A LEI DO CIBERCRIME E A COLABORAÇÃO DO ARGUIDO NO ACESSO AOS DADOS INFORMÁTICOS

A lei do cibercrime e a colaboração do arguido no acesso aos dados informáticos

O presente artigo procura indagar, à luz das disposições consagradas na Lei do Cibercrime, se um arguido pode ser coagido pelas autoridades judiciárias a colaborar na obtenção de prova armazenada no seu computador, nomeadamente através da revelação da sua palavra-passe, tendo em conta a proteção constitucional conferida pelo direito do arguido à não autoincriminação.
Com esta finalidade, analisam-se os regimes processuais instituídos em dois dos mecanismos de obtenção de prova previstos na referida Lei do Cibercrime: (i) a injunção para apresentação ou concessão do acesso a dados e (ii) a pesquisa e apreensão de dados informáticos.

Palabras clave
Cibercrime, obtenção de prova, dados informáticos.

The Portuguese Cybercrime Law And The Cooperation Of The Defendant In Obtaining Access To Computer Data

This article seeks to problematize, under the Portuguese Cybercrime Law, if an accused can be compelled by judicial authorities to cooperate on the collection of evidence stored on its computer's hard drive, notably through the disclosure of its password, taking into account the constitutional protection of the privilege against self-incrimination.
For this purpose, the procedural regimes established in two mechanisms of collection of evidence provided in the Portuguese Cybercrime Law are analyzed: (i) the injunction for presentation or granting access to data and (ii) the search and seizure of computer data.

Key words
Cybercrime, Collection of Evidence, computer data.

Fecha de recepción: 3-9-2014 *Fecha de aceptación: 1-10-2014*

O ÂMBITO E OS LIMITES DO DIREITO À NÃO AUTOINCRIMINAÇÃO

O direito à não autoincriminação (no brocardo latino *nemo tenetur se ipsum accusare)* é amplamente reconhecido no ordenamento jurídico português, e, muito embora não tenha consagração constitucional expressa, é na generalidade das vezes reconduzido às garantias processuais consagradas nos artigos 20.º, n.º 4, e 32.º, n.os 2 e 8, da Lei Fundamental.

Compreendido naquele princípio mais amplo de que nenhum arguido deve ser coagido a colaborar com a justiça em situações incriminatórias, encontra-se o direito ao silêncio, que incide, numa vertente mais direta, sobre o direito do arguido a não prestar declarações sobre a factualidade que lhe é imputada, e, numa vertente mais ampla, igualmente sobre o direito a não ter que entregar documentos ou outros elementos ou a não ter que atuar de determinada forma, como, por exemplo, indicando o local onde aqueles elementos se encontram. Como, aliás, refere Vânia Costa Ramos, *sem o direito ao silêncio, o arguido seria obrigado a declarar e cooperar sempre que estes actos não revestissem conteúdo autoincriminatório* (cfr. «Corpus Juris 2000 – Imposição ao arguido de entrega de documentos para prova e *nemo tenetur se ipsum accusare*», *Revista do Ministério Público*, N.º 108, 2006, p. 132). Este direito ao silêncio, embora não tenha consagração constitucional, já encontra respaldo na lei adjetiva penal, nomeadamente no artigo 61.º, n.º 1, alínea d), do Código de Processo Penal.

No entanto, como se sabe, o processo penal é foco permanente de tensões entre o dever de eficácia que é exigido aos responsáveis pela investigação criminal e as garantias de defesa que cabem a todos os arguidos. É, assim, neste âmbito que assume relevância a ponderação deste amplo direito dos arguidos em não colaborar para a autoincriminação, quando em confronto com outros valores como a eficácia da investigação criminal e a tutela efetiva da justiça. Desta ponderação, diga-se, desde já, têm sido assumidas pelo legislador restrições ao *nemo tenetur*, sempre por via da intervenção do princípio da proporcionalidade, com previsão constitucional expressa no artigo 18.º, n.º 2, da Lei Fundamental, como são exemplos os exames de alcoolémia e substâncias psicotrópicas (artigo 152.º, n.º 3, do Código da Estrada) ou os exames de ADN para fins de investigação criminal (artigo 8.º, n.º 1, da Lei n.º 5/2008, de 12 de fevereiro, e artigo 172.º do Código de Processo Penal).

