O «HACKING» ENQUANTO CRIME DE ACESSO ILEGÍTIMO. DAS SUAS ESPECIALIDADES À UTILIZAÇÃO DAS MESMAS PARA A FUNDAMENTAÇÃO DE UM NOVO DIREITO

PEDRO SIMÕES DIAS
Abogado (*)

1 · CONSIDERAÇÕES PRÉVIAS [1]

Let's keep it under the KISS 2 principle. Este texto é um texto jurídico. É um texto jurídico-penal. Os temas a abordar são complexos. Esta complexidade decorre não só da sempre difícil associação do mundo informático à ordem jurídica, mas também dos próprios tópicos penais, que não têm sido tratados de modo acessível. Foi intenção redigir este texto num registo terminológico acessível ao intérprete não especializado e aliviá-lo de todas as considerações laterais aos temas em discussão.

Sendo um texto de cariz jurídico-penal, versa uma matéria que apreciações mais ligeiras consideram inserir-se no amplo universo do direito relacionado com a Sociedade da Informação. Saber se, afinal de contas, existe um espaço identificativo de um direito relacionado com tal temática, ou até um ramo de direito autonomizado é um trabalho em construção, mas deve ser uma tarefa a levar a cabo.

A existência de um direito autónomo, não um Direito da Sociedade da Informação, mas um Direito das Tecologias da Informação e da Comunicação, ou um corpo jurídico tendencialmente autónomo, não é uma mera perspectiva formal ou de recondução a posteriori. Não é uma mera referência de nomenclatura. Se houver uma perspectiva prévia dos conteúdos essenciais de um tal direito, a própria construção normativa que se possa efectuar nesse domínio deve ficar influenciada por tais conceitos. Ou seja, a relação entre a criação normativa e um direito deve ser marcada por transferências simultâneas, outputs e inputs. No tocante ao Direito das Tecologias da Informação e da Comunicação, quanto mais cedo seja ensaiada uma estrutura própria, mais cedo a ela deve ser reconduzida a criação jurídica que regula as questões de um tal domínio.

Um direito autónomo é um «conjunto de normas jurídicas dotadas de individualidade específica e estruturadas de acordo com princípios gerais próprios, e, de preferência, obedecendo ao princípio da unidade» [3]. A este critério de identificação pode chegar-se mais rapidamente se a própria lógica da

* Del Departamento de Derecho Mercantil de Uría Menéndez (Lisboa).

1 O presente texto segue algumas das linhas constantes da dissertação de mestrado defendida na Faculdade de Direito da Universidade de Lisboa e que se encontra em fase de provas para publicação, intitulada «A Criminalidade Levitacional: Os Crimes Informáticos Técnicos. Considerações sobre o hacking, worms e vírus e a responsabilidade criminal dos ISPs» (o texto será objecto de publicação durante o ano de 2006), que contém uma análise muitíssimo mais extensa e profunda destas temáticas. As citações efectuadas no presente artigo sem qualquer identificação específica reportam-se a este texto.

2 «Keep it simple stupid».

3 Seguimos a posição de Faria Costa: «Algumas reflexões sobre o estatuto dogmático do chamado Direito Penal Informático», *Direito Penal da Comunicação*, Coimbra, 1998.

criação jurídica começar por obedecer e reconhecer os pequenos fenómenos que o possam identificar. É uma espécie de viciação justificada do resultado. Os inputs são tão importantes como a verificação dos contributos já existentes.

Ora, o presente texto segue esta lógica de construção, tentando ser, nesse sentido, completamente funcionalista: pegando num elemento simbólico, vamos testá-lo no sentido de saber se o mesmo tem algum perfume próprio e, em caso afirmativo, se pode ser caracterizador do tal Direito das Tecologias da Informação e da Comunicação.

Por outro lado, se conseguirmos identificar um fenómeno próprio informático – que a surgir, seguramente decorrerá da utilização e das plataformas de acesso à Internet e aos mecanimos comunicacionais permitido pelas redes de comunicações electrónicas, não vale a pena fugir ao óbvio – com expressão no domínio criminal e que esse fenómeno nos leve à intelecção da existência de bolsas de diferenciação relativamente ao plano criminal tradicional ou até então percebido, uma tal revelação permitir-nos-á contrariar um bordão tão apregoado quanto insensato como «tudo o que é ilícito no mundo geral o é na Internet e vice-versa». Abaixo com ele. OOOps!

2 · INTRODUÇÃO

O crime de acesso ilegítimo é um emblema.

É um emblema porque traduz uma censura penal e todas as reacções com tal peso são de uma imensa sedução. Dizer que é crime «is always something».

É, por outro lado, o mais emblemático crime informático.

Não no nome [4]. Não é o nome que lhe dá o pedigree. O nome não o distingue de nada em especial. Nem de qualquer outro crime. Podia ser a designação de qualquer outro vulgar tipo de ilícito existente no Código Penal. Não tem o punch do «crime de sabotagem informática», nem a pompa confusa do «crime de dano relativo a dados ou programas informáticos».

Mas é uma referência simbólica porque, para além de se tratar de um crime da dimensão técnica da criminalidade informática, aquela dimensão tem por si só um significado próprio, seja em relação ao sistema jurídico-penal, seja à conjuntura dos crimes informáticos, é com ele que toda a criminalidade informática começa.

E o seu conteúdo expressa sempre, como em nenhum outro crime deste universo, uma opção de política criminal.

Uma opção de política criminal, pois que a mesma traduz sempre um juízo sobre o mais carismático comportamento no mundo da informática: conforme a redacção do crime de acesso ilegítimo, este crime pune ou não o «hacking» (ou mero intrusismo informático). E o hacking tem um glamour único. Não é vulgar como um vírus informático (em especial quando estes se chamam «I love you»). Não é massificado e bruto como o volume de ordens do Denial of Service (DoS). É interiorista. É confessional. É expressão de saber e de arte. É demonstrar ao acedido o seu desleixo, a sua insuficiência ou, pior, a sua incompetência. Diga-se numa frase: o hacking tem um âmbito próprio e, no contexto do afirmado nas «Considerações prévias», pelas suas especificidades, é, por si só, um critério a considerar para a existência de um Direito das Tecnologias da Informação e da Comunicação.

3 · A CRIMINALIDADE LEVITACIONAL

O crime de acesso ilegítimo é um crime levitacional [5] ou crime informático (a criminalidade levitacional ou informática encontra-se tratada dispersamente, mas tem o seu núcleo essencial na Lei n.º 109/91, de 17 de Agosto).

Mais do que isso.

É, por um lado, um daqueles crimes que trata a dimensão verdadeiramente caracterizadora dos crimes informáticos – a criminalidade informática técnica e que é constituída pelos art.s 5.º a 8.º da Lei n.º 109/91, de 17 de Agosto. É preciso referir

4 O legislador utilizou a designação do tipo de ilícito proposto pela Recomendação (89) n.º 9, de 13 de Setembro de 1989, do Conselho da Europa, sobre a criminalidade relacionada com o computador. O que, tendo em conta que o diploma português seguiu as guidelines constantes daquele texto, admita-se, incontornáveis, foi solução coerente.

5 A criminalidade informática é levitacional por oposição à criminalidade tradicional, com recondução directa a uma determinada acção e à orbita geográfica da sua comissão (e que se pode designar de criminalidade hidráulica). Quase toda a criminalidade informática é levitacional, mas os crimes informáticos técnicos são-no sempre, sendo mesmo expressão máxima desta órbita.

que a criminalidade levitacional ou informática não é toda constituída por tipos de ilícito radicalmente diferentes dos outros crimes. Há uma parte desta criminalidade que tem vertentes absolutamente incaracterísticas – por exemplo, a burla informática ou o crime de falsidade filiam-se nos argumentos de política criminal dos tipos que lhe são familiares e que se encontram inscritos no Código Penal.

Por outro lado, é expressão simbólica da criminalidade que é, essencialmente, praticada através da infra-estrutura técnica corporizada na Internet. Neste sentido, um cybercrime.

Vamos por partes

Comecemos pelo quadro onde este tipo de ilícito se inscreve.

O crime de acesso ilegítimo é um crime informático técnico que tem verdadeira expressão quando praticado através de uma infra-estrutura técnica. Neste sentido, é um crime volátil, praticado à distância.

A possibilidade de os crimes poderem ser praticados à distância é uma característica incomum à generalidade dos tipos de ilícito. Alguns tipos clássicos já o permitem [6]. Mas aquela referência é uma idiossincrasia de alguns dos crimes informáticos.

Nos dias de hoje, são também tipicamente praticados à distância os crimes de sabotagem informática, o crime de dano relativo a dados ou programas informáticos e o crime de intercepção ilegítima: ou seja, crimes com uma dimensão técnica e uma componente de execução etérea. Todos estes tipos de ilícito são crimes levitacionais. Uma espécie de crimes informáticos. Chamo-lhes «crimes informáticos técnicos», que se podem definir como «as condutas criminalmente desvaliosas, simultaneamente praticadas com a utilização técnica de estruturas e sistemas informáticos e em que estes bens constituem o objecto da acção, lesando o bem jurídico segurança dos sistemas informáticos» [7].

São crimes praticados sem uma especial ligação física e sem âncoras. São também crimes que mais não fazem do que acompanhar o sentido evolutivo do sistema económico-social. Do mesmo modo que a caracterização da nova criação e da produção de riqueza deixou, há muito, a dimensão de produção hidráulica, fisicamente ligada a espaços localizados e a estruturas sólidas, a criminalidade acompanhou este sentido evolutivo. A possibilidade de expansão a nível global, apoiada na Internet, levou «a uma desvalorização dos territórios e das redes fixas que organizam as transacções nos territórios, transferindo-a totalmente para o espaço, para a levitação» [8].

