I Jornadas Nacionais sobre Violência de Género
Évora - "Tão felizes que nós fomos"
13.10.2016

Cibercrime e *Stalking*[1]

Vânia Costa Ramos
Advogada e Mestre em Ciências Jurídico-Criminais
Presidente do Forum Penal – Associação de Advogados Penalistas

A) Introdução

O tema que nos foi proposto tratar é o da cibercriminalidade e crime de perseguição, aquilo que é conhecido nos estudos criminológicos e também nas redes sociais e na opinião pública como *cyberstalking* ou – talvez pudéssemos dar um nome português deste tipo – "perseguição cibernética".

A nossa abordagem ao tema que nos foi proposto não será uma abordagem exaustiva ou aprofundada, mas antes uma primeira aproximação ao mesmo, uma vez que a matéria é uma matéria inteiramente nova.

Não só é recente o tipo de perseguição estabelecido no artigo 154º-A do Código Penal, introduzido pela Lei 83/2015, de 5 de Agosto, como é também recente e caracterizada por uma particular especificidade e complexidade a prática deste crime através dos meios tecnológicos ou de informação.

Tentaremos assim deixar aqui uma primeira panorâmica e algumas questões que se nos colocaram sobre esta matéria.

B) O que é o *cyberstalking*?

Em primeiro lugar, há que definir o que é o *cyberstalking* ou "perseguição cibernética".

Do ponto de vista criminológico ou criminógeno, não tanto olhando ainda para o tipo legal, poderá dizer-se que o *cyberstalking* é um desenvolvimento tecnológico do crime de *stalking* ou de perseguição tradicional.

Trata-se assim da utilização de comportamentos semelhantes aos do *stalking* tradicional:

[1] O presente texto, com ligeiras adaptações, corresponde à intervenção oral da autora, atualizada apenas até essa data, tendo sido mantido o estilo oral do discurso, bem como a ausência de referências bibliográficas ou notas de rodapé. Para qualquer questão ou comentário, contatar a autora através do endereço vaniacostaramos@carlospintodeabreu.com.

a) comportamentos que começam por ser até simpáticos ou sedutores, enfim, comportamentos perfeitamente normais e adequados do ponto de vista social e que a vítima, inicialmente, pode até consentir ou mesmo apreciar;
b) mas que rapidamente, em particular quando há uma rejeição, vão escalando até se tornarem numa perseguição, transformando-se em comportamentos de tipo obsessivo e que se caracterizam, de uma forma geral, pela aptidão que têm para incomodar, intimidar, causar medo e até, em alguns casos, causar grave dano psicológico (que muitas vezes tem implicações psicossomáticas e se torna em dano físico) nas vítimas;
c) em que os autores normalmente atuam com uma intenção de exercer o poder sobre o outro, de influenciar e controlar a vida do outro;

Sendo o *cyberstalking* no que respeita ao tipo de comportamentos semelhante ao *stalking* tradicional, parece-nos que deverá diferenciar-se deste pela *utilização total* dos meios cibernéticos, das tecnologias de informação.

Esta característica desde logo faz ressaltar uma diferença face ao *stalking* tradicional.

Com efeito, a utilização dos meios cibernéticos no *cyberstalking* é escolhida na maioria das vezes pela possibilidade que oferece de manter o anonimato, o que dificulta a identificação do autor.

Já o *stalker* tradicional, na maioria dos casos, é até uma pessoa com alguma relação com a vítima e que esta sabe quem é, pelo que a conduta não se baseia tanto na ocultação da identificação.

No *cyberstalking* (isto de acordo com a realidade norte-americana evidenciada em alguns estudos cujo grau de fiabilidade deve ser objecto de análise crítica), embora haja aparentemente uma grande percentagem dos agressores, talvez a rondar os 50%, que têm um qualquer tipo de relação ou de conhecimento com a vítima, há também uma grande parte em que se trata de pessoas totalmente desconhecidas.

Eles ou elas travam conhecimento com as vítimas *online*, em *chats*, redes sociais ou, enfim, pesquisando o perfil de alguém que lhes interessa e começam a estabelecer contactos que depois se tornam em conduta de perseguição ou assédio. Mas não são necessariamente alguém conhecido.

Esta diferente caracterização do fenómeno tem implicações não só para o estudo criminológico do mesmo, mas também para a reflexão sobre as formas adequadas de o combater, de o investigar e de prevenir.

Claro que o *stalking* tradicional pode ser acompanhado do envio de *e-mails* ou mensagens.

Porém, tal não o transfigura, pelo menos do ponto de vista criminológico, num crime de *cyberstalking*.

O próprio perfil do *cyberstalker*, segundo dados disponíveis em estudos norte-americanos (e que não são ainda dados muito sólidos para a compreensão deste tipo de crime), aproximar-se-á bastante mais do do criminoso de colarinho branco do que, como se diz no direito norte-americano, do de colarinho azul (expressão utilizada porque os colarinhos azuis eram os das fardas dos trabalhadores fabris, os industriais que tipicamente não teriam o colarinho branco).

O *cyberstalker* caracteriza-se em regra por estar integrado socialmente, pertencendo à classe média ou alta.

É alguém que, não sendo necessariamente um profissional, tem conhecimentos de informática bastante avançados.

Poderá ter por vezes algum historial de condutas antissociais ou perturbações de personalidade, mas pode não ter antecedentes criminais, até porque grande parte destas condutas ainda nem sequer estão ou estavam, à data da sua prática, tipificadas criminalmente.

