jurisprudência.pt

Tribunal da Relação de Guimarães
Processo nº 735/10.0GAPTL – A.G1

Relator: MARIA JOSÉ NOGUEIRA
Sessão: 29 Março 2011
Número: RG
Votação: UNANIMIDADE
Meio Processual: RECURSO PENAL
Decisão: CONCEDIDO PROVIMENTO

TELECOMUNICAÇÕES **CIBERCRIME** **CARTÃO DE TELEMÓVEL**

MENSAGENS SMS

Sumário

I - Tendo o Ministério Público determinado a pesquisa de dados informáticos supostamente guardados no telemóvel da denunciante, a apreensão das mensagens (SMS) ali encontradas deve ser autorizada pelo juiz de instrução - artigo 17º da Lei do Cibercrime (Lei n.º 109/2009, de 15/9).
II - A lei não estabelece qualquer distinção entre mensagens por abrir ou já abertas.

Texto Integral

Acordam em conferência os Juízes na Secção Criminal do Tribunal da Relação de Guimarães

I. Relatório

1. No âmbito do inquérito n.º 735/10.0GAPTL, que corre termos nos Serviços do Ministério Público de Ponte de Lima, nos quais se investiga a eventual prática de um ou mais crimes de coacção, p. e p. pelo artigo 154.º, n.º 1 do Código Penal, levados a cabo através de SMS`s do telemóvel da denunciada para o telemóvel da denunciante, efectuada, por determinação do Ministério Público, a transcrição das ditas mensagens, o Digno Magistrado titular do inquérito ordenou, invocando o disposto no artigo 17.º da Lei do Cibercrime, a apresentação do telemóvel da denunciante, juntamente com a referida transcrição, ao JI.

2. Perante o que o Mmº Juiz de Instrução proferiu o despacho que constitui fls. 7 a 14 dos presentes autos de recurso, no qual concluiu por não ocorrer motivo para a sua intervenção, considerando, assim, nada haver a determinar.

3. Inconformado com a decisão recorreu o Ministério Público, extraindo da respectiva motivação as seguintes conclusões:

1. A Lei do Cibercrime é aplicável aos autos ao abrigo das disposições conjugadas dos seus artigos 11.º, n.º 1, alíneas a) e b), e 2.º, alíneas a) e b).
2. No inquérito, o Ministério Público é a autoridade judiciária competente para ordenar a pesquisa de dados informáticos (sms`s) num sistema informático (telemóvel), nos termos do artigo 15.º, n.º 1, da Lei do Cibercrime.
3. A direcção do inquérito cabe ao Ministério Público e, nessa medida, é este quem tem de avaliar os elementos que se afiguram relevantes para a investigação de um crime.
4. Por esse motivo, é o Ministério Público quem deve tomar conhecimento, em primeira – mão, dos sms`s armazenados no telemóvel, decidindo quais (ou se algum) se afiguram úteis à produção de prova e interessam para a descoberta da verdade material.
5. Se se afigurarem úteis, o Ministério Público apreende provisoriamente os elementos que interessam e apresenta-os ao juiz para que este, se assim o entender, ordenar a apreensão definitiva dos mesmos, juntando-os aos autos, nos termos das disposições conjugadas dos artigos 17.º e 16.º, n.º 3, da Lei do Cibercrime.
6. O despacho do Ministério Público não é suficiente para conferir legalidade/ licitude à junção dos sms`s aos autos.
7. A intervenção do juiz é obrigatória, tal como dispõem os artigos 17.º e 16.º, n.º 3, da Lei do Cibercrime, e 179.º do Código de Processo penal.
8. A falta desta intervenção torna a prova recolhida no telemóvel nula, não podendo por isso ser utilizada, nos termos do artigo 126.º, n.º 3, do Código de Processo Penal.

Face ao exposto,

A decisão recorrida deverá ser substituída por outra que determine a competência do juiz de instrução para apreciar a apreensão provisória levada a cabo pelo Ministério Público, em ordem a ordenar (ou não) a junção aos autos da prova recolhida no telemóvel, nos termos das disposições conjugadas dos artigos 17.º e 16.º, n.º 3, da Lei do Cibercrime e 179.º, n.º 3, 2.ª parte, do

Código de Processo Penal.
Só assim farão V. Exas. a costumada JUSTIÇA!

4. Admitido o recurso, fixado o respectivo regime de subida e efeito, foram os autos remetidos a este tribunal.

5. Na Relação o Ilustre Procurador – Geral Adjunto, sufragando os argumentos expendidos em 1.ª instância pelo recorrente, emitiu parecer no sentido da procedência do recurso.

