Direito Penal, substantivo e adjectivo. O qual, com algumas especificidades decorrentes das características e potencialidades próprias das NTIC, tem evidenciado sem dúvida a imagem de marca do Direito Penal *neoliberal*.

3. Na verdade, a receita dos Estados *neoliberais* para colmatarem a sua retirada da actividade económica e da sociedade civil em geral, cedendo-as quase totalmente ao egoísmo da iniciativa privada e à pretensa racionalidade dos mercados livres globais, bem como a consequente degradação quer dos direitos sociais, quer da política e, portanto, da democracia, em particular da dimensão participativa desta, tem sido a progressão avassaladora de um Direito Penal, substantivo e adjectivo, profundamente *securitário*.

O seu objectivo primeiro é o de vigiarem, controlarem e reprimirem a cada vez maior mole de excluídos que o seu modelo de sociedade gera, isto é, os jovens sem emprego, os desempregados em geral, os *guetizados*, em suma, aqueles que mais poderão pôr em causa esse modelo (*v.g.*, Araújo, 2009: 162; Baratta, 2004: 206--208; Wacquant, 2001: 7; Western, 2009: 119). E são efectivamente estes que o actual Direito Penal e Processual Penal mais atinge. De facto, «[s]e o crime não é privilégio de classe, a punição parece sê-lo» (Adorno, *apud* Felix, 2007: 17).

Por isso se diz, com toda a acuidade, que as últimas décadas de novo têm acentuado «um direito da marginalidade social, que importado para o século XXI não só obsta à perseguição penal efectiva das modernas formas de criminalidade como põe em causa a própria legitimidade da perseguição penal da designada criminalidade clássica» (Mesquita, 2010: 442). Efectivamente, tal realidade não só amplia a ideia da existência de uma "justiça de classe" (Andrade, 2009: 74) como realmente a concretiza.

Por estas e outras razões, que não cabe aqui abordar, não partilhamos da perspectiva de que a resposta ao crescimento dos riscos, dos perigos e, mesmo, dos danos deva ou, sequer, possa ser obtida fundamentalmente através do Direito Penal, substantivo e

adjectivo. Do nosso ponto de vista, tais realidades ou, pelo menos, grande parte das suas formas, sobretudo as de motivação económica, como aliás, adiante-se desde já, é em regra o caso da *criminalidade informática*, só poderão ser relevantemente minimizadas por via da intervenção profusa das instâncias políticas democráticas no sistema económico e nos demais sistemas sociais, da ampliação da democracia participativa, designadamente com o incremento do controlo e da participação dos trabalhadores na gestão das empresas e outras entidades, públicas e privadas, e, enfim, da efectivação da democracia económica, social e cultural. A intervenção do Direito Penal não só deve ser de *ultima ratio* como jamais será uma solução. E muito menos poderá sê-lo no actual modelo de sociedade(6).

Mas o certo é que o *securitarismo*, ainda que em relação a certas formas de criminalidade, *maxime* ao *white collar crime* em geral, não obstante a enorme danosidade deste, como a actual crise económica tem evidenciado à exaustão, apenas com um «significado simbólico», «sem eficácia, para inglês ver» (Franco, 2000: 209), tornou-se a referência de todo o Direito Penal substantivo e adjectivo *neoliberal*.

Com efeito, apenas para o que aqui mais releva, têm sido colossais as soluções de pendor *securitário* introduzidas ao longo dos últimos trinta anos no domínio do processo penal, principalmente na fase da investigação, isto é, «naquela parte do processo em que se trata de instrumentos de controlo», e mesmo antes dela (Hassemer, 2004: 21). Por todo o lado, numa perspectiva emergen-

---

(6) Como aduz Faria Costa (2005: 30), «[p]ensemos, como ilustração, no branqueamento de capitais. Todos estamos de acordo que tal prática deve ser fortemente punida e perseguida (...). Tudo começa a complicar-se — e a complicar-se de maneira exponencial — quando vemos, por outro lado, a serem permitidas, quando não potenciadas as chamadas zonas de "off-shore". Isto é: quando vemos serem aceites como elementos de estímulo à economia plataformas de contratação onde, como se sabe e lhe é inerente, o controlo da proveniência do capital se torna mais difícil, quando não impossível. Pune-se, criminalmente — e bem, sublinhe-se a traço grosso —, o branqueamento de capitais mas permite-se, em simultâneo, um campo propício à proliferação daquela prática». De resto, no actual modelo, de um modo geral, o Direito Penal não consegue sequer penetrar nas empresas (Muñoz, 2009: 197). Desse modo, pese embora a sua elevadíssima danosidade, a criminalidade *white collar* em geral continua e continuará a apresentar elevadíssimas *cifras negras*.

cial, eficientista e funcional, facilita-se o regime das detenções, buscas, apreensões, revistas, exames ou perícias. O que tem passado em grande medida, mas não só, pelo fortalecimento dos poderes das polícias, conseguido sobretudo à custa da redução das competências e, por conseguinte, da intervenção das magistraturas([7]). Mas igualmente se tem assistido à degradação dos segredos profissionais, à ampliação do regime das testemunhas encobertas, à implementação da delação, ao estímulo e recompensa aos "arrependidos" (não pelo seu "arrependimento", mas simplesmente a troco de "auxílio" na investigação), à permissão de utilização de informações sob segredo, ao alargamento do regime das escutas telefónicas e intercepções de correio electrónico e de conversações entre presentes ou à banalização das acções encobertas (internamente e no exterior).

Nesse contexto, particular relevo tem assumido a colossal progressão dos chamados *meios ocultos de investigação*. Efectivamente, «foi nas últimas duas décadas que estes meios apareceram em massa e em força e se instalaram definitivamente no processo penal. Um fenómeno de "metastização fulgurante" (…)», não obstante «a evidência da sua drástica e comprometedora danosidade social, a desdobrar-se e a alastrar, multiplicada e amplificada, numa pluralidade de frentes» e com a agravante de não conhecerem «distinção nem diferença entre suspeito e inocente» (Andrade, 2009: 105-107). De facto, tem sido claríssima nos últimos tempos da História a «importação pelo processo penal de técnicas dos serviços secretos» (Mesquita, 2010: 440).

([7]) A título meramente ilustrativo, veja-se que a reforma de 2007 do CPP (Lei n.º 48/2007, de 29/08) concedeu às autoridades de polícia criminal a faculdade de, *por iniciativa própria*, ordenarem a detenção, designadamente de suspeitos, fora de flagrante delito, no caso de entenderem que existe fundado receio de continuação da actividade criminosa (art. 257.º, n.º 2, al. *b*), *in fine*, do CPP), bem como atribuiu às polícias *competência própria* para obterem dados sobre a localização celular (art. 252.º-A, do CPP, norma esta, aliás, de manifesta inconstitucionalidade (*vd*. RODRIGUES, 2011: 35)). De todo o modo, a facilitação das detenções, buscas, apreensões, revistas, exames e perícias em favor das polícias tem ocorrido em grande medida sub-repticiamente, por duas vias. Por um lado, através da consagração de excepções aos regimes gerais, dentro do CPP (*v.g.*, art. 174.º, n.º 5) e, sobretudo, como adiante melhor veremos, fora dele (*v.g.*, art. 53.º da Lei n.º 15/93, de 22/01). Por outro lado, pelo alargamento dos conceitos dos crimes de catálogo (*vd*. art. 1.º, als. *j*), *l*) e *m*), do CPP).

Paralelamente, têm sido criadas múltiplas entidades supra-estaduais e de cooperação internacional, facilitam-se as trocas inter-estaduais de informações, processuais e não só, simplificam-se as extradições, inclusive de cidadãos nacionais, instituem-se mandados de detenção internacionais, etc., etc.

E o pior é que não só se está em grande medida perante uma «previsão atomizada de mecanismos excepcionais, sem uma avaliação de conjunto da sua necessidade e dos valores colidentes» (Mesquita, 2010: 439), como se sabe que «o processo penal comum é geralmente bastante para reagir com firmeza» mesmo contra a «criminalidade grave e organizada» (Silva, 2005: 73).

Naturalmente, esse percurso está a fragilizar princípios fundamentais do processo penal. Com efeito, verifica-se claramente a minimização dos princípios da publicidade e da oralidade, ou «enfraquecimento do contraditório bem como do princípio da imediação» (Palma, 2004: 52).

Assiste-se, na verdade, a uma progressiva degradação das garantias processuais do suspeito e do arguido. De facto, «[a] diminuição das garantias processuais é um dos aspectos que mais rapidamente se manifestam enquanto característica do Estado punitivo» (Costa, 2005: 31). Efectivamente, sobreposto o valor segurança ao bem liberdade, os direitos fundamentais «tendem a constituir um obstáculo numa luta eficaz do Estado contra a criminalidade» (Hassemer, 2004: 22).

Assim, o processo penal *neoliberal* é cada vez mais *secretista*, imediatista, intrusivo e desleal.