Ainda no que se refere às diferenças face ao *stalking* tradicional, temos uma diferença que é evidente e que é comum a outros tipos de criminalidade informática: a distância geográfica que pode existir entre o autor do crime e a vítima.

Enquanto que no *stalking*, mais ou menos perto, haverá sempre uma proximidade geográfica maior entre a vítima e o agressor, o *cyberstalking* pode ser praticado a partir de qualquer lugar do mundo e com impacto em qualquer lugar do mundo.

Isto tem consequências muitíssimo importantes ao nível da investigação e punição deste tipo de condutas porque mesmo naqueles casos em que nós sabemos, teoricamente, ou suspeitamos de quem possa ser o *stalker* (nos casos em que há uma relação prévia entre a vítima e este e em que, portanto, esta acha que sabe quem é o *stalker*), dessa suspeita até se conseguir provar a identidade da pessoa, uma vez que estamos só a trabalhar com meios informáticos, o caminho é longo e tortuoso. Por vezes mesmo impossível.

Esta diferença revela a necessidade de olhar para este fenómeno do ponto de vista do direito penal e sobretudo do processo penal de forma diferente daquela como se olha para a forma tradicional do crime.

Na parte final falaremos sobre o instrumentário que a nossa lei processual tem, ou não tem, para investigar efetivamente este tipo de criminalidade.

Relativamente à perigosidade deste novo fenómeno – sem querer desvalorizar o *stalking* tradicional – este tipo de *stalking* tem uma potencialidade de impacto muito mais abrangente. Porquê?

Porque permite à pessoa esconder a identidade de forma relativamente fácil.

Não é preciso sermos profissionais para investigarmos um pouco na internet e descobrirmos formas de conseguirmos enviar e-*mails* sem poder ser determinado quem é o remetente (não só o endereço, mas o próprio IP físico do remetente). Não é preciso saber muito para conseguirmos fazê-lo.

Esta potencialidade para garantir o anonimato, aliada *i)* à quantidade informação pessoal que está hoje publicamente disponível na internet, *ii)* à informação que por vezes as próprias vítimas colocam *on-line* e ainda *iii)* à quantidade de empresas com fito lucrativo (relativamente às quais muitas vezes também se desconhece onde estão exatamente localizadas) que vendem dados pessoais que depois podem ser utilizados para este tipo de atuação torna o fenómeno do *cyberstalking* crescente e cada vez mais perigoso.

Por estes motivos, a repercussão do *cyberstalking* pode ter consequências bastante mais graves de futuro do que o *stalking* tradicional, pelo menos mais vastas, tornando premente a necessidade da sua prevenção.

Olhando para a perspectiva criminológica, na breve pesquisa que pudemos efetuar relativamente a Portugal, constatamos que não há ainda estudos criminológicos publicados na área do *cyberstalking*.

Foi-nos possível encontrar alguns dados em inquéritos criminológicos sobre o *stalking*, mas que não destacam especificamente o *cyberstalking* das formas tradicionais. Por este motivo, relativamente à prevalência do fenómeno em Portugal, não encontrámos dados muito fiáveis ou, pelo menos, já com uma profundidade que nos permitisse retirar aqui qualquer conclusão.

Ainda assim, decorre de alguns estudos da APAV a cujos resultados tivemos acesso e de notícias publicadas o relato de que as queixas de perseguição, em geral, já depois até da consagração legal do crime de perseguição no artigo 154.º-A do Código Penal têm vindo a aumentar. E dentro destas algumas referem-se a *stalking* com utilização de meios informáticos.

O "público-alvo" em Portugal, de acordo com esses inquéritos, embora o *stalking* e o *cyberstalking* possam evidentemente vitimizar qualquer pessoa, parecem ser as mulheres e, de entre estas, as mulheres jovens.

Enfim, é a caracterização que há até agora deste fenómeno.

Talvez a consagração legal tenha tido, pelo menos, a vantagem de tornar visível o facto de a conduta ser uma conduta merecedora de tutela penal. E, portanto, permitir às próprias vítimas perceberem que têm razão em queixar-se. E fazer com que as autoridades não desvalorizem este tipo de queixas.

Com efeito, conhecemos alguns casos de perseguição tradicional nos quais era muito difícil conseguir uma acusação pois as condutas de perseguição não passavam um determinado limite, portanto nunca entravam na ameaça com a prática de um crime grave ou nunca chegavam às ofensas à integridade física ou outros crimes que permitissem que a conduta fosse considerada criminal e levasse a uma acusação.

Por vezes as condutas eram até menorizadas, desvalorizadas pelas autoridades, por ocorrerem, por exemplo, entre vizinhos ou entre conhecidos ou por terem sido consentidas quando se iniciaram.

Parece-nos que esta é uma área onde se justificaria a realização de estudos específicos do fenómeno do *stalking*.

Por isso, deixamos aqui o repto a quem se interesse pela criminologia: fazem falta estudos sobre esta matéria. Estudos que caracterizem a prática do *stalking* com utilização de meios informáticos – qual a prevalência do *stalking* praticado exclusivamente com esses meios? Qual a prevalência do crime de *stalking* tradicional praticado não totalmente, mas também com auxílio dos meios informáticos? Qual a caracterização dos autores e vítimas? Há semelhanças ou diferenças relativamente ao *stalking* tradicional? Qual a percentagem de condutas onde foi impossível identificar o autor e porquê? Este crime é praticado isoladamente, ou em conjunto com outros crimes mais graves, tradicionais ou informáticos? E por aí fora...