6. Realizado o exame preliminar e colhidos os vistos foram os autos à conferência, cumprindo, agora, decidir.

II. Fundamentação

1. Delimitação do objecto do recurso

De harmonia com o disposto no n.º 1 do artigo 412.º do CPP e conforme jurisprudência pacífica do Supremo Tribunal de Justiça o âmbito do recurso é delimitado em função do teor das conclusões extraídas pelo recorrente da respectiva motivação, só sendo lícito ao tribunal *ad quem* apreciar as questões desse modo sintetizadas sem prejuízo das que importe conhecer oficiosamente, como são os vícios previstos no artigo 410.º, n.º 2 do CPP, mesmo que o recurso se encontre limitado à matéria de direito – [cf. Acórdão do Plenário das Secções Criminais do STJ de 19.10.1995, DR, I – A Série, de 28.12.1995].
No presente caso trata-se de saber se, encontrando-se em curso, em fase de inquérito, investigação com vista a apurar da eventual prática de um ou mais crimes de coacção, a apreensão dos registos de mensagens SMS guardadas em suporte digital no telemóvel da denunciante – encontradas no decurso de pesquisa informática – carece, ou não, da intervenção do Juiz de instrução.

2. O despacho recorrido

É o seguinte o teor do despacho recorrido:

“ No caso dos autos, como se refere na douta promoção de fls. 4, investiga-se a prática de um crime de ameaça, p. e p. pelo art. 154.º, n.º 1, do Código Penal.

Na sequência da investigação em curso, veio o Ministério Público requerer a validação da apreensão das mensagens SMS, relevantes para a presente investigação, que fossem encontradas no telemóvel da ofendida, Lucília Lima, a operar com o n.º 968553461.

Depois de melhor compulsado e estudado o âmbito e regime da Lei n.º 109/2009, de 15 de Setembro, - designadamente no confronto com o regime previsto no art. 189.º do C.P.P. – é tempo de aprofundar a razão de ser e, com base nisso, o rigor operatório dos conceitos que, sobretudo a nível processual, o legislador decidiu utilizar na "criação" de alguns dos institutos probatórios que constam do Capítulo III da citada Lei (como forma de transpor para a ordem jurídica nacional a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro).

Mas vejamos:

§ 1. O art. 189.º, n.º 1, do Código de Processo Penal, na redacção que lhe foi conferida pela Lei 48/2007, de 29 de Agosto, prevê que:
"O disposto nos artigos 187.º e 188.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à intercepção das comunicações entre presentes".

Com a reforma de 2007, o legislador manteve a intenção (que já vinha do direito pretérito, de abranger pelo âmbito da protecção do regime das escutas telefónicas qualquer forma de comunicação que implique a transmissão de dados por via telemática (aparecendo aqui, profundamente descontextualizada a comunicação entre presentes).

Contudo, nesta nova redacção do citado preceito, faz-se expressa menção à intenção de abranger no predito regime o conteúdo das transmissões "*mesmo que se encontrem guardadas em suporte digital*" (na senda, segundo parece, do entendimento perfilhado pelo Ac. do STJ de 20/09/2006, *in* CJ, XIV, t. 3, p. 189).

Entendem, por isso, os autores (cfr. Paulo Dá Mesquita, in Processo Penal, Prova e Sistema Judiciário, fls. 91/92, citando ainda Pedro Verdelho e Paulo Pinto de Albuquerque) que o legislador, com o dito acrescento, pretendeu ampliar o âmbito de tutela do regime das escutas às situações em que, mesmo

depois de cessado o estrito acto comunicacional (isto é, o envio electrónico), o produto desse acto, isto é, os dados (informáticos) recebidos, lidos e armazenados no suporte digital, já se tenha autonomizado do acto comunicacional propriamente dito.
Dizendo-se de outro modo, e reportando-nos directamente ao caso em apreço, quer a mensagem esteja a ser recebida ou não, quer já tenha sido lida ou não, i.e. mesmo depois de recebida, lida e guardada, a sua utilização probatória só pode ser feita se autorizada pelo juiz. (Neste mesmo sentido, cfr. Costa Andrade, no estudo designado "Bruscamente no verão passado", a reforma do Código de Processo Penal – Observações criticas sobre uma lei que podia e devia ter sido diferente, in RLJ, ano 137º, n.º 3950 e 3951, pp. 353/354. Este autor, depois de dar conta do erro crasso da formulação normativa, aventando a possibilidade de se proceder a uma interpretação restritiva (ou correctiva, o que vai dar ao mesmo) da dita norma logo destaca que *"não pode, na verdade, esquecer-se que uma interpretação restritiva com este sentido e alcance [i.e., de sorte a afastar a aplicação do regime das escutas aos documentos vertidos em suporte digital] configura uma verdadeira redução teleológica in malam partem. Sendo, como tal, constitucionalmente insustentável".*