Olhando agora para um caso concreto, constatando-se nos dias de hoje a importância que assumem os computadores (e demais sistemas informáticos com a mesma funcionalidade), o seu uso generalizado para as comunicações e o enorme potencial de armazenamento de informações e dados, o que concretamente se pretende apurar é se, perante a pretensão da investigação criminal em aceder aos dados informáticos de um arguido, este se encontra coagido a colaborar com as autoridades, concedendo o acesso ao seu computador / demais dispositivos eletrónicos equiparáveis, nomeadamente através da revelação da palavra-passe, no pressuposto que esta é apenas do

conhecimento do próprio. Ou será esta possibilidade uma violação inadmissível do referido princípio do direito à não autoincriminação?

A LEI DO CIBERCRIME

Havendo possibilidade, como já se viu, de restringir o princípio *nemo tenetur*, em prol de outros interesses salvaguardados pelo ordenamento jurídico, tal só pode suceder quando existe comando legal expresso e se se encontrarem respeitados os limites constitucionais para a restrição dos direitos fundamentais.

Até 2009 não havia nenhuma solução legislativa acerca da questão concreta acima colocada. No entanto, em 2009 foi aprovada a Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro), que transpôs para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro (relativa a ataques contra sistemas de informação), e adaptou o direito interno à Convenção sobre Cibercrime do Conselho da Europa, adotada em 23 de novembro de 2001.

Este diploma legal subdivide-se fundamentalmente numa parte substantiva, em que preveem os crimes informáticos anteriormente previstos na Lei da Criminalidade Informática (Lei n.º 109/91, de 17 de agosto, entretanto revogada pelo artigo 31.º da lei do Cibercrime); numa parte adjetiva, em que preveem concretas diligências de obtenção de prova; e numa terceira parte, relativa à cooperação internacional.

Com particular interesse, importa atentar nas disposições processuais, previstas nos artigos 11.º e seguintes. Desde logo, consagra a Lei do Cibercrime que a generalidade dos meios de obtenção de prova nela previstos se aplicam não só aos crimes consagrados na mesma lei (falsidade informática, dano relativo a programas ou outros dados informáticos, sabotagem informática, acesso ilegítimo, interceção ilegítima e reprodução ilegítima de programa protegido), mas também a todos os crimes cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico. Está-se, pois, perante um âmbito muito alargado de aplicação de algumas das disposições processuais previstas na Lei do Cibercrime, concretamente a preservação e a revelação expedita de dados de tráfego, a injunção para apresentação ou concessão do acesso a dados e a pesquisa e apreensão de dados informáticos e de correio eletrónico. De fora ficam apenas dois dos meios previstos nesta Lei: a interceção de comunicações (que restringe o seu âmbito de aplicação aos crimes previstos na mesma lei e ao catálogo de crimes previsto para as escutas telefónicas) e as ações encobertas (apenas admissíveis aos crimes previstos na Lei do Cibercrime e a um catálogo próprio previsto na alínea b) do n.º 1 do artigo 19.º).

Significa isto que a maior parte dos meios de obtenção de prova que se encontram previstos na Lei do Cibercrime podem ser aplicados à generalidade dos processos-crime, se, obviamente, houver interesse em proceder à recolha de prova em suporte eletrónico. O que nos leva, efetivamente, a perguntar se perante esta lei se passou a consagrar a possibilidade – alargada – de as autoridades exigirem o acesso a qualquer computador, nomeadamente ao dos arguidos.

(i) *A injunção para apresentação ou concessão do acesso a dados*

Um dos meios de obtenção de prova previstos na Lei do Cibercrime é a injunção para apresentação ou concessão do acesso a dados, prevista no artigo 14.º, a qual basicamente consagra que as autoridades judiciárias podem ordenar, a quem tenha a disponibilidade ou o controlo de dados informáticos específicos e que se encontrem armazenados num determinado sistema informático, que os comunique ao processo ou que permita o acesso aos mesmos. Prevê ainda este artigo que quem não atuar segundo as imposições previstas pode ser punido pelo crime de desobediência, previsto e punido pelo artigo 348.º do Código Penal.

Esta disposição processual reúne, no fundo, duas possíveis atuações por parte das autoridades, que ficam legitimadas quer a ordenar a comunicação ao processo dos dados informáticos pretendidos, como a exigir – em alternativa – o acesso direto das autoridades ao sistema informático para obtenção dos referidos dados, dados estes que têm que ser identificados e concretizados (n.º 2 do artigo 14.º).