C) A consagração do crime de *stalking* no Código Penal

O artigo 154.º-A do Código Penal, sob a epígrafe "perseguição", dispõe no seu n.º 1, que "[q]uem, de modo reiterado, perseguir ou assediar outra pessoa, por qualquer meio, direta ou indiretamente, de forma adequada a provocar-lhe medo ou inquietação ou a prejudicar a sua liberdade de determinação, é punido com pena de prisão até 3 anos

ou pena de multa, se pena mais grave não lhe couber por força de outra disposição legal".

A tentativa é punível.

Trata-se ainda de crime semipúblico, o que é compreensível, já que a vítima será a pessoa que está em melhor posição para decidir se pretende o processo penal com as consequências de vitimização secundária e todos os outros incómodos que dele advêm.

A consagração do crime de perseguição no nosso Código Penal foi influenciada, como todos saberão – dado até o mote destas Jornadas – pela Convenção de Istambul (Convenção do Conselho da Europa para a Prevenção e o Combate à Violência contra as Mulheres e a Violência Doméstica – STE n.º 210).

A Convenção de Istambul impõe no seu artigo 34.º aos Estados a tomada de medidas legislativas, ou outras, "necessárias para assegurar a criminalização da conduta intencional de ameaçar repetidamente outra pessoa, fazendo-a temer pela sua segurança" (http://www.apmj.pt/88-noticias/339-c-i)[2].

Atentando não só no texto da Convenção, mas no respetivo relatório explicativo, poderemos deles retirar alguns contributos para a interpretação do tipo como consagrado no nosso Código Penal.

A Convenção optou expressamente por configurar as obrigações de criminalização de uma forma neutra quanto ao género, embora não precluda os Estados de criarem disposições específicas de género.

No que se refere ao *stalking*, é de salientar que embora na forma simples consagrada no artigo 154.º-A do Código Penal não se refira a questão do género, a comissão do crime quando determinado por "ódio [...] gerado [....] pelo sexo, pela orientação sexual ou pela identidade de género da vítima" constitui forma agravada punida com pena de prisão de um a cinco anos nos termos do artigo 155.º, n.º 1, al. *e)*, do Código Penal, conjugado com o artigo 132.º, n.º 2, al. *f)*, do mesmo diploma.

Relativamente ao bem jurídico protegido, pensamos que é matéria que carece de alguma reflexão e que excede os limites desta comunicação.

Do ponto de vista sistemático, o crime enquadra-se no capítulo dos "*crimes contra a liberdade pessoal*". Há autores que sugerem estar aqui em causa o bem jurídico "paz pessoal", a segurança pessoal.

---

[2] A redação constante do Diário da República difere ligeiramente da tradução oficial do Conselho da Europa: "[...] necessárias para assegurar a criminalização da conduta de quem intencionalmente ameaçar repetidamente outra pessoa, levando-a a temer pela sua segurança" (*v.* http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1878&tabela=leis).

Esta referência recorda-nos um pouco o direito constitucional que os norte-americanos referem como o "*right to be let alone*", neste contexto em relação à intervenção do Estado. Aqui seria um "direito a ser deixado em paz" pelos outros, a ter o espaço de liberdade individual que permita a cada um de nós viver, fazer as suas escolhas e levar a vida como bem entender.

Outros autores referem a liberdade de decisão, de determinação como bem jurídico protegido. Em princípio, se a conduta de alguém, por exemplo, no meio onde essa pessoa vive, é restringida e condicionada pela atitude da pessoa que a persegue ou a assedia, parece-nos realmente que haverá um merecimento de tutela penal nessa vertente.

O relatório explicativo sublinha que a conduta tem de ser praticada de forma dolosa e com a intenção de causar na vítima uma sensação de temor (ponto 184), o que foi transposto para o Código Penal com a consagração de um crime doloso e de aptidão ou de perigo abstracto-concreto.

Ou seja, não é necessário provar que no caso concreto a conduta causou efetivamente medo ou inquietação, mas apenas que a conduta em causa era *apta a causar medo ou inquietação*.

Porém, de uma perspectiva mais prática, como sabemos, a prova, num processo concreto, de que a conduta causou de facto medo ou inquietação poderá ser determinante da prova da respetiva aptidão para causar tais sentimentos.

Parece-nos que para aferir se a conduta é apta a causar medo, deverá ser tomado como ponto de partida o "ser humano médio". Com efeito, poderão existir casos em que alguém é especialmente sensível (por razões que podem ser de índole variada) e por isso se deixa intimidar e afetar pela conduta de outrem que, em casos normais, poderá ser uma conduta desagradável mas que não merece tutela penal.

É que a vida é feita de contactos mais e menos agradáveis, mas que são todos próprios das relações humanas.

E não pode pretender-se, em nossa opinião, criminalizar todos os casos em que alguém se sinta afetado ou mesmo condicione a sua atitude por causa de uma conduta desagradável de outrem, só em razão da sua especial sensibilidade ou vulnerabilidade. ~

Isto não quer dizer que as características da vítima concreta sejam irrelevantes, mas não serão tanto as da pessoa em concreto, e já antes do "tipo de vítima" em causa – por exemplo, em razão da idade, do género, das circunstâncias relacionais entre vítima e autor, etc. Ou seja, o critério em causa é objetivo-individual.