§ 2. Volvendo ao caso dos autos, o problema que importa solucionar é o de aferir qual o regime legal que importa aplicar às mensagens *SMS* guardadas num telemóvel, que no caso é da ofendida, a fim de, a partir desse regime, se extrair as necessárias consequências (desde logo se tal prova (ou, melhor dito, o meio de obtenção) está sujeita à chamada *reserva de juiz* e, estando, em que contornos deve ser apreciado).

§ 2.1. Partindo do problema assim formulado, logo surpreende a chamada de atenção do Professor Costa Andrade (ob. cit. p. 338 e ss.) para a separação de águas que deve ser feita entre o *direito fundamental da inviolabilidade das comunicações*, que visa "*assegurar o livre desenvolvimento da personalidade de cada um através da troca, à distância, de informações, notícias, pensamentos, opiniões, à margem da devassa da publicidade*", e outros direitos, v.g., reserva da vida privada, palavra, imagem, etc., que merecem diferentes formas de tutela (processual).
Na verdade, como salienta o eminente Professor, a eventual supressão daquele direito fundamental (da inviolabilidade das telecomunicações) – supressão sujeita a óbvia reserva de lei (fazendo assim depender a validade da prova da verificação dos pressupostos substanciais da admissão do meio de obtenção e do cumprimento das regras de produção) – com as finalidades de investigação legalmente consagradas, prende-se, tão só, com a alteração do controlo ou

domínio do canal utilizado para o acto comunicacional. Quer dizer, em causa está a possibilidade de intromissão nas comunicações, a qual se encontra subtraída aos comunicadores, podendo essa intromissão dizer respeito quer ao conteúdo da telecomunicação, quer às circunstâncias atinentes à telecomunicação.
De fora desta tutela (que será feita noutro lugar) fica, por exemplo, a confiança na reserva e confidencialidade do outro interlocutor, nas situações em que, à revelia de um dos comunicadores, o outro permite que terceiro ouça a conversa.
De fora desta tutela (mas também assegurada por outra via) fica, ainda, os conteúdos e as circunstâncias da comunicação guardados na área de domínio do participante da comunicação (como referido pelo Tribunal Constitucional Alemão e citado pelo Prof. Costa Andrade, ob. cit., p. 339).

Na verdade, a tutela e/ou violação da inviolabilidade das telecomunicações só existe enquanto dura o processo dinâmico de transmissão, cessando esta tutela no momento em que a tal inviolabilidade entra na guarda *exclusiva* do destinatário (não mais podendo ser acedida pelo terceiro que tem o domínio sobre o canal ou meio de comunicação).

Concluí, então, o autor que vimos de acompanhar "*assim, depois de recebido, lido e guardado no computador do destinatário, um e-mail deixa de pertencer á área de tutela das comunicações, passando a valer como um normal escrito. E, como tal, sujeito ao mesmo regime em que se encontra um qualquer ficheiro produzido pelo utilizador do computador e nele arquivado. Podendo, como tal, figurar como objecto idóneo da busca, em sentido tradicional. Busca que pode ser executada já sob a forma de apreensão do computador, já (…) sob a forma de cópia. O mesmo valendo para a informação (conteúdos e dados de comunicação) guardado no cartão SIM de um telemóvel e relativa a conversações ou mensagens (v.g. SMS) expedidas e recebidas*" (p. 339/340).
De resto, acrescenta elucidativamente este autor, com relevância para o acertamento do regime a aplicar, que "*as intromissões que não atinjam o direito fundamental da inviolabilidade das telecomunicações não são abrangidas pelas normas que autorizam intromissões precisamente nas telecomunicações*".
Apenas uma nota para referir que, o que acaba de ser dito para o direito à inviolabilidade das comunicações vale, em toda a linha, para o direito fundamental à inviolabilidade da correspondência (apenas sendo os métodos de violação permitidos diversos).

§ 3. A par do direito à inviolabilidade das telecomunicações – mas sendo diverso deste – tem a doutrina e a jurisprudência vindo a decantar (na feliz expressão do Professor Costa Andrade) um outro direito fundamental, atinente à integridade e confidencialidade dos sistemas informáticos (ob. cit., p. 344).

Trata-se (reitera-se) de um novo tópico, que se distingue perfeitamente da questão das telecomunicações (ainda que com ele tenha várias zonas de contacto), e que, segundo percebemos, é o campo regulado pela Lei do Cibercrime (Lei n.º 109/2009, de 15 de Setembro).