Esta medida responde, assim, às dificuldades sentidas por parte das entidades que levam a cabo a investigação criminal, no acesso a um tipo de informação geralmente armazenada em sistemas informáticos com grande capacidade de armazenamento e nos quais é difícil identificar os concretos dados pretendidos, ficando a pessoa a quem é imposta esta injunção com o ónus de os autonomizar e transmitir / conceder acesso.

Trata-se, no entanto, de uma medida invasiva da esfera de proteção pessoal dos visados, caso os

dados de que tenham a disponibilidade sejam os guardados em computador próprio, os quais podem respeitar às mais diversas esferas da sua vida, particular e profissional. Repare-se que, para efeitos da Lei do Cibercrime, «dados informáticos» são todos aqueles que configuram a representação de factos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função [cfr. alínea b) do artigo 2.º].

Ora, impõe-se, por isso, saber se esta imposição pode ter por alvo o arguido, já que isso implicaria uma clara opção do legislador em restringir o já referido princípio do *nemo tenetur* em detrimento da eficácia da investigação criminal. E a resposta é negativa: o legislador ponderou bem os interesses e direitos aqui em conflito, tomando a opção clara de salvaguardar o direito à não autoincriminação ao consagrar no n.º 5 do artigo14.º que a injunção para apresentação ou concessão do acesso a dados não pode ser dirigida a suspeitos ou arguidos no processo em que for determinada a própria medida.

Igual proteção é conferida a todos os sistemas informáticos utilizados para o exercício da advocacia, das atividades médica e bancária e da profissão de jornalista (cfr. n.º 6 do artigo 14.º), encontrando-se também previsto que a esta injunção é também aplicável o regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182.º do Código de Processo Penal (n.º 7 do artigo 14.º).

Entendem-se e aplaudem-se as exceções formuladas, sendo que no que particularmente respeita à proteção do arguido (ou mesmo suspeito) parece ser esta a única forma de não impor uma colaboração ativa deste na recolha da prova da sua eventual incriminação.

Neste âmbito de proteção da esfera do arguido, bem como no que concerne à exceção dirigida às esferas de segredo (exercícios das atividades de advocacia, médica, bancária e jornalística), a questão que se coloca é se a injunção poderá ser aplicada a quem não é diretamente suspeito ou arguido, advogado, etc., mas tenha a disponibilidade ou controlo dos dados informáticos destes, por força, por exemplo, de uma relação pessoal ou, até com maior acuidade, da organização própria de uma estrutura empresarial.

Efetivamente, é comum constatar nos dias de hoje que a importância dos sistemas informáticos nos espaços próprios de exercício de profissões leva a que se contratem colaboradores próprios para o desempenho das funções informáticas. Ora, quanto aos suspeitos ou arguidos, a conclusão que se impõe é que estes colaboradores informáticos poderão ser coagidos a apresentar os dados daqueles ou a facultar o acesso aos mesmos. Esta solução vem sendo a defendida pelos Autores que já se pronunciaram sobre a (recente) Lei do Cibercrime, como Pedro Verdelho, que afirma que é possível exigir o acesso a computadores de empregados de uma empresa em cujos sistemas informáticos tenham deixado prova das suas atividades ilícitas (cfr. *Scientia Ivridica*, Tomo LVIII, N.º 320, Out.-Dez. 2009, p. 739). É evidente que esta será uma forma clara de contornar os dados não obtidos por via da restrição imposta no n.º 5 do artigo 14.º da Lei do Cibercrime, o que leva a concluir que o único valor que o legislador pretendeu efetivamente proteger foi o do direito à não autoincriminação, não impedindo que os dados dos arguidos sejam obtidos por outras vias, nomeadamente através da imposição a terceiros da injunção que se trata. Claro que nos casos em que o arguido seja a própria empresa, já não parece ser possível exigir dos colaboradores informáticos este tipo de acesso a dados.

A resposta é igualmente outra quando se aborda a exceção prevista no n.º 6 do mesmo artigo 14.º da Lei do Cibercrime e que veda a injunção relativamente a todos os sistemas informáticos *utilizados para o exercício da advocacia, das atividades médica e bancária e da profissão de jornalista*. Na verdade, ao contrário do que sucede com a exceção referente ao arguido, que visa proteger o princípio *nemo tenetur*, neste campo os valores salvaguardados já se colocam a nível de uma esfera supraindividual (a confiança da sociedade na profissão em si), não relevando a pessoa que utiliza o sistema informático, mas sim a finalidade deste, já que é a própria atividade profissional que merece do legislador uma proteção especial. Neste caso, o que está vedado é a exigência de apresentação ou acesso de dados informáticos que se encontrem nestes sistemas, pelo que já não será possível aplicar a injunção a outra pessoa que tenha a disponibilidade dos dados para além do advogado / médico, bancário ou jornalista, já que isso em nada altera o uso que é conferido ao sistema informático em causa, que continua a ser o do exercício das referidas profissões.