A conduta, tendo em conta as circunstâncias concretas da situação e relação entre vítima e agressor, há-de ser vista objetivamente pela generalidade das pessoas como susceptível de causar medo ou inquietação.

De salientar que este elemento do tipo é idêntico ao elemento incluído no tipo do crime de ameaça previsto no artigo 153.º do Código Penal, pelo que a interpretação deste na jurisprudência e doutrina constituirá certamente um auxiliar importante para a interpretação do artigo 154.º-A.

O Código Penal pune a perseguição desde que praticada de modo reiterado, configurado assim como um crime de execução duradoura

O elemento de reiteração, é essencial para distinguir aquelas condutas lícitas das que, embora aparentemente lícitas ou inócuas, quando vistas de forma conjunta constituam um padrão de comportamento intimidatório ou ameaçador (ponto 185 do relatório explicativo).

A caracterização do *stalking* como conduta reiterada prende-se com a circunstância de muitos dos comportamentos fácticos que integram o crime de *stalking* serem comportamentos socialmente adequados.

Permanecer num local, só por si, por exemplo, não constitui qualquer crime. Imaginemos que alguém frequenta um café todos os dias, onde toma o seu café. A circunstância de o *stalker* ir todos os dias tomar o seu café naquele local, só por si, não é uma conduta que mereça tutela penal, é um comportamento socialmente adequado. E, portanto, este elemento da reiteração, conjugado com a intenção de causar medo na vítima, é um elemento que nos parece essencial neste tipo de crime de forma a configurar aquela presença como perseguição ou assédio.

O objeto da ação segundo o relatório explicativo da Convenção pode ser a própria vítima, ou podem ser pessoas do seu círculo próximo, cabendo aos Estados determinarem que modalidades criminalizar (ponto 185).

Por exemplo, em vez de perseguir ou assediar a própria vítima, o autor pode decidir, para inquietar ou causar medo àquela, perseguir os seus amigos, familiares ou pessoas próximas.

Em Portugal parece ter-se optado pela inclusão de ambas as modalidades, na parte em que o artigo 154.º-A refere que a perseguição ou assédio pode ter lugar direta ou indiretamente. Caberá à jurisprudência confirmar se o *stalking* indireto integra (ou não) a previsão do artigo 154.º-A no segmento "indiretamente", ou saber se este terá outro significado.

O Código Penal pune estas condutas praticadas por qualquer meio.

Trata-se, pois, de um crime de execução livre.

O legislador poderia ter incluído no tipo uma exemplificação das condutas que possam ser consideradas "perseguição" ou "assédio" utilizando a técnica dos exemplos-padrão, ou outra. Não o fez.

O que constitui, afinal, a conduta de "perseguir" ou "assediar"?

Partindo da própria definição das palavras em causa, o vocábulo "assediar" significa "perseguir com insistência", sinónimo de "importunar", "maçar", "molestar"; ou ainda "importunar com tentativas de contacto ou relacionamento sexual" ("assediar", in Dicionário Priberam da Língua Portuguesa [em linha], 2008-2013, https://www.priberam.pt/dlpo/assediar).

"Perseguir", por seu turno, significa "ir no encalço de"; "seguir ou procurar alguém por toda a parte com frequência, insistência e falta de oportunidade", sinónimo de "acossar" ou "importunar"; "procurar fazer mal a alguém", "tratar com violência ou agressividade", sinónimo de "atormentar", "fustigar" ou "molestar"; ou ainda "procurar ou incomodar com insistência" ("perseguir", in Dicionário Priberam da Língua Portuguesa [em linha], 2008-2013, https://www.priberam.pt/dlpo/assediar).

Neste ponto, poderá ser útil o recurso à Convenção de Istambul e ao seu relatório explicativo que nos dá exemplos deste tipo de condutas (ponto 182): seguir repetidamente outra pessoa, encetar comunicação indesejada com outra pessoa ou fazê-la sentir que está a ser observada. Isto poderá ser feito quer através do seguimento físico da vítima, aparecer no seu no local de trabalho, de educação ou prática desportiva.

Poderão ainda ser abrangidos pelo comportamento ameaçador previsto na Convenção comportamentos como vandalizar a propriedade de outrem, deixar marcas subtis de contacto com os objetos pessoais de outra pessoa, afetar os animais de estimação desta.

O legislador ao referir que a perseguição ou assédio podem ser levados a cabo "por qualquer meio" pretendeu ainda, a nosso ver incluir na previsão legal a perseguição e o assédio praticados por meios informáticos, seja como auxiliares da perseguição tradicional, seja como forma exclusiva da prática do crime e, portanto verdadeiros casos de *cyberstalking*.

Poder-se-ia discutir, ainda assim, se existe necessidade, ou não, de criminalização específica para a perseguição ou assédio cometidos por esses meios, parcial ou exclusivamente.

O relatório explicativo da Convenção de Istambul refere-se explicitamente a este tipo de comportamentos, elucidando que se inclui também na previsão da Convenção o seguimento da vítima no mundo virtual, seja em salas de *chat*, *sites* ou redes sociais.

O encetar contacto indesejado com a vítima é definido como a "procura de qualquer contacto ativo com a vítima através de quaisquer meios de comunicação disponíveis, incluindo as ferramentas modernas de comunicação e de TCIs".

Prevê-se ainda a difamação *online*: criar perfis sob o nome da pessoa onde é produzida informação falsa para prejudicar essa pessoa ou imputar a essa pessoa determinados comportamentos e fazê-lo através das redes sociais.