Desligamo-nos, pois, das questões atinentes às intercepções das telecomunicações (através das escutas e quejandos) e da correspondência, para nos centrarmos (aqui no âmbito processual, que é o que nos interessa) na questão do sistema informático e dos dados informáticos que por aquele circulam e ali se encontram preservados.

Na verdade, e volvendo ao que já referimos, agora se compreende por que razão a formulação do art. 189.º, n.º 1, do C.P.P., que se insere no capítulo relativo às "escutas telefónicas", é infeliz na medida em que se reporta ao acesso a documentos guardados *ainda que os mesmos derivem de comunicações*.

É que os ditos documentos nada têm que ver com a intromissão nas telecomunicações (pois que a comunicação se iniciou, processou e finalizou, em princípio, sem qualquer intercepção ou intromissão de outra natureza). Antes, o que se pretende é aceder a um documento (pois que é isso de que se trata, quando se fala de dados informáticos subsumíveis á categoria de SMS), que se encontra guardado *digitalmente*, ou seja, num sistema informático (no caso, um sistema composto por hardware, a parte física do telemóvel, e software, o programa informático que descodifica os sinais em que se encontram armazenados directamente na "memória" do telemóvel ou virtualmente na rede a que acede o cartão SIM).

É certo que a tal mensagem (SMS) começou por ser o produto de um acto comunicacional, como a carta que se remete a alguém é destinado à realização de um acto comunicacional. Contudo, como refere, o Professor Costa Andrade, "bem podendo acontecer (…) que certos dados, que começaram por nascer como "coisas" da telecomunicação, percam, a partir de certo momento, de certas vicissitudes da sua trajectória, a natureza de dados pertinentes às telecomunicações. E, nessa medida, deixem de estar à sombra

da sua área de tutela. E passem a relevar no contexto e sob o regime de outros, contíguos e concorrentes direitos fundamentais" (p. 338).

§ 4. Volvendo ao caso dos SMS de que se ocupam os presentes autos, são várias as razões que nos levam a apartar a aplicação do regime aplicável à intromissão das telecomunicações.

Na verdade, no caso dos autos não se pretende lançar mão de um qualquer método oculto de investigação, à semelhança do que se passa com a apreensão da correspondência (na medida em que há uma *intromissão no processo de acção/interacção* dos concretos visados, que se produz no *decurso do dito processo, à revelia do visado* e a que este só tem acesso depois dos efeitos da intromissão, de sorte a dita *transformação* produzida pela dita apreensão altera a realidade fáctica de forma irremediável, quer dizer, depois de apreendida a correspondência ficou afectada a relação comunicacional) ou a intercepção das comunicações electrónicas (cfr. art. 17.º e 18.º da Lei do Cibercrime).
Se na utilização de tais métodos faz sentido que a Lei reclame uma tutela preventiva do juiz, na medida em que as pessoas atingidas não podem actualizar qualquer pretensão de reacção e tutela, no que se trata da *apreensão* de uma mensagem *SMS* é de fazer juntar ao processo um documento (um conjunto de dados, se se quiser, que exprimem uma ou mais declarações) que pode ser posto em causa pelo visado (mais cedo ou mais tarde), atentas as características do próprio documento e a (até maior) garantia de fidedignidade do mesmo. Não há aqui qualquer intromissão no processo comunicacional, na medida em que se mostra cristalizada a prova (documental).

Neste sentido, vinha a maioria da jurisprudência, ainda que fazendo uma interpretação *contra legem* do disposto no art. 189.º, n.º 1, do C.P.P. (advindo da reforma de 2007), defendendo que "*a mensagem mantida em suporte digital, depois de recebida e lida, tem a mesma protecção da carta em papel que, tendo sido recebida pelo correio e aberta, foi guardada em arquivo pessoal*" (assim é o sumário do Ac. da Rel. de Guimarães de 12/10/2009, proc. n.º 1396/08.1PBGMR – A.G1; no mesmo sentido, Ac. da Rel. do Porto, de 27/01/2010, proc. n.º 896/07.5JAPRT.P1; ainda na vigência da norma na redacção anterior à reforma de 2007, cfr. Acs. da Rel. de Coimbra, de 29/03/2006, proc. n.º 607/06; da Rel. de Lisboa de 20/03/2007, proc. n.º 7189/2006 – 7, e de 15/07/2008, proc. n.º 3453/2008 – 5).

