A INTERNET, O DIREITO E A JUSTIÇA: UMA ABORDAGEM PRÁTICO-JUDICIÁRIA[*]

TIAGO CAIADO MILHEIRO[**]

O advento da internet fez surgir no âmbito dos tribunais novas problemáticas em diversas áreas que a jurisprudência paulatinamente tem tentado solucionar.

São inúmeras as questões de ordem jurídica que se podem suscitar e relacionar com a Internet: prova digital e valoração desta prova, processo digital, responsabilidade civil, criminal, disciplinar, direitos autorais, privacidade e direitos fundamentais dos cidadãos, a responsabilidade por conteúdos inseridos na internet, a protecção de dados informáticos, entre outras.

Enfim, de uma forma sintética busca-se com esta exposição apresentar um conjunto de questões práticas e como as mesmas têm sido abordadas, analisadas e resolvidas a nível essencialmente jurisprudencial, procurando abranger diversas temáticas e áreas, como seja a privacidade dos trabalhadores, a internet versus processo disciplinar, a acção de divórcio, a internet e valoração da prova digital, a responsabilidade civil com origem na internet, o Google street view, os conteúdos no You Tube versus reserva da vida privada.

Diga-se ainda, que não se procura no âmbito desta exposição, analisar exaustivamente as soluções legais e doutrinais, mas sim expor de forma simplista realidades ocorridas e orientações jurisprudenciais.

[*] O presente escrito teve por objectivo servir de documento de apoio à intervenção no Curso de formação avançada "Direito, Justiça e Internet", da Unifoj, que decorreu nos dias 21 e 22 de Junho de 2013, em Coimbra.

[**] Juiz de Direito.

1. Privacidade dos trabalhadores, a internet vs poder disciplinar.

Uma das áreas sobre as quais, no âmbito laboral, os tribunais se têm debruçado, prende-se com a dialéctica das privacidade dos trabalhadores, o uso da internet e o poder disciplinar da entidade patronal.

Algumas situações da vida real advenientes do uso da internet e que a jurisprudência tem procurado solucionar, assentam nos seguintes **tópicos:**

Direito de reserva e confidencialidade dos trabalhadores relativamente ao conteúdo das mensagens que enviem, recebam ou consultem através do correio electrónico.

Estabelecimento pelo empregador, nomeadamente através de regulamento de empresa, de regras de utilização dos meios de comunicação e das tecnologias de informação e comunicação manuseados na empresa, nomeadamente correio electrónico. Controlo da internet, e-mail e contactos telefónicos e os princípios sobre a privacidade dos trabalhadores no local de trabalho. O uso indevido do correio electrónico, telefone e internet no ambiente do trabalho vs liberdade pessoal e individual do trabalhador.

Direito à prova vs direito de reserva e confidencialidade do trabalhador.

Como facilmente se constata todas estas temáticas estão **inter-relacionadas.**

Por um lado, a vontade da entidade patronal exercer de forma mais ***presente*** o seu poder disciplinar, controlando os trabalhadores, e procurando focos de instabilidade e comportamentos ilícitos destes, por outro, o uso de novas tecnologias, nomeadamente internet, para prova de tais comportamentos e uma esfera pessoal e privada dos trabalhadores inviolável.

Uma das questões que tem vindo a ser analisada pelos tribunais é o acesso e limitação de correio electrónico ou intranet pelos trabalhadores, quer por as mensagens "trocadas" fundarem um ilícito disciplinar, quer para controlar a produtividade do trabalhador. Tem-se discutido igualmente se é possível limitar através de regulamento o uso das tecnologias de informação e comunicação manuseados na empresa, estabelecendo tempos de utilização, vedando acessos ou colocando outros limites.

Importa chamar à colação o art. 21.º do Código de Trabalho que dispõe:

"Confidencialidade de mensagens e de acesso à informação

1 . O trabalhador goza do direito de reserva e confidencialidade relativamente ao conteúdo das mensagens de natureza pessoal e acesso a informação de carácter não profissional que envie, receba ou consulte, nomeadamente através do correio electrónico.

2 . O disposto no número anterior não prejudica o poder de o empregador estabelecer regras de utilização dos meios de comunicação na empresa, nomeadamente do correio electrónico."

Atentemos, então, como a jurisprudência tem resolvido "casos" da vida real, que se prendem com a análise daquele preceito.