A criminalidade encravada no espaço ou que atinge as pessoas pode abrir telejornais, mas já não interessa. É o passado. O passado é a criminalidade hidráulica. A expressão criminal de um certo futuro é a criminalidade informática técnica, que deve ser referida como a criminalidade levitacional técnica. Toda a criminalidade informática é levitacional, mas os crimes informáticos técnicos são expressão máxima desta órbita. Chamemos-lhe, pois, o vértice máximo da criminalidade levitacional.

Viver é um risco. Mas já era um risco há quinhentos anos.

Há quem diga que hoje o risco é maior, que a vivência num sistema social e económico determinado pela influência das novas tecnologias, que possibilita um novo acesso à informação e impõe novos ciclos de comunicação, potencia a produção do risco, que somos dominados por um sistema económico-social-cultural com riscos novos. Esta adição de riscos à vida, reconheço, incomoda-me, mas não me perturba. Vivemos numa comunidade em que a vivência é múltipla e que a soma dos novos riscos, porventura, não se traduz em mais riscos para cada um de nós. Existem é novos riscos, ou outros riscos.

Não é intenção deste texto a contextualização da chamada Risikogesellschaft enunciada por Ulrich Beck (até porque se trata de um dos tópicos de tratamento mais tocado, nos dias de hoje, em especial na dogmática penal [9]), nem tão pouco elaborar

6 A noção de crimes velhos, por meios novos.

7 É uma noção que convinha esconder até ao limite, pois que a mesma já dá alguns dos contornos essenciais do presente artigo.

8 José Félix Ribeiro: *Internacionalização das economias e as forças motrizes da globalização. Tecnologias emergentes e economias emergentes*, «Internacionalização uma opção estratégica para a economia e as empresas portuguesas», Lisboa, 1999.

9 Para a abordagem de tal matéria, sugerimos, por exemplo, Jesús-Maria Silva Sanchez: *La expansión del Derecho Penal. Aspectos de la política criminal en las sociedades postindustria-*

especificamente longas considerações de carácter criminológico. Mas fiquemos com esta ideia: aparte os grandes problemas ambientais, aqueles que são tratados nas grandes cimeiras internacionais, e que são uma guerra perdida, o verdadeiro novo risco, que é transversal a todas [10] as sociedades, é o que decorre do uso das tecnologias informáticas.

Este risco não é um risco novo apenas no sentido quantitativo. É também um novo risco, no sentido de configurar verdadeiramente um novo género de perturbação para todos nós.

Uma tal circunstância teria necessariamente expressão no domínio criminal. Tripla expressão, aliás: no tipo de problemas que coloca a quem sofre a acção; em novos tipos de acção; nos meios de acção utilizados.

Refira-se, como nota prévia, que não há praticamente relevo substantivo ou criminológico na utilização de meios informáticos [11] na comissão de crimes tradicionais (situação esta que tem reflexos no terceiro critério referido anteriormente, os «meios de acção»), sobretudo porque esta linha de delitos não leva a nenhum resultado prático na tentativa de fundamentar a existência de um novo Direito: em traços gerais, o âmbito de protecção de um tal tipo de crimes justapõe-se ao do protegido pelo Direito Penal Clássico.

Dos outros dois critérios (problemas colocados e tipos de acção) é que importa tratar porque nos irão levar a considerar a existência de novos campos que devem ser objecto de protecção e, no limite, aceitar a comissão de novos crimes, por novos meios.

4 · O CRIME DE ACESSO ILEGÍTIMO

O reconhecimento da «existência de novos problemas que devem ser objecto de tratamento» e a verificação de «novos crimes, por novos meios» é algo que está inelutavelmente ligado entre si. É difícil a destrinça completa entre quando se evidencia uma situação e começa a outra. Mas tentemos começar por esta última dimensão.

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

Ou seja, trata-se de um crime praticado por alguém com os conhecimentos técnicos suficientes para imiscuir-se numa plataforma informática – um objecto da acção novo –, sem que o respectivo titular o tenha autorizado, ou para além do consentimento expresso produzido pelo titular do sistema ou rede informáticos. Se a isto juntarmos dever ser sustentável, em abstracto e como «traço caracterizador do ilícito», a limitação da punibilidade às situações em que haja violação de mecanismos de segurança lógicos (ou intrínsecos ao sistema informático) [12], creio podermos chegar ao conceito de penetração entendido como um acto lesivo estranho aos mecanismos clássicos da comissão de delitos.

Ora, considero que este é o universo que constitui a parte essencial do património do crime de acesso ilegítimo. Em consequência, tal deverá levar a afirmar-se estarmos na presença de um crime com uma dimensão diferenciada e praticado com o recurso a meios não tradicionais. Ou seja, trata-se de um crime cujo móbil da acção, o objecto sobre o qual a acção incide e os meios utilizados para a sua comissão são realmente novos. Independentemente da forma como o tipo de ilícito se encontra construído, na sua essência, não se trata de uma inovação conjuntural. Aquelas três dimensões de diferenciação traduzem um novo estado estrutural, que inclusivamente motiva que a acção deve ser objecto de censura [13].

Permita-se-me um pequeno espaço para referir, numa breve síntese, que, do meu ponto de vista, o

les, Madrid, S.L., 1999, ou Mirentxu Corcoy Bidasolo: *Delitos de peligro y protección de bienes jurídico-penales supraindividuales*, Valencia, 1999.

10 Todas não, haverá algumas que, pelo seu manifesto atraso, lhe resistam.

11 A prática de velhos crimes, por novos meios, só incidentalmente leva à real motivação de novos ângulos de protecção, que não seja fundada na necessidade de suprir expectativas dos diversos sistemas.

12 O que será dizer, *de lege ferenda*, incluir, como elemento objectivo do tipo de ilícito geral (e não remetido para uma qualificativa do tipo), a violação de regras de segurança lógicas ou intrínsecas ao sistema informático. Defendemos esta posição precisamente por força do conceito abstracto do acesso ilegítimo, ainda que a mesma limite as margens de punibilidade do tipo.

13 A variação mais relevante assentará na (in)existência de elementos subjectivos específicos, o que conduzirá, como referimos à opção de polica criminal sobre a (des)necessidade da punição do hacking em termos literais (ou mero intrusismo informático).

elemento literal da norma legal portuguesa – o crime de acesso ilegítimo encontra-se tipificado no ordenamento jurídico português no art. 7.º da Lei n.º 109/91, de 17 de Agosto (que o legislador cuidou até de designar como «Lei da Criminalidade Informática) [14] – não incorpora todas as dimensões que devem constituir e que cristalizam o conceito de um tal tipo de ilícito. A norma legal portuguesa que resulta daquele artigo não é tão rica quanto a verdadeira dimensão de tal tipo de acção: por um lado, porque a terminologia adoptada no elemento objectivo do tipo de ilícito português, no seguimento da formulação da Recomendação (89) n.º 9, de 13 de Setembro de 1989, do Conselho da Europa, apenas refere a modalidade «aceder», não inclui a manutenção no sistema; apenas dispõe sobre a falta de autorização, o teor literal dos elementos objectivos não contém uma referência expressa à possibilidade a censura poder resultar do extravasar do consentimento prestado pelo titular; por fim, a violação de regras de segurança apenas é remetida para a qualificação.

Há quem contrarie a estrutura conceitual deste tipo de acção nos termos do referida no inicio desta sección 4, ou quem, não a contrariando, pelo menos rejeite que se esteja perante um novo móbil da acção. Estão neste caso aqueles que consideram que o sistema informático deve ser conceitualmente reconhecido como uma espécie de, ou, mesmo, como um «domicílio informático» [15] – aliás, como também é aflorado no documento do Conselho da Europa. Há até quem sustente que este sistema informático é um lugar onde se encontram alojados dados de alguém [16] e que a lógica de relação entre os dados informáticos e o sistema informático é a mesma da relação entre o domicílio físico e a pessoa em si [17], ou quem sustente tal tese invocando que o sistema informático pode representar algo de ainda mais pessoal e íntimo do que o próprio domicílio físico [18].

A consequência lógica que se deve tirar é que, para estes autores, afinal de contas, este crime mais não é que o crime de violação de domicílio ou, pelo menos, não traz nada de novo ou não foge da lógica da sua fundamentação [19 e 20]. Quem associa aquelas duas dimensões (domicílio físico/domicílio informático), fica necessariamente agrilhoado a uma lógica redutora de intelecção das condutas de acesso ilegítimo. Este facto tem consequências, pelo menos na identificação do âmbito de protecção do tipo (e que é, como se verá o critério primeiro para a elevação da censura de tais acções ao plano da repressão criminal).

Em termos conceituais, não creio que um sistema informático se deva reduzir a uma espécie de domicílio informático e muito menos considero que a prática de actos de acesso ilegítimo deva ser considerada como incidindo num «domicílio informático». Quer dizer, salvo se aceitarmos que se chame domicílio a um local onde os programas informáticos e os dados se encontrem fisicamente localizados – ideia, convenhamos, demasiado básica e rude –, aquela noção não evidencia a verdadeira dimensão que um sistema informático tem.