Acresce que, como aliás era inevitável, todo esse contexto está já a determinar a «instrumentalização do processo penal para finalidades não repressivas, como meio privilegiado para o acesso à informação relevante para a segurança do Estado (nomeadamente através da manipulação das informações criminais e concorrência de diferentes departamentos para o seu domínio)» (Mesquita, 2010: 440). De facto, cada vez mais se verifica uma tendência para a utilização do "novo" processo penal não apenas com vista à realização da justiça penal mas em favor da actividade executiva, de estruturas estaduais ou supra-estaduais endógenas àquela, enfim, de objectivos e entidades nebulosas, onde se entrecruza e confunde

a segurança do Estado com interesses e estratégias de jaez político e ideológico. O que se afigura «como uma via que, além de problemática no plano político, se apresenta como epistemologicamente perigosa, mas, acima de tudo, põe em causa o Estado de direito» (Mesquita, 2010: 441).

Por outro lado, todo esse pano de fundo tem disseminado «uma cultura processual penal» *securitarista* (Palma, 2004: 52)([8]), designadamente no seio das próprias magistraturas (*v.g.*, Araújo, 2009: 148-149, acompanhando Ferrajoli), que gera não só a crítica sistemática a um ilusório excesso de garantismo dos arguidos mas igualmente voluntarismos exacerbados e outras práticas censuráveis.

Ora, inevitavelmente, toda essa "evolução" se tem manifestado também no domínio do *combate* à chamada *criminalidade informática* e, em grande medida por esta via, no que concerne à obtenção da *prova digital*, como adiante melhor tentaremos evidenciar.

4. Em *sentido amplo*, a *criminalidade informática* «englobará toda a panóplia de actividade criminosa que pode ser levada a cabo por meios informáticos, ainda que estes não sejam mais do que um instrumento para a sua prática, mas que não integra o seu tipo legal, pelo que o mesmo crime poderá ser praticado por recurso a outros meios» (Venâncio, 2011: 17). Já num *sentido estrito*, apenas «abarcará aqueles crimes em que o elemento digital surge como parte integrador do tipo legal ou mesmo como seu objecto de protecção» (Venâncio, 2011: 17)([9]).

Rita Coelho dos Santos (2005: 32 e ss.), no entanto, adianta uma classificação tripartida, talvez mais adequada, nos termos da qual distingue:

([8]) Segundo a autora citada, essa «cultura processual» «corre dois grandes perigos: o de um estado de guerra permanente contra a criminalidade organizada em que cada agente é representado como mera peça da máquina criminosa a combater e a utilização, a torto e a direito, dos quadros legais flexibilizados para combater a criminalidade organizada no tratamento de criminalidade comum».

([9]) Benjamim Silva Rodrigues (2009: 279), porém, parece integrar na *criminalidade informática-digital em sentido próprio* ou *pura* (em *sentido estrito*, portanto) exclusivamente os tipos incriminadores cujo bem jurídico protegido seja informático.

— os crimes *tipicamente informáticos*, ou seja, aqueles que o legislador reconhece como crimes eminentemente ligados à informática, na medida em que o objecto ou instrumento da acção é um computador (em sentido amplíssimo ou «*lógico*», incluindo, nomeadamente, o *software*) ou outro equipamento tecnologicamente semelhante, não podendo o tipo ser preenchido se não se verificar qualquer acção sobre ou através desses equipamentos;

— os crimes *essencialmente informáticos*, que compreendem apenas aqueles em que o próprio bem jurídico ofendido consiste numa realidade de natureza informática com dignidade suficiente para merecer a tutela penal; e

— os crimes *acidentalmente informáticos*, isto é, aqueles em que a utilização do computador é apenas um novo *modus operandi*, não contendendo com o preenchimento do respectivo tipo legal.

De todo o modo, têm razão Mouraz Lopes e Antão Cabreiro (2006: 71), ao concluírem que a «criminalidade dita informática» é «um conceito puramente tópico que pretende abranger uma realidade vasta, difusa e, cada vez mais, ilimitada».

Porém, em face de mais este fenómeno de *neo-criminalização*, importa sobretudo ter-se presente que, nem a informática, a qual se traduz, grosso modo, na «informação automatizada», ou seja, num «específico fluxo informacional», pode ser considerada um bem jurídico-penal, dado ser um bem jurídico latíssimo e expansivo, o que vale por dizer, difuso e indeterminado, nem a generalidade dos crimes informáticos tipificados até hoje evidencia a protecção de bens jurídicos específicos, autónomos, novos, verdadeiramente diversos dos tradicionais (Costa, 1998: 108-110). Na verdade, ao invés de se traduzir no objecto da protecção dos crimes informáticos, a informática acaba por ser reduzida por estes a um "simples" meio (Macedo, 2009: 259)([10]).

([10]) O único crime informático protector de um bem jurídico-penal novo que os autores citados encontram no ordenamento jurídico português é o crime de *reprodução ile-*

Acresce que, como lucidamente conclui Faria Costa (1998: 111), «não vemos que se possa sustentar uma qualquer inovação no que tange ao modo de construir» os crimes informáticos.

Deste modo, o pretenso, mas não cientificamente sustentável, direito penal da informática, que resulta «de um movimento que aparece, de maneira nítida, como manifestação impositiva», sem prejuízo das suas especificidades, pode e deve continuar a ser tratado «com os "instrumentos" tradicionais do direito penal» (Costa, 1998: 111 e 117, respectivamente).

5. Na verdade, «em regra, as novas formas de criminalidade ligadas aos meios tecnológicos destacam-se não porque consistem em condutas substancialmente diferentes daquelas que tradicionalmente preenchem os tipos legais de crime correspondentes, mas porque, e apenas, os instrumentos (os equipamentos electrónicos e as técnicas informáticas) utilizados na prática das infracções criminosas são diversos dos tradicionalmente previstos pelo legislador penal» (Santos, 2005: 24).

Nesse contexto, como salienta João Macedo (2009: 231-232), a execução dos crimes informáticos resume-se «a três grandes categorias: a manipulação, a espionagem e a sabotagem».

A *manipulação informática*, que é a forma mais frequente de execução desses crimes, consiste na modificação de dados, podendo ocorrer na fase de integração de novos dados e de tratamento destes *(manipulação de input)* ou na fase de saída dos mesmos, por alteração dos resultados *(manipulação de output)*([11]).

Já a *espionagem informática*, também chamada "furto de dados", traduz-se no acesso a dados armazenados ou na utilização destes sem o conhecimento e contra a vontade, ainda que tão-só presumida, do seu titular.

---

gítima de programa protegido, hoje tipificado no art. 8.º da Lei n.º 109/2009, de 15/09, o qual tutela o *software*, o *logicel*. Em sentido algo divergente, *vd*. VENÂNCIO, 2011, 21.

([11]) Importa notar, por um lado, que a *manipulação*, ainda que com pesos diferenciados, ocorre em quase todos os crimes informáticos e, por outro lado, que tanto as manipulações anteriores ao *input* como as posteriores ao *output* não serão já crimes informáticos.

Por último, a *sabotagem informática* consiste na corrupção, destruição ou qualquer outra forma de danificação de sistemas informáticos ou dados.

No entanto, estas três grandes formas de execução dos crimes informáticos podem assumir procedimentos muito variados. Com efeito, as NTIC cada vez mais apresentam potencialidades que concedem uma margem imensa à imaginação e, por consequência, à actuação dos agentes dos *cibercrimes*([12]).

Ora, como anota Rita Coelho dos Santos (2005:53), «[a] criminalidade informática fez reavivar a problemática da prova». Desde logo porque implica *meios de obtenção de prova* e *meios de prova* ([13]) *digitais*, com algumas características específicas face aos "meios tradicionais".

6. De acordo com Benjamim Silva Rodrigues (2009: 39), «*[a] prova electrónico-digital* pode definir-se como qualquer tipo de informação, com valor probatório, armazenada [em repositório electrónico-digitais de armazenamento] ou transmitida [em sistemas e redes informáticas ou redes de comunicações electrónicas, privadas ou publicamente acessíveis], sob a forma binária ou digital».

([12]) A este propósito, é relevante o catálogo dos *ciberdelinquentes* apresentado por VLADIMIR ARAS (?: 11), segundo o qual:

— Os *hackers* «são, em geral, simples invasores de sistemas, que atuam por espírito de emulação, desafiando seus próprios conhecimentos técnicos e a segurança de sistemas informatizados de grandes companhias e organizações governamentais;

— «Os *crackers*, por sua vez, são os "*hackers* aéticos". Invadem sistemas para adulterar programas e dados, furtar informações e valores e prejudicar pessoas. Praticam fraudes eletrônicas e derrubam redes informatizadas, causando prejuízos a vários usuários e à coletividade»;

— «[O]s *phreakers* são especialistas em fraudar sistemas de telecomunicação, principalmente linhas telefônicas convencionais e celulares, fazendo uso desses meios gratuitamente ou às custas de terceiros»;

— «Há ainda os *cyberpunks* e os *cyberterrorists*, que desenvolvem vírus de computador perigosos, como os *Trojan horses* (cavalos de Tróia) e as *Logic bombs*, com a finalidade de sabotar redes de computadores e em alguns casos propiciar a chamada *DoS — Denial of Service*, com a queda dos sistemas de grandes provedores, por exemplo, impossibilitando o acesso de usuários e causando prejuízos económicos».