A. Caso 1: "Quando resolvi olhar-lhe para a tromba é que vi que era o nosso querido futuro boss". A tutela do curioso.

No ac. da RP, processo n.º 0610399, consultado em www.dgsi.pt, de 26.06.2006, escreveu-se no seu sumário:

"I- Nos termos do art. 21º, 1 do CT "o trabalhador goza do direito de reserva e confidencialidade relativamente ao conteúdo das mensagens de natureza pessoal e acesso a informação de carácter não profissional que envie, receba ou consulte, nomeadamente através do correio electrónico".

II- Não viola tal direito, o superior hierárquico que acede ao endereço electrónico interno da empresa e lê um e-mail dirigido à funcionária que, por regra, acede ao referido correio electrónico, através de "password" que revela a outros funcionários que a tenham que substituir na sua ausência.

III- As expressões usadas pela autora no referido e-mail – "e durante a prelecção sobre filosofia japonesa (que para estes gajos por acaso não é japonês mas sim chinês), pensei que devia estar sentada ao lado de algum yuppi cá da empresa."... "Quando resolvi olhar-lhe para a tromba é que vi que era o nosso querido futuro boss" – merecem censura, mas não constituem justa causa de despedimento."

Entendeu-se não estar em causa a esfera de privacidade ***"intocável"*** da trabalhadora, já que a mensagem foi enviada para um endereço geral da empresa, para onde são igualmente remetidas mensagens endereçadas a esta e no seu interesse. Não se tratava de um endereço exclusivo da trabalhadora, mas de uso do empregador, pelo que tratando-se de endereço partilhado nunca a trabalhadora poderia ter uma expectativa de privacidade relativamente a mensagens enviadas para o mesmo. Por seu turno, o Director que abriu a mensagem teria toda a expectativa de se tratar de uma mensagem para a empresa, pelo facto do endereço ser destinado a questões comerciais da entidade empregadora. Não posso deixar de salientar uma passagem que, confesso, não deixa de ter a sua piada, numa espécie de "tutela do curioso", escrevendo-se *"De qualquer modo se dirá que quando o julgador aprecia os factos e aplica o direito aos mesmos não pode deixar nunca de ponderar e ter em conta a natureza humana: e quem não ficaria curioso em ler uma mensagem enviada para um correio electrónico – cujos fins já descrevemos - , que começa com palavras tão carinhosas… «Oi fofinha, estás bem?». Negar tal conduta é ir contra o que é natural e se espera das pessoas nas relações do dia-a-dia"*. De todo o modo, e em suma, foi considerada legítimo o acesso ao correio electrónico, sendo, contudo, que o comportamento apesar de ter sido considerado censurável, não foi considerado suficientemente grave para constituir justa causa.

B. Caso 2: O repórter fotográfico que envia por e-mail fotos do seu local de trabalho para outro jornal (da concorrência), onde são publicadas.

Cita-se aqui o ac. da RL, processo n.º 2970/2008-4, 6.05.2008, consultado em www.dgsi.pt, em cujo sumário se escreveu:

"I - O envio de mensagens electrónicas de pessoa a pessoa («e-mail») preenche os pressupostos da correspondência privada (Internet – Serviço de comunicação privada).

II – A inviolabilidade do domicílio e da correspondência vincula toda e qualquer pessoa, sendo certo que a protecção da intimidade da vida privada assume dimensão de relevo no âmbito das relações jurídico – laborais.

III – Resulta do artigo 21º do CT que se mostram vedadas ao empregador intrusões no conteúdo das mensagens de natureza não profissional que o trabalhador envie, receba ou consulte a partir ou no local do trabalho, independentemente da sua forma.

IV - A protecção em apreço, pois, abrange a confidencialidade das cartas missivas, bem como as informações enviadas ou recebidas através da utilização de tecnologias de informação e comunicação, nomeadamente o correio electrónico.

V - Todavia a reserva da intimidade da vida privada do trabalhador não prejudica a possibilidade de o empregador estabelecer, nomeadamente através de regulamento de empresa, regras de utilização dos meios de comunicação e das tecnologias de informação e comunicação manuseados na empresa (vg: imposição de limites, tempos de utilização, acessos ou sítios vedados aos trabalhadores).

VI – Se a entidade patronal incumprir as supra citadas regras não serão de atender os decorrentes meios de prova juntos ao processo disciplinar."