§ 5. Se bem que, antes da publicação da Lei n.º 109/2009, de 15 de Setembro, a interpretação deixada de referir seja de duvidosa constitucionalidade, como adverte o Professor Costa Andrade, afigura-se-nos que presentemente é essa a única e plausível interpretação depois de publicada a Lei do Cibercrime.

Concordando-se com Paulo dá Mesquita (ob. cit., pp. 100/111), a referida Lei do Cibercrime veio, de facto, alterar indelevelmente o direito probatório, na medida em que se propôs a estabelecer um conjunto de regras gerais (de processo penal) sobre meios de obtenção de prova no domínio dos *sistemas informáticos* (por referência ao direito fundamental deixado de referir supra; Paulo Dá Mesquita chama-lhe, todavia, prova electrónica).

Como se diz neste último estudo citado, a recolha de prova em suporte electrónico, tal como prevista no capítulo III da citada Lei do Cibercrime, aplica-se na investigação de um universo irrestrito de crimes.
Na verdade, dispõe o art. 11.º, n.º 1, da citada Lei, sob a epígrafe "Âmbito de aplicação das disposições processuais", que "*com excepção do disposto nos artigos 18.º e 19.º, as disposições processuais previstas no presente capítulo aplicam-se a processos relativos a crimes: … c) Em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico".*

Ora, e aderindo-se na generalidade à posição de Paulo Dá Mesquita no que concerne aos fundamentos da "revogação parcial do art. 189.º, n.º 1, do Código de Processo Penal" (ob. cit., pp. 106/108), verifica-se que, efectivamente, o disposto no art. 189.º, n.º 1, do C.P.P. deve ser afastado não só no que tange à questão das intercepções das comunicações (cfr. art. 18.º, n.º 4, da Lei do Cibercrime), mas especificamente (e por maioria de razão) no segmento concernente ao produto das comunicações (já concluídas) que se encontrem guardadas em suporte digital, como decorre expressamente do citado art. 11.º, n.º 1, al. c), da mesma Lei.

De facto, pressupondo que no regime em causa foi equacionada, em termos de proporcionalidade (em sentido amplo), a danosidade e perniciosidade dos meios de obtenção de prova em causa (nos termos em que se vêm descrevendo), não há qualquer razão para que se não possa aplicar directamente às mensagens SMS, de forma directa e imediata, o regime das buscas e apreensões tal como regulado nos arts. 15.º e 16.º da Lei do Cibercrime.

§ 6. Dito isto, e face ao que *supra* se deixou referido, designadamente no que

contende à inaplicabilidade do disposto no art. 17.º da Lei do Cibercrime (uma vez que se não está perante uma qualquer comunicação em curso, nem sequer a mensagem passa pelo domínio de um terceiro fornecedor de serviços de telecomunicações/*provider*), por uma banda, bem assim como à revogação do art. 189.º, n.º 1, do C.P.P. (caso em que a intervenção do juiz deveria, aliás, ser preliminar à pesquisa), por outra, afigura-se-nos não existir razão para a intervenção, neste caso, do juiz de instrução.
Efectivamente, como se colhe do disposto no art. 16.º, n.º 1 e 4, da Lei do Cibercrime, a apreensão é da competência do Ministério Público, pelo que nada há a determinar.
Notifique".

3. Apreciando

Em consonância com o que deixamos expresso em sede de delimitação do objecto do recurso, nos presentes autos cuida-se de saber se, encontrando-se em curso, em fase de inquérito, investigação com vista a apurar da eventual prática de um ou mais crimes de coacção, a apreensão dos registos de mensagens SMS guardadas em suporte digital no telemóvel da denunciante – encontradas no decurso de pesquisa informática – carece, ou não, da intervenção do Juiz de instrução.

Numa análise mais detalhada passemos em revista a "cronologia dos acontecimentos".

a) Na origem do inquérito [instaurado em 29.09.2010] encontra-se a denúncia apresentada, além de outro, por Lucília Lima, imputando à denunciada factos susceptíveis de integrarem [de acordo com o titular da investigação] a prática do crime de coacção, p. e p. pelo artigo 154.º, n.º 1 do Código Penal, levados a cabo por intermédio de duas mensagens SMS, enviadas [ambas em 29.03.2010] do telemóvel desta para o seu;
b) Em face do que o Ilustre Magistrado do Ministério Público determinou a realização de pesquisa ao telemóvel pertença da denunciante, com a apreensão de todos os dados informáticos relevantes para a investigação, tudo nos termos dos artigos 15.º, 16.º, n.º 7, al. b) e 17.º da Lei do Cibercrime [Lei n.º 109/2009, de 15.09], não obstante, ter ainda ordenado que se diligenciasse no sentido de colher a autorização a que alude o artigo 15.º, n.º 3, al. a) da citada Lei e, finalmente, que uma vez efectuada a transcrição, caso se viesse a confirmar a existência das mensagens, fosse o telemóvel conservado para apresentação, juntamente com a mesma, ao JI nos termos do disposto no

artigo 17.º da Lei do Cibercrime – [cf. despacho de fls. 4];
c) Em cumprimento de tal despacho foi lavrado [em 17.11.2010] o Auto de transcrição das mensagens, com a identificação da data e hora a que foram emitidas, bem como do telemóvel de emissão - [cf. fls. 5].