([13]) Sobre a difícil distinção entre *meios de obtenção de prova* e *meios de prova*, *vd.*, *v.g.*, ALBUQUERQUE, 2007: 323.

6.1. Talvez antes de tudo o mais, este tema tem feito destacar à exaustão as dificuldades e complexidades que as NTIC colocam no que concerne à busca, preservação, apreensão, análise, tratamento e apresentação das provas nelas armazenadas ou pelas mesmas transmitidas, isto é, justamente, as *provas digitais* (*v.g.*, Santos, 2005: 52 e ss.). Nas palavras de Mouraz Lopes e Antão Cabreiro (2006: 71), o primeiro, Juiz de Direito e ex-Director Nacional Adjunto da Polícia Judiciária, e o segundo, Coordenador de Investigação Criminal e Subdirector Nacional da Polícia Judiciária, «[o] confronto diário com a investigação criminal no domínio da criminalidade dita informática (…) confronta os sujeitos activos da investigação com uma dura realidade», precisamente a que resulta das ditas dificuldades e complexidades.

Com efeito, salienta-se que aquelas tecnologias permitem a sua utilização à distância, sem qualquer contacto físico com os sistemas informáticos ou dados atingidos. Refere-se que facilitam aos seus utilizadores o encobrimento das respectivas identidades e acções, bastando ter-se presente, por exemplo, que estes podem assumir identidades virtuais, tomar a identidade de terceiros (inclusive através do "roubo" de senhas por *vírus*, *worms* ou mesmo pelos chamados *cavalos de Tróia*), praticar os actos desde um computador ligado à Internet num *cibercafé* de qualquer parte do mundo ou simplesmente apagar a informação em escassos segundos, carregando numa tecla. Aduz-se ainda que as NTIC facultam a alteração da data e hora, inclusive depois de os documentos serem gravados, bem como autorizam a alteração da restante informação, pelos próprios utilizadores ou por terceiros, sem deixar rasto, bastando recordar-se, a título ilustrativo, que as mensagens electrónicas, ao percorrerem o caminho remoto de um computador a outro, estão sujeitas a vários graus de ataque e podem ser facilmente adulteradas por inúmeras pessoas, autorizadas ou não (Taylor, Haggerty, Gresty e Hegarty, 2010: 304 e ss.).

Enfatiza-se igualmente que a *prova digital* pode estar armazenada nos mais variados e facilmente dissimuláveis meios de suporte de informação (Pen, DVD, CD, etc.). Que raramente se encontra no local da prática do crime. Que está frequentemente no domínio de terceiros (*v.g.*, Lopes e Cabreiro, 2006: 72).

Sobreleva-se também que tal prova é facilmente susceptível de erros, falhas e/ou omissões resultantes das próprias NTIC. E, pior, que mesmo quando é possível identificar esses erros, falhas e/ou omissões nem sempre se consegue distinguir os que foram causados por acção humana daqueles que resultaram dos próprios equipamentos ou programas (*v.g.*, Hagy, 2007: 15 e ss).

Adianta-se ainda que, como se tudo isso não bastasse, a *prova digital* não é susceptível de apreensão material. Efectivamente, como diz Breno Lessa (2009), um «documento eletrônico [textos, sons, imagens, etc.] nada mais é do que uma seqüência de números binários (isto é, zero ou um) que, reconhecidos e traduzidos pelo computador, representam uma informação»; tem a «sua forma original em bits, ou seja, não é impresso ou assinado em papel: sua circulação e verificação de autenticidade se dão em sua forma original, eletrônica».

Nota-se, por último, que, em face de tudo isso, as acções de investigação criminal relativas à *prova digital* exigem aprofundados conhecimentos informáticos e, muitas vezes, meios técnicos e tecnológicos de ponta.

Assim, conclui-se que se está perante uma prova «fragmentária, dispersa, frágil, volátil, alterável, instável, apagável e manipulável, invisível e espacialmente dispersa» (Rodrigues, 2011: 29). Sendo, por isso, extremamente difícil, complexo e, até, aleatório detectar, preservar, apreender, analisar, tratar, garantir a fiabilidade, assegurar a compreensibilidade e apresentar em julgamento as *provas digitais*.

6.2. Exponenciando todas essas dificuldades e complexidades apresentadas pela *prova digital* e aduzindo, designadamente, que, por virtude delas, «é no mínimo desgastante saber que cerca de 20% dos inquéritos em investigação ou investigados nesta área [da criminalidade informática] são concluídos com proposta de arquivamento por inexistência de elementos que permitam prosseguir a investigação» (*v.g.*, Lopes e Cabreiro, 2006: 72), por toda a parte muitos são os que têm vindo a reclamar a promoção de múltiplas medidas específicas e *eficientistas* tendentes a ultrapassá-las.

Desde logo, defende-se, resumidamente, que a lei, *maxime* a lei processual penal, deve permitir que as entidades policiais e judiciárias competentes possam desenvolver todas as acções necessárias e adequadas à obtenção de *prova digital* de forma agilizada, fácil, em tempo útil, enfim, *eficazmente*. Sustenta-se que essas acções possam ser realizadas quer nos equipamentos dos arguidos, quer nos de terceiros, sobretudo junto das operadoras de comunicação. E, não menos enfaticamente, pretende-se que estas sejam obrigadas a cooperar no que concerne à preservação e fornecimento de todo o tipo de dados informáticos (*v.g.*, Lopes e Cabreiro, 2006: 73 e ss.).

Ademais, alerta-se para a imprescindibilidade de uma estreita cooperação internacional no desenvolvimento das referidas acções. Salienta-se, efectivamente, que não é hoje possível conseguir a prova (*digital*) de boa parte dos crimes, informáticos e não só, sem o intercâmbio entre as entidades policiais e judiciárias dos vários países conexionados com a prática desses delitos (*v.g.*, Santos, 2005: 55-56).

Paralelamente, pugna-se no sentido de as entidades competentes para a investigação criminal serem dotadas de recursos humanos e meios técnicos e tecnológicos capazes de dar resposta às referidas dificuldades e complexidades. Pede-se a criação, no seio das polícias criminais, de unidades especializadas para o efeito. E reclama-se o desenvolvimento de uma área que alguns autores consideram ser já «um novo tipo de ciência», a «*"digital forensic"* que pretende orientar a investigação criminal, em matéria de criminalidade informático-digital, para a preservação, recolha, gravação, validação, identificação, análise, interpretação, documentação e apresentação deste específico tipo de prova» (Rodrigues, 2011: 31 e ss.).

6.3. Desde logo, importa sublinhar que a ausência de um regime processual penal próprio, autónomo e *eficientista* relativo à *prova digital*, *maxime* à sua obtenção, não parece ser tão dramática quanto se proclama.

Como vimos, Mouraz Lopes e Antão Cabreiro, em 2006, num quadro em que inexistia ainda em Portugal um regime processual

penal específico sobre a matéria, queixavam-se de ser «no mínimo desgastante saber que cerca de 20% dos inquéritos em investigação ou investigados nesta área [da criminalidade informática] são concluídos com proposta de arquivamento por inexistência de elementos que permitam prosseguir a investigação».

De facto, dito assim, até parece dramático e grave.

Todavia, a verdade foi que, nesse mesmo ano, segundo o Relatório Anual da Procuradoria-Geral da República([14]), «[o] número de inquéritos arquivados foi de 366.579, o que representa aproximadamente 51% do valor dos movimentados». Percentagem que atingiu 52,4% em 2007, 55% em 2008 e 53,9% em 2009([15]).

Assim, vistas as coisas neste contexto mais amplo, já tudo parece indiciar que aquela taxa de arquivamento dos inquéritos referentes a crimes informáticos, no mínimo, estará dentro dos parâmetros "normais".

Dito de outro modo, tudo leva a crer que as "medidas tradicionais", nomeadamente o regime processual penal geral referente à obtenção de prova, são suficientes também em relação à *prova digital*. Sem prejuízo, naturalmente, de carecerem de algumas adaptações, que respondam a certas especificidades desta prova.

Deste modo, atrevemo-nos a prever que um regime autónomo e *eficientista* no domínio da *prova digital* nem sequer irá conduzir a resultados particularmente significativos. A menos que, como adiante hipotisaremos, entretanto se degradem também os critérios do julgamento da matéria de facto.

6.4. Ademais, importa sublinhar e nunca esquecer que, pelo menos no actual estádio da evolução técnica e tecnológica, a *prova digital* é uma prova pouco segura.