Da nossa prática, podemos dar alguns exemplos do que possa constituir o crime de perseguição, mas que são anteriores à consagração legal do mesmo.

Alguns deles, como tal, não deram origem a acusação. Outros deram, com base noutros tipos acabando ou com uma absolvição ou com uma condenação, designadamente pelo crime de ameaça.

Por exemplo, alguém que, por vingança ou por qualquer motivo, decide colocar um anúncio na internet, em jornais, etc., onde insere o nome e número de telefone de outra pessoa, afirmando que esta se encontra disponível para encontros sexuais, com uma determinada orientação ou preferência sexual. Conduta que leva a que a pessoa tenha que mudar de casa, por ter sido publicitada a sua morada e contactos para aquela finalidade e em consequência ser a toda a hora do dia e da noite incomodada por pessoas que lhe tocam à campainha ou batem à porta para procurar o tipo de contacto sexual que era oferecido naqueles meios de comunicação.

Ou por exemplo alguém que recorrentemente denuncia os seus vizinhos às autoridades por diversas alegadas infracções administrativas, fazendo com que estes sejam permanentemente sujeitos a fiscalização e como tal vejam a sua atividade laboral e vida pessoal absolutamente condicionada. E alguns que viriam a redundar, excecionalmente, em condenação, ao abrigo de outros tipo de crime, por exemplo em que o tribunal adoptou uma interpretação "generosa" do crime de ameaça, de forma a abranger condutas que em princípio não ultrapassariam aquilo que agora vem previsto no artigo 154.º-A.

A diversidade de comportamentos que podem integrar o crime de perseguição torna absolutamente relevante a parte final do tipo que dispõe que a conduta em causa é punível com pena de prisão até três anos "se pena mais grave não lhe couber por força de outra disposição legal".

Este segmento remete-nos para a problemática do concurso que, no caso deste crime, nos parece que será relevante num elevadíssimo número de casos.

Com efeito, o *stalking* é uma conduta duradoura e que tende, em muitos casos, a tornar-se mais grave com o decurso do tempo. O comportamento do *stalker* evoluirá amiúde para uma perseguição ou assédio cada vez mais intrusivos e que poderão, por isso, integrar outros tipos de crime.

Por exemplo, não tendo nós podido localizar jurisprudência sobre o crime do artigo 154.º-A, não deixámos de encontrar alguma jurisprudência, fundamentalmente sobre crimes de violência doméstica, em que já se referia o fenómeno do *stalking*.

E mesmo alguns casos que foram considerados *stalking*, mas enquadrados no tipo de violência doméstica ou no tipo do crime de ameaça.

Atualmente estes casos poderão ser casos que integram a previsão de ambos os crimes, mas em que, nos termos da parte final do artigo 154.º-A do Código Penal, estaremos perante casos de concurso aparente (na modalidade de subsidiariedade).

O mesmo poderá suceder relativamente a outros crimes em que a pena aplicável é mais grave.

A problemática do concurso não se esgota porém – de forma alguma – nestes casos.

Com efeito, colocar-se-á relativamente aos crimes de difamação e injúria, por exemplo, em que deverá considerar-se se poderão ser punidos em concurso efetivo com o crime de perseguição, se tal dependerá das circunstâncias concretas do caso, ou se há sempre uma relação de concurso aparente entre os mesmos.

Mas também, por exemplo, relativamente ao crime de ameaça (que é punido com pena inferior ao crime de perseguição!) e ao crime de coação (que é punido com pena idêntica ao crime de perseguição, mas que apenas é semipúblico em alguns casos).

Na perspetiva do *cyberstalking*, poderá colocar-se a questão do concurso com outros cibercrimes, por utilização por parte do *stalker* de meios mais intrusivos como o roubo de credenciais de acesso a redes sociais, ao *e-mail* e ao próprio computador e a possível instalação de *spyware* ou *malware* nos computadores da vítima que permite fazer uma monitorização digital da vida da própria vítima, consubstanciando uma intrusão muito grave na privacidade e que dá ao *cyberstalker* um enorme poder de constranger a vida da vítima.

A resposta a estas questões é importante, não só em termos substantivos, mas desde logo em termos processuais, já que o enquadramento em um ou outro crime

determina, muitas vezes, a aplicabilidade de diferentes pressupostos de procedibilidade, já que nuns casos se trata de crimes de natureza particular (em que terá de haver constituição como assistente no prazo de 10 dias a partir da notificação para o efeito nos termos do artigo 246.º, n.º 4, do Código de Processo Penal), noutros de crimes semipúblicos, que implicam a apresentação de queixa por parte dos titulares do direito respetivo, e finalmente, ainda noutros, de crimes públicos para os quais o Ministério Público tem legitimidade de prossecução independentemente da vontade da vítima.

Isto poderá, da perspetiva do advogado, levar a que este tenha de aconselhar a vítima a apresentar expressamente queixa e a constituir-se sempre como assistente *ab initio* para evitar que por falta de prova de algum elemento do tipo, ou por ter sido adotada pelo tribunal uma opção interpretativa quanto à questão do concurso que implique a alteração da natureza do crime, o caso venha a ser arquivado ou termine com absolvição por falta de um pressuposto processual.

D) Medidas de proteção

A Convenção refere um aspeto que nos parece deveras interessante considerar do ponto de vista mais amplo da política criminal: de acordo com a Convenção de Istambul devem também ser estabelecidos meios de tutela cível dos direitos das vítimas.