Neste caso a entidade patronal acedeu ao correio electrónico do trabalhador. Tratava-se da situação de um repórter fotográfico que trabalhava para um jornal, mas que do seu local de trabalho e através da Internet enviou fotografias tiradas ao serviço da sua entidade patronal para outro jornal, ali tendo sido publicadas. Considerou-se que não poderiam ser utilizados os conhecimentos advenientes do teor de tais e-mails. Chama-se a atenção, contudo, que *"A reserva da intimidade da vida privada do trabalhador não prejudica a possibilidade de o empregador estabelecer regras de utilização dos meios de comunicação e das tecnologias de informação e comunicação manuseados na empresa, nomeadamente através da imposição de limites, tempos de utilização, acessos ou sítios vedados aos trabalhadores; sendo certo que se sustenta que a forma por excelência, para a comunicação dessas regras deve ser o regulamento de empresa".* No entanto, no caso não havia tal regulamento, nem o mail era o "profissional", pelo que não haveria qualquer motivo para acreditar que a mensagem assim o fosse, ou seja, para legitimamente acreditar que não fosse pessoal, pelo que não podendo a entidade patronal aceder a tal e-mail do trabalhador, por consequência não poderia ser valorado no processo laboral a prova que adveio de tal acesso indevido (por proibido pelo referido art. 21.º do CT).

C. Caso 3: O trabalhador que queria "criar" empresa concorrente. A ilicitude da obtenção da prova versus possibilidade da sua valoração processual.

Discute-se se o facto da entidade patronal não poder aceder ao correio electrónico dos trabalhadores, concretamente às comunicações efectuadas no decurso do período laboral, não será uma limitação do direito à prova (do ilícito disciplinar)? Haverá situações em que a prova mesmo que obtida ilicitamente, por visar correio electrónico do trabalhador poderá ser utilizada?

Para o acórdão da Relação de Lisboa, de 03.05.06, in www.dgsi.pt, processo nº 872/2006-4, *"O direito à prova surge no nosso ordenamento jurídico com assento constitucional, consagrado no art. 20º da Lei Fundamental, como componente do direito geral à protecção jurídica e de acesso aos tribunais e dele decorre (...) a possibilidade de utilização pelas partes, em seu benefício, dos meios de prova que mais lhes convierem e do momento da respectiva apresentação, devendo a recusa de qualquer meio de prova ser devidamente fundamentada na lei ou em princípio jurídico, não podendo o tribunal fazê-lo de modo discricionário. Tal direito de prova, porém, não é um direito absoluto, pois como se salienta o Acórdão do Tribunal Constitucional nº 209/95 de 20 de Abril, publicado no DR, II Série, nº 295 de 23.12.95 o direito à produção de prova não significa que o direito subjectivo à prova implique a admissão de todos os meios de prova permitidos em direito, em qualquer tipo de processo e relativamente a qualquer objecto do litígio."*.

Ou seja, este acórdão, embora salientando que o direito à prova não é absoluto, não deixa de admitir que dependendo do tipo de processo e objecto do litigio, o tribunal de forma fundamentada, lhe possa dar primazia.

Foi o que sucedeu no ac. da RL, processo 439/10.3TTCSC-A.L1-4, de 30.06.2011, consultado em www.dgsi.pt, em que também se debruçando sobre o conflito entre o direito à prova e a privacidade do trabalhador, decidiu:

"Destinando-se o dever de reserva e confidencialidade previsto no art. 22.º do Cód. Trab. a proteger direitos pessoais como o direito à reserva da vida privada consagrado no art. 26.º da Constituição da República Portuguesa e 80.º do Cód. Civil, enquanto que o dever de cooperação

para a descoberta da verdade visa a satisfação do interesse público da administração da justiça, a contraposição dos dois interesses em jogo deve, no caso concreto, ser dirimida, atento o teor do pedido e da causa de pedir da acção, com prevalência do princípio do interesse preponderante, segundo um critério de proporcionalidade na restrição de direitos e interesses, constitucionalmente, protegidos, como decorre do art. 18.º, nº 2, da Constituição da República Portuguesa, concedendo-se primazia ao último, ou seja, ao dever de cooperação para a descoberta da verdade, sobre o primeiro."

Foi um caso em que foram visualizadas mensagens do correio electrónico do trabalhador, que não se reportavam à sua vida íntima. Tratavam-se de e-mails enviados para o mail profissional do trabalhador durante o seu horário de trabalho, não existindo qualquer indício de que fosse pessoais, atento os destinatários, remetentes ou assunto do mail, mensagens essas que denunciavam que o trabalhador pretendia, à revelia da entidade patronal, criar uma empresa concorrente, desviando clientes e negócios.