Com efeito, como profusamente evidencia Vladimir Aras (?: 37-40), «no ciberespaço o exame da identidade e a autenticação dessa identidade não podem ser feitos visualmente, ou pela verificação de documentos ou de elementos identificadores já em

---

([14]) Disponível na Internet, no sítio da Procuradoria-Geral da República.

([15]) Cf. os respectivos Relatórios Anuais da Procuradoria-Geral da República, disponíveis na Internet, no sítio da Procuradoria-Geral da República.

si evidentes, como placas de veículos ou a aparência física, por exemplo.

Quando um indivíduo está plugado na rede, são-lhe necessários apenas dois elementos identificadores: o endereço da máquina que envia as informações à Internet e o endereço da máquina que recebe tais dados. Esses endereços são chamados de *IP — Internet Protocol*, sendo representados por números, que, segundo LESSIG, não revelam nada sobre o usuário da Internet e muito pouco sobre os dados que estão sendo transmitidos».

Assim, prossegue o autor citado, «salvo quando o usuário do computador faça uso de uma assinatura digital, dificilmente se poderá determinar quem praticou determinada conduta.

A assinatura digital confere credendidade ao documento ou mensagem, permitindo que se presuma que o indivíduo "A" foi o autor da conduta investigada. Mas o problema reside exatamente aí. Como a Internet não é *self-authenticating* a definição de autoria fica no campo da presunção. E, para o Direito Penal, não servem presunções, ainda mais quando se admite a possibilidade de condenação.

O único método realmente seguro de atribuição de autoria em crimes informáticos é o que se funda no exame da atuação do responsável penal, quando este se tenha valido de elementos corporais para obter acesso a redes ou computadores».

Acresce que, como assinala o mesmo autor, «[n]o ciberespaço, há razoáveis e fundadas preocupações quanto à autenticidade dos documentos telemáticos e quanto à sua integridade».

Em suma, como definitivamente conclui Breno Lessa (2009), «não há como validarmos a autoria dos documentos eletrônicos» e «não há como garantirmos que qualquer documento foi alterado, tampouco por quem foi alterado».

É certo que o legislador português, através do Dec. Lei n.º 290-D/99, de 02/08, entretanto alterado pelo Dec. Lei n.º 62/2003, de 03/04, regulou a validade, eficácia e valor probatório dos documentos electrónicos, bem como a assinatura electrónica. Porém, as referidas dúvidas sobre a autoria e genuinidade dos documentos digitais resultam de causas técnicas inultrapassáveis, não podendo ser colmatadas por lei, pelo que sempre subsistirão.

6.5. Mas a verdade é que, não obstante tudo o que se deixou dito, as NTIC vieram possibilitar enormemente o desenvolvimento de novos métodos de investigação, muitos deles integrados nos chamados *métodos ocultos* (*v.g.*, Mesquita, 2010: 85), bem como o conhecimento fácil de um manancial de informação, ainda que não definitiva, sobre as pessoas visadas e os respectivos comportamentos. Desse modo, pese embora com elevados riscos, permitem simplificar em grande medida a investigação criminal. O que, obviamente, se tornou muito sedutor para as entidades policiais e judiciárias, entre outras.

Como sublinha Costa Andrade (2009: 156), com o advento do *digital*, «a telecomunicação perde o seu carácter volátil, passando a persistir no rasto das marcas e sinais que deixa atrás de si. Os próprios sistemas de telecomunicação passam a constituir-se em criadores autónomos de dados atinentes à comunicação, dados também eles decisivamente significativos pelo muito que "dizem" e deixam adivinhar sobre o comportamento e a postura do interlocutor interveniente. De qualquer forma, a verdade é que, no seu conjunto, os dados segregados pela comunicação e pelo sistema de comunicação se revelam, muitas vezes, mais significativos que o próprio conteúdo da comunicação em si. O que, de resto, bem espelha o interesse com que, reconhecidamente, a investigação criminal procura maximizar a recolha de *dados ou circunstâncias da comunicação*, também referenciados como *dados de tráfego*».

Realidade esta que, atrevemo-nos a dizê-lo, é inclusive susceptível de gerar uma tendência em crescendo no sentido da sobrevalorização da *prova indiciária*(16), senão mesmo da facilitação da prova dos factos em sede de julgamento.

Mas mais. Apesar de todas as dificuldades e complexidades apontadas relativamente às *provas digitais*, o certo é que, no mínimo, se torna mais cómodo e menos arriscado para os agentes das entidades policiais e judiciárias procurar e obter essas provas do que as "provas tradicionais".

---

(16) Sobre o conceito de *prova indiciária* e o alcance que lhe tem sido conferido, *vd*., *v.g.*, acórdão da Relação do Porto, de 30/01/2008, Processo n.º 0744740, disponível na Internet, no sítio da DGSI.

O que tudo legitima que, no mínimo, se coloque a hipótese de as constantes e bem audíveis reivindicações no sentido, designadamente, da ampliação e facilitação do regime processual penal referente à *prova digital*, da implicação da operadoras de comunicação na preservação e apresentação desta prova e da intensificação e simplificação da cooperação internacional neste domínio, terem em vista permitir quer a obtenção de elevados índices de eficácia ou, dito de outro modo, de condenações sem necessidade de demonstração dos factos imputados aos arguidos através de provas mais seguras, quer o desenvolvimento da investigação criminal sem grandes esforços nem riscos para os respectivos agentes.

Todavia, também estas vertentes tendem a ser omitidas e, portanto, não ponderadas quando se aborda a problemática da *prova digital* e das soluções para as dificuldades e complexidades apresentadas pela mesma.

6.6. Do que vimos dizendo, podemos desde já extrair a conclusão de que as normas referentes à obtenção da *prova digital* devem ser delineadas à luz e no quadro do regime geral de obtenção da prova. Sem prejuízo, como já dissemos, de algumas adaptações, face a certas particularidades daquele tipo específico de prova.

Por isso, do nosso ponto de vista, aquelas normas devem integrar-se no CPP. Só deste modo se conseguirá alcançar a sua necessária harmonização com o regime geral de obtenção das provas. Para além das demais vantagens decorrentes da codificação, que nos dispensamos de elencar aqui.

Na verdade, os meios de obtenção da *prova digital*, não obstante com as adaptações necessárias, reconduzem-se aos "tradicionais" meios de obtenção da prova. Trata-se, com efeito, ou deve tratar-se, de exames, revistas, buscas, apreensões ou intercepções de comunicações.

Acresce que, como já deixámos antever, pese embora se suscite sobretudo no domínio da *cibercriminalidade*, a questão da *prova digital* está longe de se esgotar aí. Coloca-se relativamente a todos os tipos criminais. Basta que pensemos, a título meramente ilustrativo, nas mensagens de correio electrónico ou registos de

comunicações de natureza semelhante cujo conteúdo se reporte à prática de qualquer tipo criminal sem a menor conexão com as NTIC.

6.7. Porém, mais importante ainda é assumir-se, como, parece-nos, em boa fé se mostra devido, que ampliar, facilitar e agilizar medidas de investigação criminal e cooperação internacional no domínio da obtenção da *prova digital* torna-se ainda mais agressivo, intrusivo, desleal e perigoso do que fazê-lo em relação às "provas tradicionais".

Com efeito, pelas próprias características e potencialidades das NTIC, a concretização de tais medidas ofende, acrescida e gravemente, múltiplos direitos, liberdades e garantias, não só dos agentes dos crimes mas também, pelo menos em boa parte dos casos, de suspeitos inocentes ou terceiros acidentais. O direito à palavra, o direito à imagem, o direito à autodeterminação informacional, o direito à reserva da intimidade da vida privada e familiar, o «direito à inviolabilidade do domicílio informático (artigo 34.º, da CRP) que nos surge como uma garantia imprescindível da afirmação do direito à autodeterminação informacional e comunicacional» (Rodrigues, 2011: 31) e tantos outros direitos pessoalíssimos são em regra enormemente lesados por aquelas acções. Mas também o podem ser, e são-no bastas vezes, direitos patrimoniais, desde logo o direito de propriedade.

Ademais, trata-se em regra de acções secretistas e desenvolvidas apenas à luz dos critérios das entidades investigadoras, sem a participação dialéctica dos visados. Desse modo, são profundamente ofensivas do direito a um procedimento leal e justo([17]).

Por outro lado, frequentemente, a *prova digital* tem que ser obtida em sistemas informáticos de terceiros, *maxime* das operadoras de comunicação. O que igualmente ofende direitos destas. Para além de degradar obrigações contratuais e legais das mesmas,

---

([17]) Sobre o que é, ou devia ser (no actual processo penal já não é bem claro), o «*princípio da lealdade* do comportamento processual penal do ministério público», inerente ao ««mais alto princípio de todo o direito processual penal: o da exigência do *fair trial*», de um *procedimento leal*», *vd*. Dias, 1996: 344 e ss., acompanhando Roxin.

designadamente o dever de sigilo, o qual, em regra, protege relevantíssimos valores *sociais* e *subjectivos*.