Em primeiro lugar, um domicílio é um local. Em seguida, é um local fisicamente ancorado. A noção de sistema informático está para além do conceito de uma limitação física. Em boa verdade, o conceito de sistema informático é demasiado elástico para poder ser atapetado entre estruturas físicas. É, ou pode ser, composto por demasiados componentes, o que não permite cristalizar uma dimensão física do mesmo.

14 Este diploma legal condensou a estrutura essencial da Recomendação (89) n.º 9, de 13 de Setembro de 1989, do Conselho da Europa, sobre a criminalidade relacionada com o computador.

15 Alma-Perroni: Riflessioni sull'attuazione delle norme alla tutela della riservatezza e del segreto», *Rivista Trimestrale di Diritto Penale Economico*, 1997, n.º 4. Em Portugal, esta posição foi também a adoptada por Manuel António Lopes Rocha: *A Lei da criminalidade informática (Lei n.º 109/91 de 17 de Agosto). Génese e técnica legislativa*, Legislação, *Cadernos de Ciência e Legislação*, «Informática Jurídica e Direito da Informática», INA, n.º 8, Out.-Dez., 1993 e por Manuel Lopes Rocha (Manuel Lopes Rocha e outros: *Direito da Informática. Legislação e deontologia. Estudo introdutório de Manuel Lopes Rocha*, Lisboa, 1994). Garcia Marques e Lourenço Martins também adoptam a posição da existência de um domicílio informático. Aparentemente, vão até mais longe (por exemplo, em relação àqueles outros autores portugueses), consideram, na linha do constante da Recomendação (89) n.º 9, de 13 de Setembro de 1989, do Conselho da Europa, que, «em primeira linha», se trata de uma protecção do «designado domicílio informático, algo de semelhante à introdução em casa alheia» (*Direito da Informática*, Coimbra, 2000). Já veremos como se deve contrariar esta argumentação.

16 Galdieri: «La tutela penal del domicilio informatico», *Problemi giuridici dell'informatica nel MEC*, Milão, 1996.

17 Idem.

18 Por exemplo, Giorgio Pica: *Diritto Pennale Delle Tecnologie Informatice – Computer's crimes e reati telematiche, Internet, Banche-dati e privacy*, série *Diritto Attuale*, Milão, 1999.

19 Previsto e punido no art. 190.º do Código Penal.

20 Exactamente o professado por Garcia Marques e Lourenço Martins.

Mas reconheço completa razão quando se relaciona o sistema informático com a pessoa humana: o sistema informático pode ajudorra pessoa. Num conjunto significativo de situações, pode até expressar algumas das vertentes da dimensão humana. O que não reconheço é que o sistema informático seja necessariamente, como o faz, por exemplo, Giorgio Pica, uma extensão da pessoa humana e, de novo, muito menos, que isso deva reconduzi-lo à ideia de um domicílio. O domicílio tem uma função social única: o da habitação na sociedade moderna e o «significado social» da sua violação determina a protecção de um bem jurídico específico. Não estou a ser, de todo, inovador. Esta é precisamente a posição há muito sustentada por Costa Andrade [21]. Os sistemas informáticos não têm aquele significado e a posição que admite a existência de um domicílio informático vê a sua fragilidade completamente exposta quando os titulares dos sistemas informáticos sejam pessoas colectivas, aos quais manifestamente aquele conceito não se ajusta.

Quanto à reprodução de tal imagem (de domicílio informático), à luz da norma legal, ainda é mais periclitante a sustentabilidade de tal posição. Basta atentar no elemento literal do tipo previsto no art. 7.º da Lei da Criminalidade Informática: o crime de acesso ilegítimo também é praticado quando as acções incidam sobre redes informáticas. Ou seja, quando alguém aceda a uma rede informática. Seja por força da definição constante da al. a) do art. 2.º da Lei da Criminalidade Informática, seja porque o expoente máximo desta rede pode ser a Internet. Como é que ela pode funcionar como um domicílio? É demasiado etérea para tal.

A noção de domicílio informático é uma muleta, mas, como quase todas, não é suficientemente rigorosa, nem cristaliza o conjunto de valores que devem ser objecto de protecção.

Repetindo o anteriormente afirmado, o acesso ilegítimo cria um novo tipo comissivo, inovador em três dimensões essenciais num tipo de ilícito. Se juntarmos a isto a conclusão de que esta estrutura de inovação é acompanhada pela cristalização de um novo objecto de protecção, fechamos o círculo quanto a termos achado uma nova criação (mas isto já será adiantarmo-nos ao resultado que a metodologia de fundamentação do presente texto irá proporcionar).

Quase consensualmente, a doutrina portuguesa continua a considerar que o Direito Penal deve ser construído segundo um paradigma funcional teleológico e de política criminal, um conceito material de crime, em que a função do bem jurídico tem relevo primordial. Mesmo as novas posições, mais próximas das chamadas teoria da acção e da teoria da sociedade, consideram que o Direito Penal deve ter uma intervenção protectora de um conjunto de valores que foram cristalizados como de tal forma importantes que a sua compressão deve ser objecto de reacção criminal.

É, pois, a evitação da lesão das tais cargas axiológicas que legitima a intervenção penal, mas esta reacção não deve ser desproporcionada ao efeito que visa atingir.

5 · O BEM JURÍDICO-PENAL «SEGURANÇA DOS SISTEMAS INFORMÁTICOS»

Não é nossa missão a delimitação dogmática do conceito de bem jurídico-penal. Tomemos, então como definição-base que o bem jurídico é a «expressão de um interesse, da pessoa ou da comunidade, na manutenção ou integridade de certo estado, objecto ou bem em si mesmo socialmente relevante e, por isso, juridicamente reconhecido como valioso» [22]. Não resistimos a compor esta definição com uma dimensão que creio dever ser acentuada. Aquela dimensão de conteúdo (a dimensão axiológica ou o interesse) tem expressão quando o processo relacional da pessoa com o objecto de valoração se veja afectado por actos não controlados por aquela. Indo um pouco mais além, porque nos é benéfico para a fundamentação da nossa posição, a sustentação de que um determinado bem jurídico ascenda à categoria de um bem jurídico-penal também deve ser determinada pelo mecanismo relacional da própria comunidade com o objecto de valoração.

Ou seja, a compreensão de que um determinado valor deve ser objecto de uma fortíssima protecção não pode decorrer do seu valor intrínseco, mas sempre da sua projecção para o sistema social. Esta projecção é efectuada em dois planos: o plano do

21 Expressa, por exemplo, em *Consentimento e acordo em Direito Penal*, Coimbra, 1991.

22 Cfr. Figueiredo Dias e Costa Andrade: *Direito Penal – Questões fundamentais. A doutrina geral do crime*, Coimbra, 1996.

eu individual e o plano da composição massificada das diversas individualidades. Quer isto dizer que a lógica da fundamentação de um bem jurídico-penal se perspectiva como «mecanismo de validação e de preservação das componentes axiológicas societárias e individuais».

O bem jurídico é, pois, a consideração de um fenómeno relacional do eu e da comunidade (que é a composição de um sem número de eus) com o objecto de valoração. Retenhamos esta premissa, em especial, aqueles dois pólos relacionais, pois é ela que torna mais clara a justificação da existência de bens jurídicos intermédios (e já veremos como será determinante no presente estudo) e que valida o modo com se deve compreender o objecto de protecção inscrito no crime de acesso ilegítimo.

O bem jurídico é, assim, um marco essencial na fundamentação penal: é «a tutela de bens jurídicos que simultaneamente define a função do Direito Penal e marca os limites da legitimidade da sua intervenção». O bem jurídico é, pois, um critério incontornável, o elemento a partir do qual a construção do tipo deve ser erigido.

Se conseguirmos compreender que aqueles tipos levitacionais, de cariz técnico (a tal referida criminalidade informática técnica, dos art.s 6.º a 8.º da Lei da Criminalidade Informática), evidenciam um novo fenómeno de protecção, poderemos ostentar a bandeira de, até no seu plano mais essencial – a existência de um novo bem jurídico-penal –, sermos tocados por um universo novo e próprio, que decorre das esferas tecnológicas e das telecomunicações: um daqueles apports decisivos para o embrião de um Direito Penal da Informática e, por via disso, um contributo para um Direito das Tecnologias da Informação e da Comunicação.

O bem jurídico típico da criminalidade levitacional técnica é expressão de um mundo próprio. Contudo, já sustentei noutras ocasiões que este valor se inscreve numa família mais ampla de bens jurídico-penais, que se reconduzem a um macro-bem jurídico que reina sobre toda a criminalidade levitacional (em sentido amplo).

A criminalidade levitacional constitui um tipo de criminalidade polifacetada, que tem na criminalidade informática técnica a sua expressão de glória, o seu símbolo (não tenho, apesar de tudo, por adquirido que esta ordem criminal técnica seja a mais violenta criminalidade informática, a quantitativamente mais expressiva, ou a mais perturbante para o sistema económico-social).

O problema dos símbolos é que, por vezes, podem tornar menos óbvios os contextos mais amplos. No caso, podem levar a que se considere que é uma criminalidade tão específica que não deve ser tocada por outros domínios da criminalidade levitacional. Não o creio. Todos os objectos de protecção, no universo da criminalidade especificamente informática ou levitacional (e não meramente praticada por meios informáticos), devem ser reconduzidos a um super-bem jurídico conceitual que se pode apelidar de «bem informático».