É, pois, este o contexto em que surge o despacho recorrido.

Se bem se alcança da decisão em crise o Mm.º Juiz, não questionando a aplicação, ao caso, da Lei do Cibercrime [Lei n.º 109/2009, de 15.09, em vigor desde 15.10.2009 – cf. artigo 32.º], entende, à luz do disposto no seu artigo 16.º, n.ºs 1 e 4, que a apreensão é da competência do Ministério Público, não sendo de convocar o artigo 17.º uma vez que não se estaria perante "uma qualquer comunicação em curso, nem sequer a mensagem passa pelo domínio de um terceiro fornecedor de serviços de telecomunicações/provider".

Uma breve observação para referir que em face do artigo 11.º da Lei n.º 109/2009, no qual vem definido o âmbito material de aplicação das disposições processuais nela incluídas, sobretudo se lido em conjugação com o artigo 14.º da Convenção sobre o Cibercrime adoptada em Budapeste em 23.11.2001 [aprovada pela Resolução da Assembleia da República n.º 88/2009 e ratificada, em 29.08, pelo Decreto do Presidente da República n.º 91/2009], cujo teor, no essencial, reproduz para o direito interno, não nos suscita dúvida de maior a aplicação da Lei do Cibercrime, desde logo por estar em causa a apreensão de dados informáticos (SMS) num sistema informático (telemóvel) – [cf. artigo 2.º, als. a) e b) da LC].
No mesmo sentido pronuncia-se Paulo Dá Mesquita, evidenciando, embora, a redacção equívoca da exposição de motivos da proposta de lei, referindo *"O carácter pernicioso do enquadramento sistemático das referidas regras processuais e os equívocos que o mesmo pode gerar são, aliás, ilustrados por enganos verificados na própria exposição de motivos onde, a par da correcta delimitação do âmbito do direito processual consagrado no diploma, em certos trechos se indiciam perspectivas restritivas que não correspondem nem ao normativo do texto, nem à obrigação do Estado português decorrente da ratificação da Convenção."* – [cf. "Processo Penal, Prova e Sistema Judiciário", Coimbra Editora, págs. 99/100].
E a idêntica conclusão chega Pedro Verdelho quando, reportando-se às normas processuais incluídas na LC, escreve "*Estas últimas têm como óbvio intuito virem a ser aplicadas a investigações em que estejam em causa infracções criminais previstas na própria lei. Porém, além desta óbvia declaração de aplicabilidade, o art. 11.º estende o regime processual da lei do Cibercrime a*

dois segmentos de criminalidade cuja investigação, na prática, somente será viável se puderem ser utilizados meios de prova especiais, como os utilizados na investigação da cibercriminalidade, independentemente de tais meios de prova poderem ou não, de acordo com as normas gerais do Código de Processo Penal, ser usados. Trata-se dos crimes cometidos por meio de um sistema informático e dos crimes cuja prova esteja guardada em suportes digitais. Portanto, em ambos os casos previstos passa a ser possível recorrer aos novos instrumentos processuais descritos na Lei do Cibercrime." – [cf. A nova Lei do Cibercrime, *in* "SCIENTIA IVRIDICA", REVISTA DE DIREITO COMPARADO PORTUGUÊS e BRASILEIRO, OUTUBRO – DEZEMBRO 2009, TOMO LVIII, n.º 320, págs. 733/734].

Dito isto, vejamos, então, as disposições legais pertinentes.

Nos termos do artigo 15.º da LC, sob a epígrafe *Pesquisa de dados informáticos*: "1. *Quando no decurso do processo se tornar necessária à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência*".

Por seu turno, sobre a *Apreensão de dados informáticos*, dispõe o artigo 16.º do citado diploma:
"1. *Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a apreensão dos mesmos.*
(…)
3. Caso sejam apreendidos dados ou documentos informáticos cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular ou de terceiro, sob pena de nulidade esses dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto."
(…)".