A tudo isso acresce que, em virtude das referidas acções de investigação criminal, informação de múltipla natureza chega ao conhecimento de um número elevado de pessoas indeterminadas. Ora, esta situação gera enormes riscos de a informação vir a ser utilizada fora dos procedimentos respectivos, para finalidades alheias a estes. O que se mostra particularmente intenso em face do reclamado envolvimento das operadoras de comunicação na investigação criminal. E tão mais intenso quanto é certo que o sector das telecomunicações tem sido «em grande medida afectado pela desregulamentação, pela abertura à concorrência e pelas privatizações, a que acrescem os agrupamentos de vocação mundial que se vão constituindo entre os seus operadores» (Desgardins e Lemaire, 1999: 54-55 e 247-248).

Vale a pena recordar aqui a, como sempre, profundíssima reflexão de Costa Andrade (2009: 127-129): «A "privatização da investigação" conheceu recentemente um novo impulso com a privatização generalizada (pelo menos na Europa) das empresas de telecomunicação. A que estão confiadas as tarefas de intromissão, intercepção e gravação de telecomunicações e, em geral, da produção e "armazenamento" de dados processualmente relevantes, bem como a sua apresentação ao processo penal. E tanto no que respeita ao conteúdo e dados da comunicação como no que respeita aos dados de localização. Um quadro entretanto reforçado com o aparecimento de novos meios e procedimentos tecnológicos de comunicação, com destaque para a produção e transmissão de dados por *internet*, inteiramente nas mãos de privados. E a quem são, mais uma vez, cometidos meios de obtenção de prova, como a intromissão no correio electrónico, as diferentes formas da chamada *busca online*, a *intercepção de comunicações telefónicas através da internet (VoIP)*. (…) [N]ão pode esquecer-se que ela [a intervenção dos privados] comporta os riscos e está exposta aos abusos conaturais aos "sistemas de contacto" (…) entre o público e o privado. Perigos agravados e reforçados à medida do aumento da dimensão das empresas de telecomunicação, algumas delas à escala global (*v.g.*, Google, Microsoft) e da crescente assimetria de poder entre

aquelas empresas e os indivíduos. E mesmo entre elas e os próprios Estados. Tudo a antecipar a possibilidade de as intromissões arbitrárias nas telecomunicações e as utilizações abusivas dos dados deixarem de ser um exclusivo do Estado. E a fazer subir as margens do cuidado e da preocupação. Isto atenta a especificidade dos *goals* ou interesses dos privados e dos seus "códigos" de valoração das coisas e dos factos. Não raro a induzir soluções centrífugas e irreconciliáveis com as que são reclamadas pelo direito e pela justiça. E a fazer impender sobre a Administração da Justiça e a sua decantada autonomia o peso insustentável da heteronomia».

6.8. Ora, os direitos, liberdades e garantias, como aliás os demais direitos fundamentais referidos no art. 17.º da CRP, gozam do regime jurídico-constitucional decorrente, *maxime*, dos arts. 18.º, 19.º, 20.º, n.º 5, 21.º, 22.º, 165.º, n.º 1, al. *b*), 272.º, n.º 3, e 288.º, al. *d*), da Constituição. De entre esse regime, cumpre destacar aqui o princípio da proibição do excesso (art. 18.º, n.º 2, da CRP) — «qualquer limitação, feita por lei ou com base na lei, deve ser adequada (apropriada), necessária (exigível) e proporcional (com justa medida)» (Canotilho, 2003: 417) —, bem como o princípio segundo o qual as normas ordinárias restritivas dos direitos, liberdades e garantias não podem diminuir a extensão e o alcance do conteúdo essencial dos preceitos constitucionais que os consagram (art. 18.º, n.º 3, da CRP).

Seguindo o ensinamento de Gomes Canotilho e Vital Moreira (1991: 133-134), «[a]lém de precisarem de autorização constitucional, as restrições de direitos fundamentais carecem também de *justificação*, não podendo legitimar-se senão pela necessidade de salvaguardar outros direitos ou interesses constitucionalmente protegidos e não podendo ultrapassar a medida necessária para o efeito (art. 18.º-2). (…). Os direitos fundamentais só podem ser restringidos quando tal se torne *indispensável*, e no *mínimo necessário*, para salvaguardar outros direitos ou interesses constitucionalmente protegidos.

No fundo, a problemática da restrição dos direitos fundamentais supõe sempre um *conflito positivo de normas constitucionais*, a saber entre uma norma consagradora de certo direito fundamen-

tal e outra norma consagradora de outro direito ou de diferente interesse constitucional. A regra de solução do conflito é a da *máxima observância* dos direitos fundamentais envolvidos e da sua *mínima restrição* compatível com a salvaguarda adequada do outro direito fundamental ou outro interesse constitucional em causa.

Por conseguinte, a restrição de direitos fundamentais implica necessariamente uma *relação de conciliação* com outros direitos ou interesses constitucionais e exige necessariamente uma tarefa de ponderação ou de *concordância prática* dos direitos ou interesses em conflito».

Assim, dentro ou fora do CPP, na *relação de conciliação* e na tarefa de ponderação ou de *concordância prática* entre, por um lado, a concretização do *interesse objectivo* na *eficácia da investigação criminal* e, portanto, na obtenção de *prova digital*, sem dúvida um interesse constitucionalmente tutelado, decorrente, desde logo, do princípio do Estado de Direito (art. 2.º da CRP), e, por outro lado, a salvaguarda dos direitos fundamentais que tal concretização afecta, o legislador ordinário tem de considerar, antes de mais, a enorme agressividade das sobreditas medidas investigatórias para muitos destes direitos. Mas igualmente não pode deixar de levar em linha de conta quer o "normal" grau de eficácia, mesmo no domínio da *criminalidade informática*, dos "meios tradicionais" de obtenção de prova, quer a parca fiabilidade daquele tipo de prova, quer ainda os efeitos nefastos que o acesso fácil ao manancial de informação precária permitido pelas NTIC pode gerar, tanto no âmbito da própria investigação criminal como sobretudo no quadro do julgamento da matéria de facto.

Por outro lado, continuando a seguir o ensinamento de Gomes Canotilho e Vital Moreira (1991: 143), «[u]ma das regras essenciais da interpretação das normas infraconstitucionais é a *interpretação conforme à Constituição* (…). No campo dos direitos fundamentais tal regra quer dizer, *interpretação mais favorável aos direitos fundamentais*. Significa isto que, em caso de dúvida, deve prevalecer a interpretação que, conforme os casos, restrinja menos o direito fundamental, lhe dê maior protecção, amplie mais o seu âmbito, o satisfaça em maior grau. No caso dos direitos de liber-

dade, esta regra equivale, em certo sentido, ao velho princípio *in dubio pro libertate*».

Desse modo, em sede jurisdicional, a interpretação e aplicação de eventuais normas *eficientistas* de um regime processual penal atinente à *prova digital* deve favorecer os direitos fundamentais colidentes. Sendo certo que igualmente deve considerar o "normal" grau de eficácia, mesmo no domínio da *criminalidade informática*, dos "meios tradicionais" de obtenção de prova, a reduzida segurança daquela prova e as consequências negativas que a facilitação do acesso à imensa informação precária permitida pelas NTIC pode provocar, quer no âmbito da investigação criminal, quer no quadro do julgamento da matéria de facto.

7. No plano do Direito Internacional, têm sido produzidos múltiplos documentos relativos à *criminalidade informática* e, concomitantemente, à *prova digital*. Pela sua maior relevância para a ordem jurídica portuguesa e para a matéria ora em análise, importa sublinhar aqui três deles.

Assim, no quadro do Conselho da Europa, foi aprovada em Budapeste, a 23/11/2001, a chamada Convenção sobre o Cibercrime([18]). Portugal foi, aliás, um dos primeiros países a subscrever essa Convenção, pese embora apenas tenha procedido à respectiva ratificação em 2009, pela Resolução da Assembleia da República n.º 88/2009 e pelo Decreto do Presidente da República n.º 92/2009, ambos publicados a 15/09.

Tal diploma tem em vista harmonizar as legislações nacionais, fundamentalmente no que concerne à:

— delimitação de conceitos jurídico-informáticos;

— tipificação de *cibercrimes*;

— fixação de regras sobre a aplicação espacial da lei penal relativamente a estes crimes;

([18]) Benjamim Silva Rodrigues (2011: 54-56) considera a expressão errada, quer por incorrectamente traduzida, quer por redutora, propondo antes a fórmula *«Convenção sobre a Cibercriminalidade»*. Todavia, a expressão comummente utilizada em Portugal tem sido Convenção sobre o Cibercrime, razão única por que a acolhemos aqui.

— consagração de medidas processuais de obtenção de *prova digital*;

— implementação de medidas de cooperação internacional com o mesmo objectivo e, genericamente, de *combate* à *criminalidade informática*.

Já no âmbito da União Europeia, cumpre destacar a Decisão-Quadro n.º 2005/222/JAI, do Conselho, de 24/02, relativa a ataques contra sistemas de informação.