Este super conceito mais não é do que um referencial axiológico «umbrella» que está no topo da pirâmide. Um protectorado vertical que abarca a pluralidade dos bens jurídicos protegidos pelos tipos de crimes relacionados com os computadores. É um conceito que deve ser tido como suficientemente amplo e elástico que lhe permita isso mesmo. É, pois, um conceito aberto e continuamente em construção, mas que deve rejeitar os significados e os valores que não se inscrevam na sua família. Pela sua falta de concretude, porque é uma estrela que vela pelos valores concretos de protecção, não haja qualquer dúvida: o bem informático não é o bem jurídico que se reconhece do elemento objectivo de ilícito, o que será afirmar, do comportamento fixado na norma legal como proibido [23 e 24]. Não é o bem jurídico protegido pela norma legal. É uma referência de princípio que o bem jurídico-penal concreto não se importa de reconhecer.

A existência de um bem informático pode constituir ajuda para o intérprete naquelas situações sombrias em que não é claro se a dimensão técnica da acção deve ser reconduzida ao universo da cyberlaw penal. Não se trata só de um mero referencial heurístico. É um referencial dogmático, com valor prático [25].

---

23 Figueiredo Dias/Costa Andrade: «O crime de fraude fiscal no novo direito penal tributário português (considerações sobre a factualidade típica e o concurso de infracções)», *Revista Portuguesa de Ciência Criminal*, ano 6, Fasc. 1.º, Jan.-Mar., 1996.

24 Exactamente como se encontra aqui expresso, porque tratando-se esta criminalidade, por ora, de uma criminalidade extra Direito Penal de Justiça, o objecto de protecção é artificial, resulta da redacção do tipo. Não é, pois, um dado ontológico, como em regra, são os bens jurídicos protegidos na codificação penal.

25 Apesar da sua diversidade, as diversas dimensões do bem jurídico compõem-se num só bem jurídico-penal, suficiente denso e equilibrado para ser considerado uno. Neste sentido, compreendo que cada tipo criminal da criminalidade levitacional técnica e, em especial, o crime de acesso ilegítimo, cristaliza apenas um e só um bem jurídico. A polaridade do bem jurídico que temos tratado não deixa de corporizar uma «noção unitária» de bem jurídico-penal.

A agregação de um conjunto de valores sob o mesmo tecto tem um efeito dominó: leva à consideração de novos valores. Contudo, obriga-nos a um critério de exigência: esta conceitualização só faz sentido se formos sensíveis à existência de um conjunto de valores novos que a massificação das plataformas informáticas gera e, cumulativamente, se considerarmos que estes valores devem ser objecto de protecção penal. Em consequência, admitirmos que o objecto de protecção que resulta de alguns tipos de ilícito é verdadeiramente novo e, por isso, estamos perante tipos autonomizados do estilo de crimes que havia previamente.

O quadro é o seguinte:

Do meu ponto de vista, a generalização da informática no sistema económico-social criou um novo mecanismo relacional do indivíduo e da própria sociedade. Há novas preocupações, que são cada vez preocupações mais graves (saber se é através do Direito Penal que o «eu» e a «sociedade» devem ficar tranquilos é uma outra discussão – admitamos que sim). O novo modo relacional apresenta, então, novos fenómenos patológicos que considero não serem meras «aparições de carácter patológico» (Krankheitserscheinungen) [26]. Não são episódicas, nem fugazes. Vieram e permanecem.

Depois, considero que, em especial na criminalidade levitacional técnica, estes fenómenos podem e devem ser considerados como novos objectos de protecção. E, mesmo, considero que os mesmos já se encontram identificados no recorte de algumas normas penais.

Se considerar, como alguns autores o fazem [27], que a comissão de actos perfumados pela informática não deva levar, designadamente naquele tipo de criminalidade técnica, à protecção de algo de novo, ou melhor, que os bens jurídicos já existentes no universo dos últimos 30 a 100 anos permitem compreender os anseios, as preocupações, a necessidade de protecção criada pelo novo universo informático, então, terei que concluir que não há nada de novo a equacionar. Todos os problemas devem ser tratados no universo dos bens jurídicos clássicos. Pode até considerar-se que não é analogia proibida a aplicação dos tipos de ilícitos existentes no Código Penal a estas situações. Se nada de novo há, não se justifica a autonomização de um direito (designadamente no âmbito penal).

Estas posições são mais seguras, mais prudentes. Com certeza. Mas considero que são insuficientes para compreender a complexidade dos novos problemas, logo não constituem a melhor interpretação. Ou, reportando o sentido desta afirmação para a metodologia da fundamentação penal, uma tal posição é demasiado pobre para poder compreender os novos fenómenos relacionais dos sistemas sociais que a informática cria.

Chegámos ao centro do nosso problema: qual o âmbito de protecção do crime de acesso ilegítimo previsto no art. 7.º da Lei da Criminalidade Informática? Uma pergunta mais ampla como «qual o sentido de política criminal para a tipificação do crime de acesso ilegítimo?» importaria um estudo mais amplo, que imporia a análise de temas como a necessidade da fixação de um crime de barreira, a justificação de uma protecção avançada, o perigo informático, o problema da construção do tipo ao nível subjectivo e a punição das condutas de hacking, etc. É uma outra dimensão que nos foge, por ora, por falta de espaço.

Centremo-nos, pois, na questão formulada.

Nos termos da nossa lei, pratica o crime de acesso ilegítimo quem, não estando para tanto autorizado e com a intenção de alcançar, para si ou para outrem, um benefício ou vantagem ilegítimos, de qualquer modo aceder a um sistema ou rede informáticos.

Aceder a um sistema ou rede informáticos é a componente do elemento objectivo que constituiu o núcleo essencial do tipo.

Partemos desta dimensão e, metodologicamente, testemos e reforcemos as conclusões obtidas com os demais elementos do tipo que devem ser objecto de interpretação.

No caso de tipos de Direito Penal Secundário, em geral, é da exteriorização do tipo que se clarifica o bem jurídico protegido, pelo que a questão seguinte que se deverá colocar é a seguinte: o que é que fica perturbado no mecanismo relacional do eu/sociedade com a plataforma informática (porque o objecto sobre o qual a acção incide é precisamente «produtos informáticos») quando alguém lhe acede, sem consentimento?

Esta é dimensão teórica da questão (e a que deve ser, no início, formalmente colocada).

---

26 Manuel Lopes Rocha: «A Lei da criminalidade informática», cit.

27 Por exemplo, Faria Costa, Giorgio Pica, etc..

A forma como o problema deve ser colocado na prática é uma outra [28]. O problema deve, então, ser visto do seguinte modo:

O que é que mais me perturba quando alguém acede, sem o meu consentimento ou excedendo o meu consentimento, ao meu computador?

Mas esta questão é insuficiente (estamos a adiantarnos e a fornecer desde já algumas pistas). Tendo em conta o «tipo» de bem jurídico em causa, é também necessária a formulação da seguinte questão:

O que é que mais perturba a sociedade quando alguém acede, sem o respectivo consentimento ou excedendo-o, a um determinado computador?

Há três respostas possíveis.

Considerar-se que tais actos podem levar a danos nos sistemas e redes informáticos. Nesse sentido, é uma dimensão essencialmente patrimonial que está em causa, como efeito directo da acção ilícita. Como caricatura, diria ser, em regra, o caso daquelas pessoas cujos sistemas informáticos foram comprados como objecto de decoração.

Entender-se, no oposto (é verdadeiramente o oposto), que a preocupação maior é o conteúdo dos sistemas informáticos enquanto expressão da própria pessoa: seja em termos de tipos de programas compilados, seja todo o historial da pessoa que ali pode estar registado. É, porventura, a preocupação dos mais conhecedores e dependentes da informática.

Se entendermos que outra coisa não deve ser protegida para além daquelas duas respostas, então, nada de novo existe no universo do crime de acesso ilegítimo, pois que o âmbito de protecção não se diferencia do estilo de bens jurídicos previstos na órbita dos crimes contra o património ou na órbita dos crimes contra a reserva da vida privada. E, neste sentido, nada os separa.

Há uma terceira resposta possível. A resposta a adoptar: o crime de acesso ilegítimo é a resposta às acções que, tendo outras dimensões de protecção (e já veremos como se expressa esta multiplicidade), podem determinar a minha e a nossa perda de confiança no sistema informático e nas redes informáticas e degradar a minha relação com o novo estilo de vida que se verifica, por força da pressão que é imposta pela informática. Este deve ser considerado o traço essencial da protecção da norma legal. Um nome para este âmbito de protecção: «segurança dos sistemas informáticos» (também não foge deste domínio a designação de «intangibilidade dos sistemas informáticos»).

Mas dir-se-á, «segurança dos sistemas informáticos» é o bem jurídico que alguma doutrina portuguesa enuncia há cerca de quinqe anos. O nome sim. O verdadeiro significado do bem jurídico em causa não.

Na verdade, desde o início da década passada que, primeiro, Manuel António Lopes Rocha [29] e, depois, Manuel Lopes Rocha e António Bernardo Colaço identificam expressamente no tipo de acesso ilegítimo o bem jurídico «segurança do sistema informático». Com o reconhecimento intelectual que lhes tenho e que sabem ser muito, acho que aquela identificação é um acaso. Por um lado, a designação daquele bem jurídico é a que foi expressamente referenciada na Recomendação do Conselho da Europa para o tipo em causa. Aquele texto não deu qualquer outra directriz. Aqueles autores pegaram naquela noção, adoptaram-na. Mas deram-lhe, ambos, o seguinte cunho: preservar o sistema informático como quem preserva a inviolabilidade do domicílio informático.