Aliás, a Convenção permite, quanto ao *stalking*, que os Estados decidam não punir criminalmente a conduta, desde que apliquem medidas proporcionais e dissuasoras de efeito equivalente, podendo apresentar uma reserva à Convenção nesse sentido, de acordo com o artigo 78.º, n.º 3, (como sucedeu com a Dinamarca e a Roménia). Portugal não apôs qualquer reserva à Convenção.

Os meios de tutela cível poderão ser particularmente úteis, quer como meios autónomos, quer no âmbito do próprio do processo penal.

É que, na prática, quando uma vítima de *stalking* procura um advogado, o Ministério Público, a polícia, enfim, as autoridades, o que a preocupa no imediato é pôr fim à perseguição da forma mais rápida possível.

Alguém que procura a justiça para se queixar de uma conduta destas é, normalmente, alguém cuja vida já está a ser condicionada pelo comportamento do *stalker* e que não raras vezes já se viu constrangida a mudar hábitos, mudar de trabalho, mudar de local de residência.

A vítima já foi e está a ser prejudicada e quer uma resposta efetiva e em tempo real das autoridades.

Se vem consultar um advogado vai perguntar: "Vamos apresentar queixa? E agora, o que vai acontecer? O que é que eu posso fazer se a pessoa continuar?".

Sucede que como o crime de *stalking*, pelo menos na forma simples, apenas é punido com pena até três anos de prisão.

Não é uma pena totalmente irrelevante, do ponto de vista da sua gravidade.

Porém, quando conjugamos essa pena com as medidas de coação previstas no Código de Processo Penal (e alguns meios mais intrusivos de recolha da prova que trataremos mais à frente), essa moldura penal cria barreiras à utilização de certos mecanismos processuais essenciais à proteção da vítima.

O primeiro deles é o da proibição de contactos – a medida de coação da proibição ou imposição de condutas, que pode passar por exemplo, pela proibição de contactos, exige que a conduta seja punível com pena superior a três anos de prisão (artigo 200.º do CPP). Portanto, não é aplicável ao crime de *stalking* na sua forma simples. E isto apesar de o tipo de crime prever uma possível pena acessória de proibição de contactos com a vítima...

Quanto à medida de coação de prisão preventiva até admitimos que se o *stalking* não tiver ultrapassado uma determinada barreira e não for enquadrável em qualquer dos outros tipos de crime mais graves que permitiriam a aplicação dessa medida de coação, isso possa ter sido uma opção intencional (e sensata) do legislador.

Porém, quanto à medida de afastamento ou de proibição de contactos não nos parece que a exclusão da respetiva aplicação tenha sido adequada (ou eventualmente sequer pretendida pelo legislador). Parece-nos que neste aspeto, como vem sendo apanágio do legislador, a reforma da parte substantiva no Código Penal não foi acompanhada de uma reforma na parte processual. E pensamos que o atual panorama legislativo deveria ser repensado e deveria ser prevista especificamente a possibilidade de aplicação dessa medida de coação para este tipo de crime.

Independentemente da medida de coação (até porque esta pode não ser o meio mais adequado e útil a prever esse tipo de perigos) poderia ter-se consagrado a possibilidade de aplicação medidas tutelares cíveis específicas que poderão até ser mais eficazes.

A própria Convenção refere no artigo 53.º que os Estados deverão adoptar medidas legislativas ou outras "necessárias para assegurar a disponibilidade de ordens de restrição ou proteção adequadas para as vítimas de todas as formas de violência" previstas na Convenção, incluindo portanto o caso do *stalking*.

Outro exemplo será o da tomada de ação imediata para por fim à conduta de perseguição ou assédio.

Por exemplo, se a vítima for perseguida por um *cyberstalker* que criou um *site* com uma falsa identidade em que a difama, a primeira coisa que a vítima pretende é que esse *site* seja bloqueado, que ele deixe de poder estar acessível. E que deixe de estar acessível não é só em Portugal, mas em todo o muno (porque é muito fácil a partir de um terminal localizado em Portugal – basta instalar o *TOR* – aceder a um *site* que está bloqueado em Portugal, mas não noutros Estados).

Certamente os meios cíveis gerais poderão enquadrar este tipo de pretensões, mas deve ponderar-se se estes meios são adequados e suficientes e se há ou não necessidade de referir especificamente a sua aplicabilidade aos casos de perseguição, ou mesmo se nestes casos os pressupostos de aplicação das medidas tutelares devem ser os mesmos ou se deverão revestir alguma especificidade (para um exemplo de aplicação destes meios tutelares, veja-se o acórdão do Tribunal da Relação de Lisboa de 27.10.2010, processo n.º 18645/10.9T2SNT.L1-2, disponível em www.dgsi.pt).

Parece-nos que estes aspetos carecem de alguma reflexão académica e forense e intervenção judiciária ou legislativa.

Talvez primeiro a reflexão, depois a intervenção, para que a intervenção seja mais eficaz.

E) Questões processuais

Conforme vimos já, as especificidades do fenómeno do *cyberstalking* levantam questões processuais particulares deste tipo de crime.

Na investigação do *cyberstalking* é sempre ponto crucial chegar à identificação do autor do crime. Primeiro problema: como estamos no mundo digital, temos que aceder aos dados da pessoa em causa, saber de onde é que vem determinado *e-mail* e qual é o IP que está associado a esse *e-mail*, ou a quem pertence um determinado perfil de utilizador, ou conta, ou qual é o IP associado.