Também este diploma, que no essencial acompanha a Convenção sobre o Cibercrime, tem por objectivo a harmonização das legislações dos Estados membros, pese embora desta feita apenas relativamente à:

— delimitação de conceitos jurídico-informáticos;

— tipificação de crimes informáticos;

— fixação de regras sobre a aplicação espacial da lei penal relativamente a estes crimes;

— implementação de medidas de cooperação internacional com vista à obtenção de *prova digital* e, genericamente, ao *combate* à *criminalidade informática*([19]).

Por fim, também no domínio da União Europeia, deve igualmente destacar-se a Directiva n.º 2006/24/CE, do Parlamento e do Conselho, de 15/03. Reporta-se este último diploma, que aliás foi aprovado "à pressa"([20]), à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações.

Em nota final, pelo relevo que aqui assume, deve referir-se que todos os aludidos diplomas internacionais proclamam a necessidade de aplicação do princípio da proporcionalidade no que con-

---

([19]) Como bem assinala PAULO DÁ MESQUITA (2010: 97, nota 30), a Decisão-Quadro n.º 2005/222/JAI não compreende normas processuais.

([20]) Como referem MOURAZ LOPES e ANTÃO CABREIRO (2006: 71), a Directiva n.º 2006/24/CE resultou de uma «discussão e aprovação rápida», já que pretendeu dar resposta à ocorrência dos atentados terroristas de Londres.

cerne à compatibilização das medidas que prevêem com os «direitos humanos» (preâmbulo e art. 15.º da Convenção sobre o Cibercrime, preâmbulo da Decisão-Quadro nº 2005/222/JAI e preâmbulo e art. 4.º da Directiva n.º 2006/24/CE).

8. Entre nós, a Lei n.º 109/2009, de 15/09, transpôs para a ordem jurídica interna a sobredita Decisão-Quadro n.º 2005/222/JAI, do Conselho da E.U., e adaptou ao direito português a mencionada Convenção sobre o Cibercrime, do Conselho da Europa.

Resumidamente, a Lei n.º 109/2009:

— introduziu e, sobretudo, ampliou diversos conceitos jurídico-informáticos (sistema informático, dados informáticos, dados de tráfego, etc.);

— alargou os tipos incriminadores dos *cibercrimes* que antes se encontravam previstos na Lei n.º 109/91, de 17/08, a qual revogou;

— estabeleceu, quanto à sua aplicação no espaço, o princípio da competência universal;

— consagrou múltiplas medidas processuais de obtenção de *prova digital* e, genericamente, de *combate* ao *cibercrime*;

— fixou diversas obrigações para terceiros, *maxime* às operadoras de comunicação, com vista à preservação e apresentação de *prova digital*;

— definiu várias medidas de cooperação internacional no que concerne à obtenção de *prova digital* e, genericamente, ao *combate* à *criminalidade informática*, tendo aliás determinado para o efeito a criação na Polícia Judiciária de um «ponto de contacto» disponível em permanência, 24 horas por dia, 7 dias por semana.

Para o que aqui mais importa, desde logo se constata que a Lei n.º 109/2009 consagra um *regime processual penal geral* de obtenção de *prova digital*, potencialmente dirigido a *todos* os crimes. Desse modo, impunha-se a integração das suas normas no CPP, concretamente no Título III («Meios de obtenção de prova») do

respectivo Livro II («Da prova»)([21]). Pelo que só uma intenção mal dissimulada do legislador em ampliar e facilitar os meios de obtenção daquela prova o pode ter levado a optar por produzir (mais) um diploma especial.

Na verdade, verifica-se que a Lei n.º 109/2009, com vista à obtenção de *prova digital*, consagrou múltiplos e extensíssimos meios processuais, deveres para terceiros e mecanismos de cooperação internacional profundamente agressivos, intrusivos, desleais e perigosos.

Assim, como *medidas processuais gerais*, esse diploma veio permitir:

— a preservação expedita de dados (art. 12.º);

— a revelação expedita de dados de tráfego (art. 13.º);

— a injunção para apresentação ou concessão do acesso a dados, sob cominação, à boa maneira *securitária*, do crime (mais um) de desobediência (art. 14.º)([22]);

— a pesquisa de dados informáticos (art. 15.º);

— a apreensão de dados informáticos (art. 16.º);

— a apreensão de correio electrónico e registos de comunicações de natureza semelhante (art. 17.º).

A par, o mesmo diploma estabeleceu a possibilidade de imposição de diversas obrigações a quem tenha a disponibilidade ou o controlo sobre dados informáticos, *maxime* às operadoras de comunicação. De entre essas obrigações, destacam-se:

([21]) Aliás, como refere PAULO DÁ MESQUITA (2010: 97-98), a própria apresentação da Lei n.º 109/2009 foi «algo esquizofrénica ao dizer-se num passo que se visa superar a «desadequação da ordem jurídica nacional às novas realidades» depois da revisão de 2007 do Código de Processo Penal, afirmando-se noutro que a nova lei está «totalmente em linha» com a referida lei «desadequada»». Embora numa perspectiva algo diversa, também BENJAMIM SILVA RODRIGUES (2011: 116 e ss.) critica a solução legislativa adoptada.

([22]) De resto, a cominação do crime de desobediência é uma medida ineficaz, mostrando-se mais apropriada, por exemplo, a fixação de uma sanção pecuniária compulsória (MESQUITA, 2010: 113). Em suma, é tal a ânsia do legislador *neoliberal* em criminalizar comportamentos, servindo-se do Direito Penal como *prima ratio*, que o faz mesmo quando esse procedimento se mostra menos eficiente do que soluções de outras naturezas, designadamente de natureza civil.

— a preservação expedita de dados, mediante ordem da autoridade judiciária competente ou, em certos casos, do próprio órgão de polícia criminal;

— a indicação à autoridade judiciária ou ao órgão de polícia criminal, por parte do fornecedor de serviço a quem aquela preservação tenha sido ordenada, espontaneamente, logo que o souber, de outros fornecedores de serviço através dos quais a comunicação dos dados tenha sido efectuada;

— a apresentação ou concessão de dados, mediante injunção da autoridade judiciária competente, sob pena, como já se referiu, de punição por desobediência.

Ademais, a Lei n.º 109/2009, como o legislador fez questão de nela proclamar expressamente (art. 11.º, n.º 2), é cumulativa com a Lei n.º 32/2008, de 17/07([23]), a qual transpôs para a ordem jurídica portuguesa a já aludida Directiva nº 2006/24/CE, do Parlamento e do Conselho, de 15/03, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações. E ambas essas leis cumulam-se ainda com o Dec. Lei n.º 7/2004, de 07/01 (Lei do Comércio Electrónico).

Ora, a Lei n.º 32/2008 impõe ainda aos fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações a obrigação de conservarem, pelo período de um ano, os dados necessários para (*i*) encontrar e identificar a fonte de uma comunicação, (*ii*) encontrar e identificar o destino de uma comunicação, (*iii*) identificar a data, a hora e a duração de uma comunicação, (*iv*) identificar o tipo de comunica-

---

([23]) Sobre os problemas que podem decorrer dessa cumulação, *vd*. MESQUITA, 2010: 110-111. Por outro lado, importa igualmente ter-se presente a Portaria n.º 469/2009, de 06/05, a qual estabelece os termos das condições técnicas e de segurança em que se processa a comunicação electrónica para efeitos da transmissão de dados de tráfego e de localização relativos a pessoas singulares e a pessoas colectivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, nos termos previstos na Lei n.º 32/2008.

ção, (*v*) identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento, e (*vi*) identificar a localização do equipamento de comunicação móvel, neles se incluindo os dados telefónicos e da Internet relativos a chamadas telefónicas falhadas (arts. 4.º, 5.º e 6.º).

Por seu lado, também o citado Dec. Lei n.º 7/2004 ([24]), referente ao comércio electrónico, o qual transpôs para a ordem jurídica interna a Directiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 08/06, bem como o artigo 13.º da Directiva n.º 2002/58/CE, de 12/07, fixa às prestadoras de «serviços da sociedade da informação» muitas outras obrigações de jaez equivalente (*v.g.*, art. 13.º), bem como medidas restritivas (*v.g.*, art. 7.º).

Todas essas obrigações não só fragilizam direitos e deveres contratuais e legais das referidas entidades como do mesmo passo se traduzem em outras tantas medidas agressivas, intrusivas, secretistas e desleais relativamente a direitos fundamentais das pessoas contra quem se pretende utilizar os dados em causa. Mas mais. Muitas delas assumem carácter meramente preventivo, situam-se fora do processo penal e mostram-se manifestamente desproporcionais ou, mesmo, desnecessárias, o que as torna inconstitucionais, por ofensa às normas do n.º 2 do art. 18.º e do n.º 4 do art. 34.º da CRP (Rodrigues, 2011: 34 e ss.).