6 · AS DIMENSÕES DO BEM JURÍDICO «SEGURANÇA DOS SISTEMAS INFORMÁTICOS»

Como referi, o bem jurídico «segurança dos sistemas informáticos», conforme deve ser desenhado, tem outra dimensão. É outra coisa.

É preciso referi-lo sem subterfúgios: aquele bem jurídico é um bem jurídico complexo. Tem um corpo idiossincrático que lhe dá a tonalidade própria, mas abrange outras dimensões. Nesse sentido, é algo difuso. Aliás, sendo um bem jurídico que devemos considerar inscrito noutras normas penais informáticas (e aqui a cisão com a demais doutrina portuguesa é completa, pois que nenhum

28 Não divaguemos sobre os novos mecanismos de dependência de todo o sistema social, cultural e económico que a informática criou. É dogma incontestado (assim, uma primeira questão como «há algum valor que possa ser comprimido por tais tipos de acesso?» deve ser liminarmente respondida num sentido afirmativo).

29 «O crime informático na legislação portuguesa», *Revista do Ministério Público*, ano 15.º, n.º 57, Jan.-Mar., 1994.

outro autor o reconhece, por exemplo, no crime de sabotagem informática ou no crime de intercepção ilegítima), os diversos elementos que o compõem não têm, nas diversas normas, o mesmo peso. Pode até considerar-se que, nalgumas delas, o peso da sua essência não é sequer o elemento mais forte [30].

Por outro lado, a noção que adoptamos deste bem jurídico mais não faz do que abarcar o carrossel caleidoscópio de incidências que resulta da acção de acesso ilegítimo. Na verdade, o tipo de lesão provocada por estas condutas é estilhaçada. Tem múltiplos contornos. Pode danificar bens. Pode levar à perda de criações. Pode levar à perscrutação de conteúdos. Pode levar à cessação de utilização do equipamento informático.

Isto é uma evidência. Não devemos, pois, ser obedientemente defensivos, agrilhoados ao medo de se considerar que este bem jurídico tem diversas dimensões.

Primeira dimensão: a dimensão essencial ou caracterizadora

A informática está em todo o lado. No nosso dia-a-dia. Tornou-se de uso corriqueiro. Esta desnatização do uso da informática leva a que, no nosso espírito, se afaste, como ideal, toda a contingência de eventuais problemas de utilização de tais plataformas, por força de actos não consentidos. Nem nos passa pela cabeça que se deixe de utilizar os equipamentos. Só que, no inverso, precisamente o peso interrelacional de tais plataformas leva a que as mesmas fiquem mais expostas. Se tornem mais vulneráveis.

Isto é, o plus das múltiplas funcionalidades dos sistemas informáticos torna-os mais apelativos a actos disruptivos praticados por delinquentes. No pólo contrário, aquilo que se pretende é assegurar que os sistemas informáticos funcionem sem anomalias estranhas ao seu próprio funcionamento e, nesse sentido, é necessário salvaguardar a «confiança no funcionamento de determinado sistema». Sem isso, as consequências podem ser devastadoras.

O maior perigo que pode advir dos actos que incidam sobre plataformas informáticas é que uma pessoa e, por contágio a sociedade em geral, ou no caso de acções que incidam sobre redes informáticas, directamente o próprio sistema social, se desacreditem da utilização do sistema. A quebra de confiança na utilização destes sistemas traduz-se na generalização de um medo ou de uma sensação de insegurança na utilização de tais equipamentos, de que, afinal de contas, essa utilização traduza um desperdício de tempo e de recursos.

Em suma, o carácter essencial deste bem jurídico visa determinar a protecção da confiança de todos nas funcionalidades da informática, tentando assegurar que estes (já basta o risco da existência de bugs que lhe é intrínseco) se encontrem disponíveis na sua plenitude, o que será dizer, esteja salvaguardada a integridade dos mesmos [31]. Ou seja, o foco mais essencial deste bem jurídico é a «evitação das operacionalidades», das funcionalidades dos sistemas, que se quer permaneçam intactas, fiáveis e fiéis aos seus utilizadores. Directamente associado a este domínio, até por força da causa de justificação «falta de autorização» que se encontra inscrita no tipo de ilícito, somos conduzidos à preservação da «circularidade fechada da comunicação» [32], um domínio em que o usus excludendi deve ser salvaguardado.

Mas há outras duas dimensões que, em abstracto, constam do bem jurídico «segurança dos sistemas informáticos».

Segunda dimensão: a dimensão quantitativa da perda

É horizontal a toda a criminalidade levitacional a aceitação e o reconhecimento de que as situações de break-in podem importar consequências ao nível dos bens informáticos sobre as quais incidem. Aquelas situações podem levar à ruptura de

30 Mas essa matéria fica para outra altura.

31 Na dogmática internacional, esta dimensão é já professada por um conjunto significativo de autores, que, de alguma forma, mas não tão densamente e ficando-se apenas por esta dimensão primeira do bem jurídico, já enunciaram este bem jurídico. Cfr. entre outros, Sarzana: «Gli abusi nel setore informatico. Spunti per una ricerca criminologica e vitimologica», *Diritto dell'Informazone e dell' Informatica*, 1989, A. Rossi Vanini: «La Criminalità Informatica: le tipologie di computer crimes di cui alla L. 547/93, Dirette alla tutella della riservatezza e del segreto», *Rivista Trimestrale di Diritto Penale Dell'Economia*, ano 7, n.º 3, Jul-Set, 1994, Esther Morón Lerma: *Internet y Derecho Penal: Hacking y otras condutas ilícitas en la red*, Pamplona, SA, 1999, e Mariluz Gutiérrez Francês, em, por exemplo: «El intrusismo (Hacking): Represión Penal Autónoma?», *Informática y Derecho*, n.ºs 12-15, Mérida, 1995.

32 Adoptamos a terminologia de Faria Costa, «comunicação fechada» («As telecomunicações e a privacidade: o olhar (in)discreto de um penalista», *As telecomunicações e o direito na Sociedade da Informação,* Coimbra, 1999).

programas informáticos, à danificação de estruturas do equipamento informático, à destruição de documentos e conteúdos ancorados na plataforma informática, ou, ainda, à perda ou suspensão das funcionalidades dos mesmos (veja-se, como caso emblemático, as situações de DoS). Estas quatro vertentes têm algo em comum: a produção de danos para quem sofre tais acções.

Do gráfico do desvalor, em geral tido na aferição dos crimes, dir-se-á que esta é a dimensão que mais acentua o desvalor do resultado. E um particular resultado, que tem que ver com o plano da patrimonialidade. Só que, ao contrário do que consideram diversos autores, estes tipos não se circunscrevem a este universo, estão muito para além dele e esta confissão não é um sinal de fraqueza da posição adoptada, é apenas a confirmação da elasticidade deste bem jurídico o único que permite compreender a multiplicidade do fenómeno relacional do sistema social com a informática.

Terceira dimensão: A tutela de conteúdos.

Do mesmo modo e com a mesma linha de argumentação do referido na dimensão da patrimonialidade, é inelutável que os sistemas informáticos (e a redes informáticas, conforme a definição da al. a) do art. 2 da Lei da Criminalidade Informática) comportam uma dimensão da realização humana, traduzida em documentos, em registos, em tipos de programas seleccionados que se encontram ancorados naquelas plataformas informáticas. É uma dimensão mais próxima da expressão da privacidade ou da «privacy». Apesar da incidência da acções sobre estes dados constituir um resultado, a perscrutação dos conteúdos vertidos nos sistemas informáticos preconizam essencialmente o desvalor da acção.

Se adoptássemos uma atitude de considerar no crime de acesso ilegítimo apenas a protecção de qualquer uma destas últimas dimensões, estaríamos a amputar o significado conceitual do bem jurídico das suas outras dimensões, que se revelam decisivas para compor o âmbito de protecção do fenómeno relacional que lhe está subjacente.

Mas também é verdade que não se pode prescindir delas. Das duas últimas dimensões resulta a existência de um figurino ambivalente do bem jurídico segurança dos sistemas informáticos, que está, pois, para além da sua dimensão típica (a primeira dimensão referida). Há uma diversidade qualitativo-quantitativa que, simultaneamente, mas não necessariamente em pesos equivalentes, toca a noção de património e a noção da reserva privada.

Ora, estas dimensões axiológicas não são clusters. Não se encontram fechadas numa redoma, nem são estáticas. Já referi que compreendo que o bem jurídico «segurança dos sistemas informáticos» é o horizonte de protecção de três tipos da criminalidade informática levitacional técnica (crime de acesso ilegítimo, crime de sabotagem informática e crime de intercepção ilegítima). Estes tipos são constituídos por elementos objectivos razoavelmente distantes, o que quer dizer que se direccionam para a censura de acções que podem encontrar-se relativamente afastadas entre si. Não era admissível que se compreendesse que estes tipos conjungavam do mesmo modo todos aqueles valores.

Estas cargas axiológicas, como todos os valores, são relativas. Não devem ser tidas como imóveis. Não faz sentido, nem tal pode ser admitido, que se pretenda compreender que estas dimensões sejam estanques, ou que o seu peso não possa variar no mecanismo relacional que fundamenta a censura criminal que se consubtsancia na tipificação de diversos crimes. Nesse sentido, a ponderação destes valores não é, nem necessariamente homogénea e proporcionada nos diversos tipos de ilícito, nem a sua correlação de forças é a mesma nos diversos crimes levitacionais técnicos. Ou seja, nem a relação «dimensão própria»/«dimensão quantitativa»/«dimensão qualitativa» é necessariamente proporcional, nem é imutável, pois que, por um lado, pode a protecção de um determinado valor ser tida como mais relevante do que as outras, como pode essa relação variar consoante o tipo de ilícito em causa.