(ii) *As pesquisas e apreensões de dados informáticos*

Nos artigos 15.º e 16.º da Lei do Cibercrime prevê-se a possibilidade de proceder a «buscas» e apreensões no ambiente informático, diligências através das quais podem ser copiados para o pro-

cesso os dados ou documentos informáticos necessários à produção de prova.

Neste âmbito já não se encontra consagrada uma exceção de imposição das medidas processuais ao arguido, tal como se encontra previsto na injunção para apresentação ou concessão de acesso a dados, podendo-se, porém, encontrar também um regime mais restritivo para as pesquisas e apreensões realizadas a sistemas informáticos utilizados para o exercício da advocacia, das atividades médica e bancária e da profissão de jornalista (cfr. n.º 6 do artigo 15.º e n.º 5 do artigo 16.º, que remetem para as regras especiais consagradas no Código de Processo Penal, em salvaguarda das esferas de segredo profissional).

Está aqui presente o entendimento que vem sendo afirmado pelos tribunais (nomeadamente pelo Tribunal Europeu dos Direitos do Homem, no Acórdão *Saunders*) e pela doutrina, no sentido de existir uma natural delimitação negativa do direito à não autoincriminação, sempre que a prova em causa seja passível de ser obtida independentemente da vontade do arguido (como sucede, por exemplo, com os documentos apreendidos mediante um mandado de busca e com a recolha de tecidos corporais existentes no local do crime para posterior análise de ADN). De forma a não comprometer a eficácia destas buscas e apreensões, não se coloca na disponibilidade do arguido a possibilidade de se pesquisarem e apreenderem os objetos, documentos e comunicações, encontrem-se em suporte físico ou informático, já que se entende que estes existem e estão acessíveis independentemente da sua colaboração.

A questão põe-se, contudo, quando o acesso à pesquisa e à apreensão dos dados ou documentos informáticos é obstaculizado pela não revelação pelo arguido da palavra-passe do computador (ou outro qualquer sistema informático, tal como se encontra definido na alínea a) do artigo 2.º da Lei do Cibercrime). Entende-se, no entanto, que o interesse da questão nem chega a ser o de apurar da legitimidade do arguido em recusar a revelação da palavra-passe e com isso impedir o acesso a dados e documentos eventualmente incriminatórios. Na verdade, no limite, o que poderá estar em causa é o acesso por parte das autoridades judiciárias aos dados informáticos ser imediato ou diferido, já que a não colaboração do arguido apenas conduz à necessidade de apreender *o suporte onde está instalado o sistema ou onde estão armazenados os dados do computador*, que é uma das formas de executar a diligência de apreensão prevista no artigo 16.º da Lei do Cibercrime (em alternativa à cópia dos dados que pode ser imediatamente realizada na diligência e junta ao processo). Assim se conclui, portanto, que a recusa do arguido na revelação da palavra-passe não veda efetivamente o acesso aos dados informáticos, ao abrigo do *nemo tenetur*, apenas fazendo com que tenha que haver, mais tarde, um desbloqueio técnico da palavra-passe.

Por último, refira-se que já no que concerne à possível recusa do arguido, no decurso de uma diligência de pesquisa e apreensão de dados informáticos, em facultar o acesso a contas de correio eletrónico baseadas, não no computador, mas sim na Internet (*webmail*), a Lei do Cibercrime consagrou que a pesquisa se pode estender a «outros sistemas informáticos» ou a «partes diferentes do sistema pesquisado» (cfr. n.º 5 do artigo 15.º da Lei do Cibercrime). Neste caso (cfr. Pedro Verdelho, *Scientia Ivridica*, Tomo LVIII, N.º 320, Out.-Dez. 2009, p. 742), mesmo que o arguido se recuse a colaborar com a investigação, não revelando de sua vontade a palavra-passe destas contas de e-mail, o legislador legitimou as autoridades judiciárias a *intervir diretamente junto do servidor/alojador dessa conta*.

Rita Castanheira Neves e Hélder Santos Correia*

* Abogados del Área de Derecho Público, Procesal y Arbitraje de Uría Menéndez (Lisboa).