Por outro lado, em face do disposto no art. 11.º, n.º 1, da Lei n.º 109/2009, como aliás já adiantámos oportunamente, as sobreditas *medidas processuais gerais* e obrigações aplicam-se a *todos os processos relativos a crimes*:

— tipificados nessa lei;

— cometidos por meio de um sistema informático;

— em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico.

Assim, essas medidas e obrigações são, como diz Pedro Venâncio (2011: 90-91), «de aplicação geral. Trata-se da criação de

---

([24]) O Dec. Lei n.º 7/2004 sofreu diversas alterações introduzidas pelo Dec. Lei n.º 62/2009, de 10/03.

meios de obtenção de prova digitais para o combate da criminalidade, seja qual for a sua forma (…)». Efectivamente, conforme refere Paulo Dá Mesquita (2010: 98), «[a]s regras de direito probatório previstas no diploma não são assim meras normas processuais sobre *cibercrimes* ou sequer apenas relativas a crimes praticados em *sistemas informáticos*, mas correspondem a um regime consideravelmente mais abrangente sobre *prova electrónica* em processo penal aplicável a qualquer crime».

Isto é, todas aquelas medidas e obrigações podem ocorrer irrestritamente na investigação da generalidade dos tipos criminais, independentemente da moldura penal ou da natureza destes. Processos de pequena criminalidade ou referentes a crimes semipúblicos e, mesmo, particulares admitem, pois, essas medidas.

Na verdade, os princípios da necessidade e da proporcionalidade parecem ter servido apenas para o legislador justificar a introdução de medidas processuais ainda mais radicais.

Com efeito, o art. 18.º da Lei n.º 109/2009 permite igualmente o recurso à intercepção de comunicações em processos relativos a crimes:

— previstos nessa lei;

— cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, quando tais crimes se encontrem previstos no art. 187.º do CPP.

Por sua vez, o art. 19.º da Lei n.º 109/2009 vai mesmo ao ponto de admitir o recurso às acções encobertas previstas na Lei n.º 101/2001, de 25/08, nos termos estabelecidos nesta, no decurso de inquéritos relativos aos seguintes crimes:

— os previstos na Lei nº 109/2009;

— os cometidos por meio de um sistema informático, quando lhes corresponda, em abstracto, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e

> nas comunicações, a discriminação racial, religiosa ou sexual, as infracções económico-financeiras, bem como os crimes consagrados no título IV do Código do Direito de Autor e dos Direitos Conexos.

A propósito desta última medida, vale a pena recordar a ponderação de Paulo Dá Mesquita (2010, 126): «Uma originalidade nacional que não decorreu de qualquer previsão da Convenção do Conselho da Europa, nem da Decisão-Quadro (…). No n.º 1 do art. 19.º, sem qualquer fundamento sistemático ou teleológico, amplia-se de forma drástica o catálogo de crimes previsto no art. 2.º do Regime Jurídico sobre Acções Encobertas (Lei n.º 101/2001, de 25-8). No plano político criminal, a solução adoptada apresenta-se incorrecta ao descaracterizar a tabela desse regime procedendo a uma associação inopinada entre crimes informáticos e crimes cometidos por meio de um sistema informático e acção encoberta (…). No plano jurídico-constitucional transgride, claramente, a linha do admissível, ao prever uma medida de carácter muito excepcional para um leque muito amplo de crimes, sem aprofundamento normativo dos princípios da proporcionalidade e da necessidade. Com efeito, passam a admitir-se *quaisquer* acções encobertas para um amplo catálogo de crimes, alguns dos quais integrados na pequena criminalidade (…), parecendo ainda pretender-se o emprego da medida para crimes negligentes com pena superior a 5 anos (…)».

Acresce, prossegue o autor citado (2010: 127), que «[n]o n.º 2 do art. 19.º, aprofundando a incongruência sistemática consagra-se uma norma espúria no ordenamento jurídico português ao prever, sem qualquer outro enquadramento, «o recurso a meios e dispositivos informáticos» em acções encobertas», podendo «estar-se, por esta via, a abrir-se, sem suficiente ponderação (ou freios claros) a porta à intercepção de comunicações para fins de prevenção (…), constitucionalmente incompatível com o disposto no art. 34.º da Constituição».

Por último, importa ter-se presente que *todas* as medidas, gerais ou excepcionais, e obrigações previstas na Lei n.º 109/2009, cumulam-se ainda, em tudo o que as não contrarie, com as estabelecidas no CPP.

Já no domínio das medidas de cooperação internacional fixadas na Lei n.º 109/2009, destacam-se:

— a preservação e revelação expeditas de dados informáticos em cooperação internacional (art. 22.º);

— a pesquisa, apreensão e divulgação de dados informáticos em cooperação internacional (art. 24.º);

— o acesso das autoridades estrangeiras competentes, sem necessidade de pedido prévio às autoridades portuguesas, a dados informáticos armazenados em sistema informático localizado em Portugal, quando publicamente disponíveis (art. 25.º, al. *a*));

— a recepção ou acesso das autoridades estrangeiras competentes, sem necessidade de pedido prévio às autoridades portuguesas, através de sistema informático localizado no seu território, a dados informáticos armazenados em Portugal, mediante consentimento legal e voluntário de pessoa legalmente autorizada a divulgá-los (art. 25.º, al. *b*)).

Sendo certo que estas medidas de cooperação internacional se aplicam indistintamente em *todos* os casos de investigações ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos e, bem assim, de recolha de prova, em suporte electrónico, de um crime, de acordo com as normas sobre transferência de dados pessoais previstas na Lei n.º 67/98, de 26/10 (art. 20.º da lei n.º 109/2009).

Acresce que estas medidas adicionam-se às estabelecidas na Lei n.º 144/99, de 31/08([25]), referente à cooperação judiciária internacional em matéria penal (*v.g.*, Venâncio, 2011: designadamente 91 e ss.).

Mas há mais, e pior. Evidenciando uma das mais vincadas imagens de marca do processo penal *neoliberal*, a Lei n.º 109/2009, quer no âmbito das suas normas processuais, quer no das referentes

---

([25]) A Lei n.º 144/99 sofreu já múltiplas alterações, respectivamente pelas Leis n.º 104/2001, de 25/08, n.º 48/2003, de 22/08, n.º 48/2007, de 29/08, e n.º 115/2009, de 12/10.

à cooperação internacional, veio conceder enormes poderes aos órgãos de polícia criminal, relativamente à preservação, pesquisa e apreensão de dados informáticos.

Com efeito, reunidos os pressupostos previstos nesse diploma, o órgão de polícia criminal dispõe de *competência própria* para:

— ordenar a preservação expedita de dados informáticos (art. 12.º, n.º 2)([26]);

— proceder à pesquisa de dados informáticos (art. 15.º, n.º 3);

— efectuar a apreensão de dados informáticos (art. 16.º, n.º 2).

Para além de atribuir essas *competências próprias* ao órgão de polícia criminal, o diploma em análise permite ainda que este *ordene* a preservação, pesquisa ou apreensão de dados informáticos mediante delegação da autoridade judiciária competente (arts. 12.º, n.º 2, 15.º, n.º 1, 16.º, n.º 1, e 22.º, n.º 4)([27]).

Bem se justificam, pois, as apreensões manifestadas por Benjamim Silva Rodrigues (2011: 36): «Temos dúvidas que o presente regime de monitorização dos dados de tráfego, localização e conexos, não venha, a final, servir outros "desideratos" e resvalar para uma nova forma de "terrorismo societário" (mediante alienação do fim) que tem a especificidade de ser, de forma algo contraditória, levado a cabo pelo Estado português que, cada vez menos, surge como o *"guardião do cofre da nossa privacidade electrónico-digital"*».

([26]) Em relação à preservação expedita de dados informáticos, é de notar que o anteprojecto do diploma em apreço nem sequer fazia depender a possibilidade de *decisão autónoma* do órgão de polícia criminal da urgência ou perigo de demora.

([27]) A Proposta de Lei n.º 289/10/4.ª, que veio a dar lugar à Lei n.º 109/2009, atribuía ainda ao órgão de polícia criminal competência para *ordenar*, mediante delegação da autoridade judiciária competente, *a renovação* da preservação de dados, por períodos de 3 meses, até ao limite de um ano. Porém, relativamente a mais essa competência foi acolhida a proposta de eliminação apresentada pelo Grupo Parlamentar do PCP (cf. RODRIGUES, 2011: 111, que transcreve na íntegra as propostas de alteração à referida Proposta de Lei apresentadas pelos Grupos Parlamentares).

9. Em conclusão, pese embora sejam necessárias medidas adequadas à obtenção da *prova digital* no domínio do processo penal, verifica-se que a Lei n.º 109/2009 e os diplomas conexos tiveram sobretudo em vista responder aos apelos dos que reivindicavam a densificação, facilitação, agilização, enfim, o *eficientismo* dessas medidas, integrando-se na linha *securitarista* que caracteriza o processo penal *neoliberal*.