Por fim, sob a epígrafe *Apreensão de correio electrónico e registos de comunicações de natureza semelhante*, prescreve o artigo 17.º:
"*Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a*

um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurarem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal."

Retomando a situação em apreço constata-se que, em face dos termos da denúncia, o Ministério Público, determinou a pesquisa de dados informáticos supostamente guardados no telemóvel da denunciante, ordenando, em simultâneo, para o caso dos mesmos virem a ser efectivamente encontrados, a respectiva apreensão e, uma vez efectuada a transcrição, resultando confirmada a existência das mensagens, a conservação do telemóvel para apresentação, juntamente com a mesma, ao JI, nos termos do disposto no artigo 17.º da LC.
Da análise que fazemos do despacho recorrido não resulta estar em causa a aplicação feita dos artigos 15.º e 16.º da LC, relativamente aos quais, julga-se, não suscitar dúvida que a pesquisa e apreensão, assim, determinadas, são da competência da autoridade judiciária que preside em cada fase do processo, ou seja durante o inquérito encontra-se a mesma deferida ao Ministério Público.
Contudo, o conhecimento dos dados informáticos obtidos no decurso de tais diligências nem sempre dispensam a autorização judicial, como o demonstra o n.º 3 do artigo 16.º e o artigo 17.º da Lei do Cibercrime.
No primeiro preceito, incluem-se "*os dados ou documentos informáticos cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular ou de terceiro*", os quais, uma vez apreendidos, no âmbito de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, tem de ser apresentados, sob pena de nulidade, ao juiz, com vista à ponderação, tendo em conta os interesses concretos em causa, sobre a sua junção aos autos.
A propósito de tal opção refere Paulo Dá Mesquita que "*aparentemente, visará dar expressão normativa ao Ac. n.º 607/2003, do Tribunal Constitucional no domínio dos dados íntimos em suporte digital*", observando, não obstante, que caso "*o preceito corresponda a uma simples consagração legal do acórdão …, ressalta a incapacidade de traçar uma previsão equivalente à dimensão do referido aresto, diários íntimos*", prosseguindo no sentido de que se "*o art. 16.º, n.º 3, tivesse uma ambição mais vasta de constituir expressão de uma*

teoria geral sobre a protecção da privacidade no quadro da admissão da prova em suporte digital o problema seria mais vasto" por força de factores que de seguida evidencia, concluindo que as "*Dimensões problemáticas suscitas pela infelicidade legislativa que não podem ser justificadas pela eventual especificidade da prova electrónica, já que … se centram no conteúdo da comunicação, matéria que exige um tratamento global da prova documental independentemente do suporte."* – [cf. ob. cit. págs. 116/117].
No segundo normativo inscrevem-se as mensagens de correio electrónico ou registos de comunicações de natureza semelhante, encontrados, no decurso de pesquisa informática ou outro acesso legítimo a um sistema informático, neste armazenados, caso em que o juiz "*pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal."*

No fundo, é a necessidade, ou não, de convocar, no caso, este artigo 17.º que constitui o ponto de discórdia entre o recorrente e o decisor.
Em abono da posição por si sufragada o Mm.º Juiz chama à colação, entre outros, os ensinamentos do insigne Professor Manuel da Costa Andrade a propósito da disciplina das intercepções telefónicas resultante da reforma de 2007 ao Código de Processo Penal, particularmente da redacção introduzida no artigo 189.º, cuja visão critica resulta, sem margem de dúvida, da obra citada – [cf. "Bruscamente no Verão Passado" a reforma do Código de Processo Penal, Observações críticas sobre uma Lei que podia e devia ter sido diferente", vg. págs. 185 e ss.].
Mas não só! Com efeito, parece estribar, ainda, a solução preconizada na posição de Paulo Dá Mesquita enquanto refere *"No art. 17.º, apesar da redacção pouco clara, a remissão para as regras do processo penal sobre apreensão de correspondência parece implicar que a mesma reconduz o intérprete à teleologia do regime processual sobre apreensão de correspondência, pelo que não são objecto da sua tutela especial, nomeadamente, mensagens de correio electrónico já acedidas pelo destinatário."* – [cf. ob. cit., pág. 118].
Na nossa perspectiva, modesta, embora, não obstante a posição que vem sendo defendida pelos ilustres autores, maioritariamente sufragada na jurisprudência, mesmo após as alterações introduzidas pela reforma de 2007, mormente no artigo 189.º, n.º 1 do Código de Processo Penal – [cf. os acórdãos da RC 29.03.2006, proc. n.º 607/06; RL de 20.03.2007, proc. n.º 7189/2006 – 7; RL 15.7.2008, proc. n.º 3453/2008 – 5; RG de 12.10.2009, proc. n.º