Trata-se, pois, de um conjunto de variáveis que, na análise comparada dos tipos, o intérprete deve cuidar de tratar.

7 · UM BEM JURÍDICO COM DUAS DIMENSÕES. UM BEM JURÍDICO INTERMÉDIO

Configurado, em traços gerais, o bem jurídico «segurança dos sistemas informáticos» devemos introduzir uma nova variável na consideração daquele bem jurídico-penal, que o vai caracterizar como ainda mais complexo. Nas secções anteriores, cuidámos de compor um bem jurídico que pareça razoável como protecção do tipo de incriminação em causa, mas o texto foi construído em torno da justificação da protecção de uma esfera de valores próxima da ofensa individual. Neste sentido, tentá-

mos responder à primeira questão que formulámos previamente.

Também referimos então que este plano de protecção era excessivamente limitado para compreender toda a expressão do tipo de bem jurídico em causa e que era necessário formular um segunda questão: «o que é que mais perturba a sociedade quando alguém acede, sem o respectivo consentimento ou excedendo-o, a um determinado computador?»

Será razoável colocar esta questão? Isto é, faz sentido perspectivar que o tipo de lesões produzidas no âmbito da criminalidade levitacional técnica pode ter ressonância para além da esfera do lesado individual? Sim, sim. O sentido das respostas a estas questões não pode ser outro.

Não é objecto do presente texto entrarmos em questões de fundamentação criminologia ou de enquadramento contextual desta criminalidade. Tomemos apenas as seguintes premissas que, creio, são consensuais. Acompanhando o percurso da relação do eu com a informática, a sociedade não prescinde hoje do uso de estruturas informáticas. A economia não sobrevive sem estas plataformas. E, quanto a este sistema económico, até, numa dupla perspectiva: a par da circunstância de as unidades clássicas (indústrias, comércio e serviços tradicionais e as entidades públicas) as terem adoptado como forma de tornar mais ágeis, eficientes e rentáveis os seus negócios ou áreas de intervenção, há um novo campo de exercício dos respectivos objectos sociais que pressupõe a existência de infra-estruturas informáticas estáveis: os operadores dos, em geral, chamado e-commerce e e-government. Particularmente quanto a estes operadores, a estabilidade do funcionamento dos equipamentos não é uma dependência resultante de um esforço de modernização. É um pressuposto do seu funcionamento. Foi a própria modernização que impôs estes modelos de expressão comercial.

Ora, quando as infra-estruturas informáticas sofrem instabilidade fruto de acções delitivas, os próprios operadores desmotivam-se. Deixa de justificar-se a aposta na inovação e na apresentação de novos modelos de comércio ou de novas funcionalidades. Mas não são só aqueles que sofrem os efeitos de tais actos. Os próprios consumidores ou utilizadores das estruturas deixam de reconhecê-las como formas de utilização. Desconfiam delas, consideram-nas ineficazes. De novo, decai a justificação para se imporem novos modelos de expressão.

Não pensemos, por ora, no caso do crime de acesso ilegítimo. Utilizemos uma situação mais óbvia. Alguém pode contestar que a verificação de situações de DoS (que podem não ser particularmente lesivas em termos de danos produzidos nos equipamentos) sobre, por exemplo, a «Amazon» ou às diversas empresas que disponibilizem bens online, leva a um processo de descredibilização e de desconsideração deste tipo de actividade e que, quer os próprios operadores, que se vêem impossibilitados de fazer negócio, quer os utilizadores, que se impacientam com a circunstância de não conseguirem efectuar as transacções que pretendem [33], sentem um misto de impotência e de revolta pela utilização dos acessos através da Internet?

O reconhecimento deste facto é a aceitação de que não se pode fugir a enquadrar uma importantíssima dimensão extra-individual do bem jurídico «segurança dos sistemas informáticos» e que se traduz, em geral, na compreensão da necessidade de assegurar a performance de um bem indispensável para a realização da colectividade (pelo menos, nos pressupostos em que esta agora assenta) e, em especial, na manutenção da integridade do tráfego informático, também ela, pressuposto da realização colectiva.

Já não bastava ao bem jurídico em causa ser polifacetado quanto às cargas axiológicas que lhe devem ser agregadas, este bem jurídico tem, também, dois planos de protecção: um plano individual e um plano colectivo. Esta «bi-dimensão estrutural» determina-lhe uma amplíssima tutela de protecção, dimensão esta que «estará legitimada sempre que estes sejam úteis para o fim do homem na sociedade» [34].

O bem jurídico segurança dos sistemas informáticos tem, então, dois ângulos de projecção: o plano colectivo ou supra-individual e o plano individual. Estamos, pois, a configurar este bem jurídico como um bem jurídico intermédio. Não se vocaciona apenas para a protecção de uma esfera individual, como nos bens jurídicos ligados à pessoa ou ao património [35], nem tão somente para a órbita colectiva (como é regra nos crimes contra a sociedade, a economia).

---

33 E todos sabemos quais os tempos médios de espera, por partes dos cibernautas, nos acessos a sites.

34 Neste mesmo sentido, Jesús-María Silva Sanchez: *Aproximación al Derecho Penal contemporáneo (reimpresión)*, Barcelona, 1992.

35 Esta afirmação tem que ser tida com alguma margem de condescendência.

Nenhum destes dois planos, em termos parcelares, consegue abarcar a verdadeiramente complexa teia relacional ligada aos valores, às cargas axiológicas, em causa. É absolutamente imperativa a configuração de que a protecção se deve projectar para aquelas duas esferas. Ou seja, é um conceito de bem jurídico cujo objecto de tutela da norma penal não está adstrito a uma determinada pessoa, nem à colectividade, de per si, mas referencia-se-lhes, a ambos.

Permitam-me esta associação. Tal como a regra na interpretação das normas penais de que, para a consumação de um determinado tipo, o dolo deve percorrer todos os elementos objectivos do tipo de ilícito (no caso de tipos dolosos, obviamente), também aqui este plano supra-individual do bem intermédio «segurança dos sistemas informáticos» percorre os diversos iteres axiológicos (as três dimensões de valores) daquele bem jurídico. Quero com isto dizer que o ângulo de protecção colectivo é tocado pelas referidas três dimensões do bem jurídico em causa.

Na verdade, também o sistema social global [36] é tocado pela necessidade de protecção dos três tipos de valores agregados a este bem jurídico.

Senão vejamos.

Deve ser reconhecido que o plano colectivo é marcado pelo âmbito mais próprio deste bem jurídico. Na verdade, é forçoso aceitar que o mecanismo relacional do sistema social com a informática fica perturbado com a real perda de domínio e de controlo sobre as suas «próprias» estruturas informáticas e que os actos delitivos afectam decisivamente aquela relação instituída.

Mas também não deve deixar de ser reconhecido que pode haver um sentimento colectivo de ânsia de protecção da integridade dos próprios sistemas informáticos e redes informáticas, na lógica patrimonial da evitação de danos.

Como não pode ser afastado o reconhecimento social da necessidade de preservação dos conteúdos constantes ou que circulam nas plataformas informáticas.

Temos, então, um duplo ângulo de horizonte que deve abarcar a tripla dimensão de valores sustentados no bem jurídico «segurança dos sistemas informáticos». Uma protecção extra-individual e uma dimensão individual que se espalha, em ambos os planos, por três «preocupações»: a necessidade de salvaguarda do poder dispositivo sobre os bens informáticos, sem que os mesmo devam ser objecto de actos disruptivos; a dimensão quantitativa da perda; finalmente, a dimensão qualitativa que é expressão mais directa da preservação da comunicação fechada.

Encontrando-se sempre no horizonte de protecção dos crimes levitacionais técnicos estas três dimensões, a forma como o plano supra-individual configura a valoração destas três dimensões e o peso que cada uma delas deve ter varia consoante o tipo de ilícito que se esteja a analisar. Ou seja, tal como no plano individual, a preponderância destes valores para a sociedade não é exactamente a mesma no crime de acesso ilegítimo, no crime de sabotagem informática, ou no crime de intercepção ilegítima.

Já veremos como esta variável é composta no crime de acesso ilegítimo. Por agora, é necessário fechar o círculo da fundamentação teórica deste bem jurídico.

8 · O BEM JURÍDICO NO CRIME DE ACESSO ILEGÍTIMO

Da estrutura conceitual do bem jurídico, que foi enunciada supra, resulta que o bem jurídico-penal em questão é complexo, é elástico, aceita o diferente peso das suas variáveis, consoante o tipo de ilícito em que se inscreva.

Isto é tanto assim, quer na acentuação das diversas dimensões axiológicas que o bem jurídico comporta, quer na dicotomia que se estabelece entre os dois planos que o bem jurídico intermedeia. Temos, pois, um jogo de cinco variáveis, divididas em dois níveis.