Desde logo há casos em que nunca chegaremos a uma solução que nos permita identificar a pessoa, porque a pessoa usou meios que conseguem mascarar o IP e muitas vezes vão redundar a ordens jurídicas que não cooperam e, portanto, não vão fornecer a identificação pretendida.

Mas mesmo nos casos em que é possível identificar a pessoa ou pelo menos o IP em causa, há desde logo um problema que é a acessibilidade dos dados e a rapidez da sua obtenção.

A investigação da maioria destes crimes implica por definição que, imediatamente após a apresentação de queixa, sejam ordenadas e realizadas diligências de recolha de prova que vão implicar contactar os fornecedores de serviço para remeterem dados, pelo menos dados de base (identificação, morada, telefone, nome, etc.) associados a um determinado IP, a um determinado serviço de telecomunicações ou comunicação digital subscrito pela pessoa.

E, além destes, para remeterem dados de conteúdo (por exemplo, os *e-mails* armazenados nesses servidores e que foram enviados por essa pessoa e que poderão ter metadados úteis para a investigação) que estão sujeitos a um regime processual completamente diferente.

A primeira coisa que se pode fazer é, claro, notificar o servidor, o fornecedor de serviços para fornecer os dados de base. Problema: se o fornecedor de serviço não é português...

É que se alguns de nós poderão usar servidores ou *service providers* portugueses, a grande maioria dos internautas usa servidores ou *service providers* estrangeiros.

Focando-nos no *cyberstalking*, parece-nos forçoso concluir que, na maioria dos casos, os dados de que necessitamos vão estar armazenados no estrangeiro (ou não será possível saber até onde estão localizados).

Existem vários *service providers* que permitem o contacto direto das nossas autoridades para solicitar a obtenção de dados (existem algumas notas práticas elaboradas pelo gabinete de cibercrime da Procuradoria-Geral da República, que identificam as formalidades adotadas pelos *service providers*).

Por exemplo: a *Google*, a *Microsoft* ou o *Facebook* recebem milhares de centenas de milhares de pedidos deste tipo, de todo o mundo.

Portanto, essas próprias empresas, que evidentemente têm de prestar alguma colaboração com as autoridades, mas que também pretendem salvaguardar a privacidade dos seus utilizadores no âmbito dos contratos que com eles celebram, criaram formas de uniformizar os pedidos de acessos a dados.

Para quem investiga (mais até do que aos advogados, muito embora possamos evidentemente sugerir ou requerer tais diligências) é imprescindível conhecer esses procedimentos. Com efeito, basta seguir o procedimento errado para o pedido não

chegar em devida forma ou não ser respondido atempadamente e com isso verificar-se uma consequência drástica para a investigação: a eliminação dos dados que permitiriam identificar o autor do crime.

Se dentro da União Europeia há algumas normas que uniformizam mais ou menos o período de conservação dos dados, fora da União Europeia não há essa uniformização. Muitos dos *service providers* podem guardar a informação durante apenas três meses, por exemplo como sucede com os dados de uma determinada comunicação guardados pela *Google*. É, portanto, essencial apresentar queixa rapidamente e também que a investigação seja rápida na obtenção dos dados.

Dentro da União Europeia e dos países que subscreveram a Convenção Cibercrime do Conselho da Europa, naquilo que toca a tomar, não só medidas de recolha de prova, mas de cessação da atividade delituosa (por exemplo, desligar um site ou impedir certas conexões), existe a rede 24/7 e há meios mais rápidos de ação nesta matéria do que quando saímos do âmbito dos Estados signatários da Convenção Cibercrime onde é quase impossível à vítima conseguir resultados em tempo útil sem ter de recorrer diretamente aos serviços de um advogado ou das instâncias formais de controlo do país onde os dados se encontram.

Ora, evidentemente, nem todas as vítimas têm capacidade financeira para o fazer.

As dificuldades de acesso aos dados que permitem a identificação do *cyberstalker* e de acesso a medidas que possam interromper a atividade delituosa e as suas consequências agravam o potencial de risco.

É que, perante esta impossibilidade de fazer valer os seus direitos pelas vias legais formais, as vítimas tenderão a fazer justiça pelas próprias mãos, o que neste caso tem de ser feito em regra recorrendo aos serviços de terceiros "cibermercenários" conhecidos por "*ethical hackers*" – *hackers* que atuam em prol "do bem" e que muitas vezes proporcionam à vítima o único meio de obter os dados ou fazer cessar a atividade criminosa: contra-atacar com atividades informáticas tipificadas como ilícitas (que poderão, eventualmente, estar nestes casos a coberto de causas de exclusão da ilicitude).

Ainda no que se refere aos problemas processuais, como o crime de perseguição é punido na sua forma simples com pena de prisão até três anos, se observarmos o regime processual da Lei do Cibercrime (Lei 109/2009, de 15.09) logo encontraremos várias barreiras à investigação do *cyberstalking*.

Considerando o *cyberstalking* da forma que descrevi inicialmente, na sua forma pura em que não se trata de um *stalker* tradicional que envia alguns *e-mails* e SMS de vez

em quando, mas sim de um *stalker* que leva a cabo a perseguição *on-line* e usa a capa do anonimato que a internet torna facilmente acessível, deparamo-nos com três tipos de problemas. Um deles talvez possa ser resolvido por via de interpretação, os outros não.