Nesse quadro, sem prejuízo da inconstitucionalidade material de múltiplas normas daqueles diplomas, exige-se uma redobrada ponderação dos valores em jogo em sede de interpretação e aplicação de todos os seus dispositivos por parte das autoridades competentes, as quais deverão aplicar efectivamente o princípio da proibição do excesso.

Para além de se exigir igualmente particular cautela por parte do julgador na apreciação das provas digitais, *maxime* as *indiciárias*, dada a fragilidade desta prova.

BIBLIOGRAFIA

ALBUQUERQUE, Paulo Pinto de, Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, 3.ª ed., Lisboa, Universidade Católica, 2007.

ALMEIDA, Carlota Pizarro de, A Cooperação Judiciária Internacional, *in* Jornadas de Direito Processual Penal e Direitos Fundamentais, Coordenação Científica de Maria Fernanda Palma, Coimbra, Almedina, 2004.

ANDRADE, Manuel da Costa, "Bruscamente no Verão Passado", A Reforma do Código de Processo Penal — Observações críticas sobre uma Lei que podia e devia ter sido diferente, Coimbra, Coimbra Editora, 2009.

ARAÚJO, Dyellber Fernando de Oliveira, Institutos Penais de Emergência — "Novas" Fórmulas Para Velhos Dilemas — Uma Análise dos Novos Estudos de Política Criminal Voltada aos Indesejados da Sociedade, *in* Direito Penal Hoje, Novos Desafios e Novas Propostas, organizado por Manuel da Costa Andrade e Rita Castanheira Neves, Coimbra, Coimbra Editora, 2009.

ARAS, Vladimir, Crimes de Informática — Uma nova criminalidade, disponível na Internet, *in* <http://www.informatica-juridica.com>, consultado no dia 26/04/2011.

BARATTA, Alessandro, Criminología Crítica y Crítica del Derecho Penal — Introducción a la sociología jurídico-penal, Avellaneda, Argentina, Siglo XXI, 2004.

CANOTILHO, J. J. Gomes, Direito Constitucional e Teoria da Constituição, 7.ª ed., Coimbra, Almedina, 2003.

CANOTILHO, J. J. Gomes, e MOREIRA, Vital, Fundamentos da Constituição, 2.ª ed., Coimbra, Coimbra Editora, 1991.

CASTRO, Aldemário Araújo, A Internet e os tipos penais que reclamam ação criminosa em público, *in* Revista de Direito Eletrônico, Rede 02, ano 1, n.º 2, Setembro/Novembro de 2003, publicação oficial do Instituto Brasileiro de Direito Eletrônico, disponível na Internet, *in* <http://www. ibde.org.br/revista>, consultado no dia 26/04/2011.

CHESNAIS, François, A Mundialização do Capital e as Causas das Ameaças de Barbárie, *in* O Livro Negro do Capitalismo, 3.ª ed., Porto, Campo das Letras, 1999.

COSTA, José Francisco de Faria, Algumas Reflexões sobre o Estatudo Dogmático do Chamado "*Direito Penal Informático*", *in* Direito Penal da Comunicação (Alguns Escritos), Coimbra, Coimbra Editora, 1998.

COSTA, José de Faria, A criminalidade em um mundo globalizado: ou *plaidoyer* por um direito penal não-securitário, *in* Revista de Legislação e de Jurisprudência, Ano 135.º, N.º 3934, Setembro-Outubro 2005, Coimbra, Coimbra Editora, 2005.

DESGARDINS, Bruno, e LEMAIRE, Jean-Paul, Desenvolvimento Internacional da Empresa. O Novo Ambiente Internacional, Lisboa, Instituto Piaget, 1999.

DIAS, Jorge de Figueiredo, Do princípio da «objectividade» ao princípio da «lealdade» do comportamento do ministério público no processo penal, *in* Revista de Legislação e de Jurisprudência, Ano 128.º, N.º 3860, Março de 1996, Coimbra, Coimbra Editora, 1996.

FELIX, Sueli Andruccioli, 3.º Encontro de Segurança Pública e Cidadania — Violência e Políticas Públicas de Segurança: pesquisa e ação — Relatório Científico, disponível na Internet, *in* <http://www.levs.marilia.unesp. br>, 2007, consultado no dia 21/03/2011.

FRANCO, Alberto Silva, Globalização e criminalidade dos Poderosos, *in* Revista Portuguesa de Ciência Criminal, Ano 10, 2, Abril-Junho 2000, Coimbra, Coimbra Editora, 2000.

FONTANEL, Jacques, A Globalização em «Análise» — Geoeconomia e estratégia dos actores, Lisboa, Instituto Piaget, 2007.

GADREY, Jean, Nova Economia Novo Mito?, Lisboa, Instituto Piaget, 2001.

GONÇALVES, Maria Eduarda, Direito da Informação. Novos Direitos e Formas de Regulação na Sociedade da Informação, Coimbra, Almedina, 2003.

HAGY, David W., Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors, *in* National Institute of Justice, Jan-2007, U.S. Department of Justice, 2007.

HASSEMER, Winfried, Processo Penal e Direitos Fundamentais, *in* Jornadas de Direito Processual Penal e Direitos Fundamentais, Coordenação Científica de Maria Fernanda Palma, Coimbra, Almedina, 2004.

LESSA, Breno Lessa, A invalidade das provas digitais no processo judiciário, 2009, disponível na Internet, in <http://jus.uol.com.br/revista>, consultado no dia 26/04/2011.

LOPES, Domingos, Direitos Humanos em Questão — Dever de Ingerência Humanitária?, Porto, Campo das Letras, 2008.

LOPES, José Mouraz, e CABREIRO, Carlos Antão, A Emergência da Prova Digital na Investigação da Criminalidade Informática, *in* Sub Judice — Justiça e Sociedade, n.º 35, Abril-Junho de 2006, Coimbra, Almedina, 2006.

MACHADO, Carla, Crime e Insegurança — Discursos do medo, imagens do «outro», Lisboa, Editorial Notícias, 2004.

MACEDO, João Carlos Cruz Barbosa de, Algumas Considerações Acerca dos Crimes Informáticos em Portugal, *in* Direito Penal Hoje, Novos Desafios e Novas Propostas, organizado por Manuel da Costa Andrade e Rita Castanheira Neves, Coimbra, Coimbra Editora, 2009.

MESQUITA, Paulo Dá, Processo Penal Prova e Sistema Judiciário, Coimbra, Coimbra Editora, 2010.

MUÑOZ, Nuria Pastor, Tem o Direito Penal Económico Capacidade de Fazer Frente à Nova Realidade Económica, *in* Revista Portuguesa de Ciência Criminal, Ano 19, 2, Abril-Junho de 2009, Coimbra, Coimbra Editora, 2009.

NETO, João Araújo Monteiro, Crimes informáticos uma abordagem dinâmica ao direito penal informático, 2003, disponível na Internet, *in* <http://www.unifor.br>, consultado no dia 26/04/2011.

PALMA, Maria Fernanda, O Problema Penal do Processo Penal, *in* Jornadas de Direito Processual Penal e Direitos Fundamentais, Coordenação Científica de Maria Fernanda Palma, Coimbra, Almedina, 2004.

PASSET, René, A Ilusão Neoliberal — O Homem é Joguete ou Actor da História, Lisboa, Terramar, 2002.

ROBERT, Philippe, O Cidadão, o Crime e o Estado, Lisboa, Editorial Notícias, 2002.

RODRIGUES, Benjamim Silva Rodrigues, Da Prova Penal, IV, Da Prova-Electrónico-Digital e da Criminalidade Informático-Digital, Lisboa, Rei dos Livros, 2011.

____ Direito Penal. Parte Especial, I, Direito Penal Informático-Digital, Coimbra, Coimbra Editora, 2009.

SANTOS, Rita Coelho dos, O Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos, Boletim da Faculdade de Direito, Coimbra, Coimbra Editora, 2005.

SILVA, Germano Marques da, Meios Processuais Expeditos no Combate ao Crime Organizado (A Democracia em Perigo), *in* Lusíada, Série II, n.º 3, Lisboa, Universidade Lusíada, 2005.

TAYLOR, M., HAGGERTY, J., GRESTY, D., e HEGARTY, R., Digital evidence in cloud computing systems, *in* Computer Law & Security Review, n.º 26, 2010, disponível na Internet, *in* <www.sciencedirect. com>, consultado no dia 26/04/2011.

VENÂNCIO, Pedro Dias, Lei do Cibercrime Anotada e Comentada, Coimbra, Coimbra Editora, 2011.

ZÖLLER, Mark A., O intercâmbio de informações no domínio da investigação penal entre Estados-membros da União Europeia, *in* 2.º Congresso de Investigação Criminal, coordenado por Maria Fernanda Palma e outros, Coimbra, Almedina, 2009.

WACQUANT, Löic, As Prisões da Miséria, Rio de Janeiro, Zahar, 2001.

WESTER, Bruce, Punição e Desigualdade na América, Coimbra, Almedina, 2009.