Também foi referido que, na intermediação entre os planos pessoal e extra-individual (ou colectivo), estes têm sempre, na linha do horizonte, os três tipos de valores intrínsecos ao tipo. Em termos abstractos, os bens jurídicos intermédios protegem cumulativamente bens jurídicos penais individuais, mas não deixam de ter a mira dos interesses relacionais colectivos, «ou, então, protegem bens jurídico-penais colectivos e, simultaneamente, têm, como mira de observância, referências individuais». Este bem jurídico tem uma necessária dupla dimensão que oscila consoante os tipos de ilícito em que se encontre inscrito, não necessitan-

36 Que incluem todos os demais sistemas.

do sequer de serem combinados de forma homogénea. Quer dizer, a estrutura de relação entre o eu e o objecto de protecção e a estrutura de relacionamento entre a pluralidades de eus, o referencial sistémico, e aquele objecto deve percorrer todos os iteres substantivos, isto é, os valores intrínsecos ao bem jurídico, e apurar o modo como lidam com os diversos valores em causa.

Tendo perante nós um corpo normativo de direito secundário e aceitando aquela regra genérica de que é do recorte do tipo que se vislumbram os bens jurídicos protegidos por normas penais de direito penal extravagante, a interpretação dos crimes informáticos técnicos (nomeadamente os art. 6.º a 8.º da Lei da Criminalidade Informática) deve levar-nos a reconhecer nos respectivos tipos de ilícito a necessidade de protecção do bem jurídico «segurança dos sistemas informáticos».

Mas o tipo deve levar-nos a um esforço interpretativo suplementar: sendo o bem jurídico em causa complexo, há que reconhecer, na porosidade literal do tipo, qual a correlação de forças que o mesmo determina. Isto é, qual o peso relativo das diversas dimensões (os três tipos de valores – a saber, a preservação da confiança dos users «num meio comunicacional e num equipamento dele absolutamente independente»; o acento material, quantitativo; a protecção da expressão-conteúdo inserta naqueles equipamentos) e como jogam ou funcionam entre si os seus planos (a variabilidade entre o plano individual e o plano colectivo).

É esta árdua tarefa que se impõe ao intérprete

Se o crime de acesso ilegítimo é o crime que centraliza as questões no âmbito da criminalidade informática técnica, seria mais ou menos óbvio que também é o tipo de ilícito informático técnico que melhor equilibra as diversas variáveis em causa. O que faz todo o sentido, se pensarmos que é um «tipo de entrada» e que, por isso, desvenda as demais possibilidades de acção delitiva. O crime de acesso ilegítimo é um crime barreira, que visa evitar a prática de crimes tidos como mais graves. Ou pelo menos, relativamente aos quais a dimensão do dano ou da revelação de conteúdos é mais intenso. Na posição expressa neste texto isso não quer dizer crimes necessariamente mais graves em absoluto, mas tão só crimes cuja incidência nas dimensões qualitativa e quantitativa é mais acentuada. Os crimes sucedâneos (aqueles que o crime de acesso, como crime barreia pretende, no limite, evitar) serão mais compreendidos pela comunidade. Serão aparentemente mais sentidos, mas não serão forçosamente os que lesam mais intensamente o bem jurídico em causa. Ou, em termos mais rigorosos, poderão não lesar tão intensamente todas as dimensões do bem jurídico como outros tipos de ilícito aparentemente mais inócuos.

Mas voltemos ao crime de acesso ilegítimo. Este tipo de ilícito é um crime central, que como crime barreira, tem sempre como horizonte último a demais criminalidade informática técnica, pois que é a esta criminalidade que este se dirige. Mas, de acordo com os seus elementos objectivos, trata-se tão só de um crime através do qual o legislador pune as condutas de um certo tipo de penetração informática (que na lei portuguesa tem um sentido criminológico de não punir as condutas de hacking, ou mero intrusismo informático).

Só que é indiscutível o valor deste tipo para além da sua configuração formal. Há um claro sinal de que este crime também se encontra tipificado para alertar para a proibição de outros actos de delito. Estamos, pois, perante a fixação e uma barreira prévia à consumação de certos tipos tido como de maior desvalor. Esta protecção avançada perspectiva-se, então, relativamente a uma amplíssima gama de resultados (desde a evitação de danos em programas ou sistemas informáticos, a outras incidências de acção sobre redes ou sistemas informáticos, ou a não intercepção de telecomunicações informáticas). É um campo largo a que o crime se alonga.

Como crime de entrada que é, segue a regra dos demais tipos quanto ao critério da intensidade da lesão: orbita no mundo do perigo. Em geral, estes crimes são instituídos como crimes de perigo e, mais especialmente, como de perigo abstracto [37].

Em geral, referi eu. Não é, em regra, assim quando o objecto de protecção do tipo de ilícito se configura como um bem jurídico intermédio. Nestas situações, a tradição dogmática tende a considerar que não há uma ofensa de perigo à dimensão colectiva. A prática das acções tidas como desvaliosas impõe quase automaticamente o resultado dano, a própria

37 Sobre o perigo no Direito Penal, cfr. Claus Roxin: «*Derecho Penal - Parte General, Tomo I, Fundamentos. La Estructura de la Teoria del Delito*», trad. e notas de Diego-Manuel Luzón Peña, Miguel Diaz y Garcia Conlledo e Javier de Vicente Remesal, Madrid, 1997, e Ricardo M. Mata y Martin: «Bienes jurídicos intermedios y delitos de peligro», *Estudios de Derecho Penal*, Granada, 1997.

lesão (e não o resultado perigo), na dimensão colectiva, que deve sentir o toque de tais acções. O perigo só é tido na dimensão individual, pois que ao dano que se verifica no plano colectivo pode vir a suceder-se o dano no plano individual. Ou seja, a conduta que provoca danos na dimensão colectiva do bem jurídico é, em abstracto, suficientemente razoável para que se enquadre a possibilidade de se provocar um dano individual. Neste sentido, tende a considerar-se que estes crimes que lesam bens jurídico intermédios são de dano para a vertente colectiva e de perigo (abstracto) para a vertente individual. Estas são, aliás, também as regras que se devem considerar quando se tratar dos crimes de sabotagem informática e de intercepção ilegítima.

Só que o crime de acesso ilegítimo é um crime muito especial. É, como já referi, um emblema, o símbolo de entrada da criminalidade informática técnica. Eu creio dever considerar-se que a prática de actos de acesso ilegítimo não tem necessariamente de conduzir ao dano na vertente colectiva do bem jurídico.

O legislador tipificou como crime as condutas de acesso a sistemas e redes informáticos não consentidas e que tenham sido levadas a cabo com a intenção de se obterem «outros» resultados. Todos nós devemos reconhecer que as margens de justificação da aplicação do ordenamento penal a estas condutas está no limiar da aceitabilidade. Aceita-se e justifica-se. Mas é no limbo. Se, aparentemente, parece não haver qualquer indeterminação quanto aos elementos objectivos fixados no tipo (não se trata da tipificação de presunções activas ao nível dos elementos objectivos do tipo de ilícito), a razoabilidade daquela censura é periclitante.

Perante um tipo que é menos, digamos assim, menos incisivo, o resultado que decorra da acções típicas não é necessariamente tão directo. Não há necessariamente uma lesão fruto do comportamento do agente. Neste sentido, creio poder considerar-se que, de um acesso ilegítimo não tem que resultar necessariamente o dano na vertente colectiva. O que acontece é que aquelas condutas são suficientemente razoáveis para que haja o perigo de a comunidade sentir a possibilidade de sofrer actos lesivos, ou seja, há o perigo concreto para o plano colectivo.

No plano individual, o perigo para a consideração do desvalor do resultado (sobretudo este) e da acção é abstracto, pois que, em abstracto, as condutas são suficientemente direccionadas para provocar danos na confiança dos titulares dos sistemas informáticos ou dos utilizadores das redes informáticas e nos bens informáticos em concreto de determinado utilizador ou, ainda, nos conteúdos ali existentes.

Em suma, creio que, relativamente ao crime de acesso ilegítimo, se pode sustentar estarmos perante uma situação de perigo-perigo: perigo concreto para o plano colectivo e perigo abstracto para o nível individual. Quer isto dizer, que se trata de um crime de perigo concreto-abstracto.

Analisado o crime de acesso ilegítimo quanto ao critério da intensidade da lesão, dos seus fundamentos e das conclusões a que chegámos já resulta que o crime em causa é um crime de centro, quanto à ponderação dos seus diversos valores. Mas, no tocante aos dois planos (individual e colectivo), este crime acentua o nível supra-individual do bem jurídico. Com efeito, este tipo de crime, quer pela sua dimensão de protecção avançada genérica, quer pelo horizonte de recondução aos demais tipos de ilícito, expressa mais impressivamente um objecto de tutela colectiva. O sinal que se dá é claramente a necessidade de protecção geral da manutenção da integridade e da fiabilidade das estruturas informáticas e, bem assim, de não se dever tocar nos mecanismos de comunicação socialmente instituídos. Do texto constante do art. 7.º da Lei n.º 109/91 resulta mais acentuadamente a protecção deste plano.

Não quer isto dizer que o plano individual não tenha expressão, obviamente. Tem-na e é, até, objecto de um particular elemento objectivo: a causa de justificação «falta de autorização».

Prevê o crime de acesso ilegítimo que a censura relativamente ao break-in só deve ser aceite quando o mesmo decorra da falta de autorização para tal acesso. Em termos dogmáticos, esta reserva é expressão de uma vertente negativa da comunicação, em que alguém fecha o espaço de comunicação a um conjunto pré-seleccionado de agentes. Os outros não entram. Não devem poder entrar, o que é expressão da preservação da «dimensão comunicacional fechada».

Em regra, a preservação da comunicação não necessitaria de ser expressa. A mesma já resulta do sentido cognitivo da protecção e poderia ser enquadrada nos termos gerais do Direito Penal, como causa de exclusão da ilicitude (art. 31.º, n.º 1, al. d), art.s 38.º, n.º 2, e 39.º, todos do Código Penal) – em especial quando o consentimento fosse expresso, ou fosse de presumir.