1396/08.1PBGMR-A.G1; RP de 27.1.2010, proc. 896/07.5JAPRT.P1; em sentido divergente *vd*. os acórdãos do STJ de 20.09.2006, *in* CJ, ASTJ, Ano XIV, T. III, págs. 189 e ss. e da RL de 24.042009, proc. n.º 158/2009, *in* www.pgdlisboa.pt] – não vislumbramos à luz do direito constituído – [cf. n.º 1 do citado artigo 189.º do CPP e artigo 17.º da Lei do Cibercrime], lastro para semelhante interpretação.
Apesar de proferido na sequência das alterações ao Código de Processo Penal, operadas pela reforma de 2007, relembramos o ensinamento da Professora Fernanda Palma quando refere "*Não há dúvida de que a SMS é uma comunicação análoga ao telefonema de viva voz e que coloca, por isso, idênticas exigências de tutela de reserva da vida privada. A reforma do processo penal reconheceu-o, ao submeter o correio electrónico e outras formas de transmissão telemática de dados ao regime restrito das escutas telefónicas*", sendo que relativamente às mensagens de texto ou de voz que já foram abertas (e lidas ou ouvidas) pelo destinatário acrescenta *"…o artigo 189.º, n.º 1 do Código de Processo Penal, continua a aplicar o regime das escutas às mensagens que já estão guardadas em suporte digital, equiparando-as, assim, às conversações em curso"* – [cf. "Crimes confidencias", Correio da Manhã, de 24.08.2008, disponível in www.cmjornal.xl.pt; no mesmo sentido vd. Natália Lima, "Escutas telefónicas e reconhecimentos de pessoas", in http://penal2trabalhos.blogspot.com.].

Também no artigo 17.º da Lei do Cibercrime, não vem estabelecida qualquer distinção entre mensagens de correio electrónico e/ou registos de comunicações de natureza semelhante, armazenados em sistema informático, já acedidas, ou não, pelo respectivo destinatário; entre mensagens a abrir ou já abertas, tão pouco entre comunicações e mero arquivo informático, sendo que não podia o legislador ignorar a polémica a propósito instalada, potenciada pela reforma de 2007 do Código de Processo Penal.
E se a vontade de mudança constitui realidade incontornável à face da dita reforma - [cf. Paulo Dá Mesquita, quando refere *"Referência no art. 189.º, n.º 1, do CPP às comunicações guardadas em suporte digital que, na nossa leitura, revela uma inequívoca intenção de que a cessação do acto de envio electrónico (relativo a escrito, som e/ou imagem) não corresponda ao fim do âmbito de tutela extensiva do regime das escutas, nomeadamente a exigência de integração num crime de catálogo e a reserva judicial … A intencionalidade da alteração legislativa extrai-se da circunstância de incidir numa questão que vinha sendo suscitada e decidida de forma maioritária em sentido oposto"*, ob. cit., pág. 91] - não se alcança como se possa atribuir relevância à distinção supra enunciada, a nosso ver, repete-se, sem suporte na letra da lei, sequer,

pelos motivos já aflorados, na "*mens legislatoris*".
Sublinhando que no sistema legal da Lei do Cibercrime "*não poderá nunca haver mensagens de correio electrónico apreendidas para serem utilizadas como prova num determinando processo sem que haja um despacho de um juiz nesse sentido*", defendendo, contudo, nem sempre ser exigível a existência de uma prévia decisão judicial para a respectiva apreensão, que pode revestir a natureza provisória - *vg.* quando surgida no decurso de uma pesquisa realizada com a autorização do Ministério Público – discorrendo, ainda, sobre a articulação entre a dita norma e o regime da apreensão da correspondência previsto no Código de Processo Penal *vd*. Pedro Verdelho, ob. cit., págs. 740 a 746.

Conclui-se, pois, no sentido de carecer de autorização judicial a apreensão de mensagens de correio electrónico ou de registos de comunicações de natureza semelhante [como são as SMS] encontradas, no decurso de pesquisa informática ou outro acesso legítimo [como ocorreu no caso] a um sistema informático [telemóvel], neste armazenadas, impondo-se, em consequência, a revogação de despacho recorrido.

III. Decisão

Termos em que acordam os Juízes na Secção Criminal do Tribunal da Relação de Guimarães em conceder provimento ao recurso, revogando o despacho recorrido, o qual deverá ser substituído por outro, que procedendo à avaliação/ponderação de acordo com o disposto no artigo 17.º da Lei do Cibercrime, decida em conformidade.

Sem tributação

Guimarães, 29 de Março de 2011