Em primeiro lugar, no que se refere à utilização de meios ocultos de investigação. Para conseguir perceber quem é ou até para tentar localizar fisicamente o *stalker* é por vezes necessário monitorizá-lo ou encetar ações encobertas (físicas ou virtuais) para tentar fisicamente conduzir o *stalker* a um determinado local para se conseguir ligar a pessoa virtual à pessoa física. Quando podem ser usadas tais ações no domínio da cibercriminalidade?

No caso dos crimes previstos na Lei do Cibercrime e dos "crimes cometidos por meio de um sistema informático, quando lhes corresponda, em abstrato, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infracções económico-financeiras, bem como os crimes consagrados no título IV do Código do Direito de Autor e dos Direitos Conexos".

Isto conduz-nos à conclusão de que o *cyberstalking* quando não evolui para outro nível de criminalidade mais grave, que se enquadre noutro tipo de cibercrimes ou crimes clássicos, não está coberto por essa legislação. Portanto, a ação encoberta não é possível ser utilizada no *cyberstalking*.

Em segundo lugar, a própria monitorização dos *e-mails*, das telecomunicações em tempo real (seja por *Skype*, *Whatsapp* ou outras) pode ser monitorizada no âmbito da Lei do Cibercrime. Porém, a utilização de medidas de monitorização está sujeita (e bem) a um catálogo definido de crimes. Que crimes são esses?

Os crimes previstos na Lei do Cibercrime e os crimes "[c]ometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, quando tais crimes se encontrem previstos no artigo 187.º do Código de Processo Penal" (artigo 18.º).

O *stalking* ou o *cyberstalking* não estão aqui incluídos. O que parece um pouco absurdo, sobretudo tendo em conta que a utilização deste meio de obtenção de prova está prevista para os crimes de "injúria, de ameaça, de coação, de devassa da vida privada e perturbação da paz e do sossego, quando cometidos através de telefone".

Ora se já é discutível – mas talvez ainda possível – incluir por meio de interpretação no artigo 187.º outro tipo de comunicações que não o telefone, no segmento em que se refere o crime de injúria ou difamação cometida através de telefone (em particular quando estamos a aplicar aquela norma por remissão do artigo 18.º da Lei do Cibercrime), parece-nos vedada a conclusão de que ali se poderia incluir o crime de *stalking* ou *cyberstalking* como tipificado no artigo 154.º-A.

Com efeito, estamos a tratar de meios de obtenção de prova que contendem com direitos, liberdade e garantias e que estão sujeitos ao princípio da legalidade e que como tal não admitem aplicação analógica.

O terceiro problema – que é o que talvez possa ser resolvido por via de interpretação e que se aplica num contexto de outro tipo de recolha de prova digital – é a questão da apreensão do correio electrónico já recebido.

Por exemplo, *e-mails* que não estão em circulação, mensagens escritas ou comunicações que deixam rasto digital, mas que já estão guardadas num servidor do destinatário ou de um terceiro, mas que já foram acedidas.

Essas, nos termos da Lei do Cibercrime podem ser recolhidas por aplicação do regime de apreensão da correspondência previsto no Código de Processo Penal, para o qual remete o artigo 17.º da Lei do Cibercrime.

Quanto a esta remissão, a doutrina discute se a mesma inclui ou não a remissão para o limite também da pena aplicável de três anos constante do artigo 179º do Código do Processo Penal.

Há alguma divisão doutrinária no sentido de saber se a remissão da Lei do Cibercrime para o regime da correspondência inclui ou não este pressuposto. Se concluirmos que inclui, não é possível apreender *e-mails* recebidos para investigação do crime de *stalking* ou *cyberstalking*, o que, como em qualquer outro crime hoje em dia, mas em particular no caso do *cyberstalking*, evidentemente dificulta bastante a investigação do mesmo, já que é praticado exclusivamente com recurso a meios de comunicação digital.

Só para terminar, devemos confessar que ao pensarmos um pouco no *cyberstalking* ficámos algo perplexas com a impossibilidade de utilizar as medidas de investigação informática mais intrusivas para a investigação deste crime, sobretudo considerado na sua forma pura.

Claro que ainda há a necessidade de melhor estudo e caracterização criminológica deste fenómeno. Mas em princípio o *cyberstalking* é um crime, por natureza, cometido na internet e utilizando o anonimato que esta proporciona.

Ora, parece-nos que será difícil ou mesmo impossível investigar tal crime sem recurso a estas medidas de investigação mais intrusivas específicas para os cibercrimes. Qual seria a melhor forma de resolver este problema?

Parece-nos que talvez a mais simples seria a introdução de um tipo específico de *cyberstalking* na Lei do Cibercrime.

Com essa introdução – que nos parece adequada tendo em conta a fenomenologia do delito em causa – estes meios de obtenção de prova passariam a ser aplicáveis ao *cyberstalking* sem se cair no risco da tentação de alterar a medida da sanção aplicável ao crime do artigo 154.º-A apenas para permitir usar aqueles meios de obtenção de prova, o que nos parece pouco adequado face à medida da sanção prevista para outros crimes próximos, como os de ameaça ou de coação.

E também não se estenderia de forma genérica a aplicabilidade desses meios de obtenção de prova ao *stalking* tradicional, o que não parece justificar-se por este poder ser investigado com outros meios menos intrusivos.

Enfim, tudo questões que consideramos serem certamente merecedoras, pelo menos, de maior estudo e reflexão e, em alguns casos, de ação mais pronta e eficaz de todos os profissionais do foro e, no limite, de intervenção legislativa.