No entanto, no caso do crime de acesso ilegítimo (contrariamente ao que sucede na demais criminalidade levitacional técnica), as vantagens da utilização de uma tal cláusula (ainda que deva ser aperfeiçoada) aconselham à manutenção da sua existência. Por um lado, trata-se de uma técnica recorrente nos tipos clássicos com traços conceituais aproximados. Isto leva a que, mais do que um novo elemento de interpretação do tipo, que pode sempre consistir num ruído interpretativo [38], é um elemento objectivo pacífico e reconhecido. Não é um elefante no Harrods. Convive-se bem com ele. Por outro lado, se (voltamos, de novo, a este ponto) estamos perante uma norma penal de Direito Secundário cujo objecto de protecção resulta, em geral do próprio recorte da norma, é precisamente esta dimensão que melhor dilucida e de forma expressa, a existência de bem jurídico em causa. Já não é só o elemento que sofre a acção (o bem informático, que tem um titular mais ou menos individual) que cristaliza a tal dimensão pessoal, a causa de justificação aponta-a expressamente.

Questionou-me um dia, em sessão pública, o Senhor Professor Costa Andrade sobre se esta construção, designadamente a configuração de um plano colectivo no bem jurídico, não apresentava alguns problemas quanto à formulação do consentimento. Vindo de um penalista com uma longuíssima tradição no estudo do acordo e do consentimento no Direito Penal, tomei a questão com cautela. A pergunta era uma provocação com sentido. Efectivamente os bens jurídicos com planos colectivos têm problemas ao nível da expressão do consentimento. Se são colectivos, há acordos colectivos? Fazem sentido? Respondi que é também precisamente por essa dificuldade que faz sentido considerar que este bem jurídico é intermédio, que tem, também, um referencial individual e que tal causa de justificação se apresenta ligada a este plano. Por isso, não contende com as dificuldades no acordo que as dimensões colectivas sempre comportam.

Em suma, o crime de acesso ilegítimo alonga-se para o plano colectivo, mas não deixa de ter também como referente o plano individual.

Finalmente, aqueles dois planos devem abarcar os três tipos de cargas axiológicas intrínsecos ao bem jurídico-penal em análise.

O crime de acesso ilegítimo é um crime de centro, que se projecta para uma diversidade activa, censurada em outras normas penais. Por ser maleável, direi que não é, quanto à oscilação dos valores do bem jurídico que deve proteger, desequilibrado. É um crime em que as diversas dimensões se encontram razoavelmente equilibradas. As diversas dimensões estão claramente representadas, mas há uma que tem a primazia sobre as demais.

Há, ou não fosse este crime um símbolo desta criminalidade, um acentuar da dimensão própria do bem jurídico. Quer isto dizer que o valor protegido neste tipo de ilícito é essencialmente a preservação da manutenção dos mecanismos de expressão informática, de comunicação. Na verdade, quando alguém vê o seu sistema acedido ou a comunidade sente que uma determinada rede foi objecto de um acesso indesejado, a sensação que resulta é de desconforto perante a situação, de impotência. É uma preocupação de algo difusa definição. Dela resulta o feeling de que a todo o momento podemos estar vulneráveis, ou de que os nossos sistemas podem, a todo o momento, não responder fielmente ao que as suas funcionalidades lhe possibilitam. Há, pois, que atender à necessidade de protecção do acesso do user à plataforma de acesso à comunicação e que esta seja efectuada de acordo com os padrões normais. Ou melhor, o não destruir ou danificar a relação de confiança nestas estruturas informáticas.

Esta é, em termos miméticos, outra forma de traduzir a dimensão própria do bem jurídico, dimensão esta que tem mais peso, em relação às demais, no crime de acesso ilegítimo.

Mas as demais também se encontram tratadas no tipo em causa.

A dimensão qualitativa, simultaneamente de forma implícita e de forma expressa.

De forma implícita quando a acção modal «aceder», prevista no tipo, contém necessariamente o horizonte amplo de o acesso ter como resultado mediato e final o acesso a conteúdos, à expressão do eu que se encontram registados nos equipamentos e programas informáticos.

De igual modo, a existência da já referida causa de justificação «falta de autorização», ao expressar a manutenção da circularidade da comunicação em termos fechados, implicitamente deve levar-nos a considerar estarmos perante a preservação das cargas axiológicas referentes aos conteúdos que constam dos sistemas e redes informáticos ou que cir-

38 Quanto mais elementos uma norma penal tiver, mais complexa é a sua interpretação.

culam nas redes informáticas. Há, pois, uma evidente recondução da protecção deste tipo para a tal dimensão qualitativa.

E, depois, esta dimensão fica expressamente reconhecida no tipo com a norma qualificativa constante da al. a) do n.º 3 do art. 7.º da Lei n.º 109/91. Quando o legislador entendeu dever considerar, compondo até como qualificação da norma penal geral, a possibilidade de existência de um resultado de acção concreto que incide sobre «segredos comerciais ou industriais» e de «dados confidenciais» há uma ressonância directa daquela dimensão qualitativa do bem jurídico «segurança dos sistemas informáticos». É incontornável. Não pode ser desconsiderada.

De forma expressa, a dimensão quantitativa também é considerada no tipo de ilícito previsto no art. 7.º da Lei da Criminalidade Informática, designadamente quando se prevê a qualificação dos actos de acesso que determinem a obtenção de um patamar elevado de benefícios ou de vantagens patrimoniais (na al. b) do n.º 3).

Estamos num domínio perfeitamente inserido na lógica de fundamentação patrimonial de alguns tipos de ilícito. Há benefícios, há uma quantificação patrimonial que é expressão também de situações de concorrência desleal [39].

A este argumento acresce a qualificação da alínea anterior (a al. a) do n.º 3). Se, à primeira vista, a obtenção de segredos pode determinar a lesão da dimensão qualitativa (conforme referido supra), também não se pode afastar que esta circunstância não deixa de ser um determinador económico. Aqueles segredos e dados confidenciais têm um valor quantitativo próprio e, nesse sentido, também compõem o ramo da dimensão quantitativa do bem jurídico.

Ainda assim, na ponderação entre estas duas dimensões, creio que o sentido de maior peso deve ser atribuído à dimensão quantitativa, pois que esta última, como ressonância mais mediata da acção, tem maior visibilidade.

Em suma, as diversas dimensões axiológicas estão preenchidas pelo tipo de ilícito. Os dois planos são reconhecidos no tipo. Mas como vemos, nenhuma das componentes dos dois tipos de variáveis (dimensões e planos) tem peso homogéneo.

9 · CONCLUSÃO

Estas últimas secções não demonstram só o reconhecimento de o bem jurídico protegido no crime de acesso ilegítimo ser «a segurança dos sistemas informáticos», ou a justificação de se construir o bem jurídico conforme efectuámos. Levam a um alcance mais longínquo: à falência das construções simplistas neste âmbito.

O tipo é complexo, já o reconhecemos. Mas não é artificialmente complexo. A sua complexidade é determinada pela extrema complexidade e profusão dos valores que são emanados do fenómeno relacional que fundamenta a sua existência. É esencial reconhecer este facto.

Se o crime de acesso ilegítimo contém uma modalidade de acção diferenciada, se há especificidades no objecto da acção e se o seu objecto de protecção é também único (ou, pelo menos, diverso dos bens jurídico-penais considerados fora da criminalidade levitacional ou informática), estamos perante um crime com um «referencial autónomo, que transcende o horizonte clássico dos tipos de ilícito». É, pois, um crime novo, praticado por novos meios.

Quando nos foi colocado este desafio, abraçámo-lo essencialmente para tentar desmistificar algum imobilismo e descrença que parecem existir quanto ao modo como o ordenamento jurídico se deve adaptar a eventuais novas situações que devam ser objecto de protecção ou de regulação.

Em especial, no domínio penal, no domínio da ilicitude. O que, aliás, nos permitiu, através de um mero exemplo, como tantos outros existem, desmontar e negar aquele pavoroso símbolo de que «o que é ilícito no mundo real é ilícito na Internet e vice-versa» e concluir que há espaços caracterizadores próprios e que nem tudo é reproduzível do mesmo modo, nos dois universos.

Creio que são argumentos como estes que devem começar a compor novas linhas argumentativas do direito, novas lógicas de fundamentação e, simultaneamente, determinar a forma como o ordenamento jurídico próximo destas matérias deve ser construído.

Pouco importa que haja quem visceralmente rejeite o novo Direito das Tecnologias da Informação e

39 O modo como esta norma se pode articular com o art. 260.º do Código da Propriedade Industrial, o que será dizer analisar as situações em matéria concursal, é também um interessante tema de estudo.

da Comunicação (e os novos diplomas legais neste entorno, tais como o Decreto-Lei n.º 7/2004, de 7 de Janeiro, a Lei n.º 5/2004, de 10 de Fevereiro, ou o Decreto-Lei n.º 62/2003, de 3 de Abril, todos eles transpondo relevantíssimos pacotes de directivas comunitárias e as suas originais soluções, desmentem-no claramente).

Há manifestos exemplos de curvas de diferenciação – em especial provocadas pelos novos meios de acesso à informação e às novas formas de comunicação – relativamente ao que está previamente instituído. Não deve o direito cuidar de forma particular, ou seguindo uma linha diferenciada, estas situações?