Não se deixou de admitir tratar-se de prova ilícita, dando-se neste caso prevalência ao direito à prova, escrevendo-se que *"as limitações quanto à admissibilidade dos meios de prova, em processo civil, são as que resultam do art. 519.º, mero afloramento do princípio do inquisitório, consagrado pelo art. 265.º, ambos do Cód. Proc. Civil, e não outras, face à inexistência de qualquer concretização das normas constitucionais respeitantes a direitos fundamentais, na área do processo civil, em que a garantia constitucional é menos intensa do que acontece no processo penal, onde já existe uma regulamentação completa das situações em que se concretiza a licitude na obtenção de determinados meios probatórios. Doutro modo, a garantia constitucional constituiria a desprotecção dos meios de prova mais valiosos, em benefício dos mais falíveis, a verdade material ficaria à mercê das vicissitudes da prova testemunhal e o processo civil seria o parente pobre do dispositivo em via reduzida."*

A questão da admissibilidade da prova ilícita será melhor analisada adiante, importando neste momento **reter** a existência de decisões jurisprudenciais na área laboral, que optaram por "aceitar" provas em violação do art. 22.º do CT, considerando como interesse preponderante, em determinados casos concretos e dependendo do circunstancialismo fáctico, a descoberta da verdade material.

Sobre esta matéria Joana Vasconcelos (in "O Contrato de Trabalho. 100 Questões", 2004, págs. 91 a 93) :

"Pode o empregador ler os e-mails pessoais do trabalhador?

"Não, em caso algum. A nossa lei garante, sem mais, o direito à reserva e à confidencialidade de quaisquer mensagens de natureza pessoal – cartas, faxes, correio electrónico, sms, telefonemas, etc. – que o trabalhador envie ou receba no local de trabalho, ainda que utilizando meios de comunicação pertencentes ao empregador.

As mesmas reservas e confidencialidade são asseguradas relativamente a informação não profissional que o trabalhador receba ou consulte – por ex., via Internet – no local de trabalho.

Esta garantia não cede nem nas situações em que a recepção ou envio de mensagens, ou o acesso a informação não profissional contrarie regras definidas pelo empregador quanto à utilização de meios de comunicação e de tecnologias de informação, e constitua infracção disciplinar. Quando tal suceda, o empregador pode controlar, por ex., o remetente ou o destinatário de mensagens de correio electrónico e o seu assunto, de modo a aferir o seu carácter pessoal, mas nunca o seu conteúdo, tal como pode verificar quais os sites a que trabalhador acedeu, mas não o conteúdo da pesquisa efectuada ou da informação neles obtida.(. . .)

(…) Pode o empregador proibir a utilização do correio electrónico da empresa para mensagens pessoais?"

Sim. O empregador pode, em geral, estabelecer regras quanto à utilização de meios de comunicação – telefone, fax; telemóvel; correio electrónico - e de tecnologias de informação – ligações à Internet pertencentes à empresa, designadamente proibindo ou restringindo a sua utilização para fins pessoais dos trabalhadores a quem são atribuídos. O desrespeito de tais regras pelo trabalhador constitui infracção disciplinar.

A existência de tais regras - e, sobretudo, o controlo do seu respeito pelos trabalhadores - não afecta, em caso algum, o direito à reserva e à confidencialidade que a nossa lei garante relativamente a mensagens pessoais e à informação não profissional que o trabalhador receba, consulte ou envie, designadamente através de correio electrónico. Mais exactamente, o empregador não pode aceder ao conteúdo de tais mensagens ou de tal informação, nem mesmo

quando esteja em causa investigar e provar a eventual infracção disciplinar decorrente do incumprimento de tais regras de utilização" (negrito nosso).

Assim, cumpre concluir que tal tutela (sendo certo que também não consta que a respectiva abertura e visualização tenha sido levada a cabo na presença do trabalhador ou de seu representante …) impede , no caso concreto, a utilização do conteúdo das mensagens em apreço como meio de prova no processo disciplinar que a requerida intentou ao trabalhador.

Tal raciocínio encontra suporte no disposto nº 8º do artigo 32º da Constituição que estatui em sede de garantias em processo criminal, que "são nulas todas as provas obtidas mediante …., abusiva intromissão , no domicilio , na correspondência ou nas telecomunicações".

Também com interesse nesta matéria documento aprovado pela Comissão Nacional de Protecção de Dados (CNPD), na sessão plenária de 29 de Outubro de 2002 (http://www.cnpd.pt/bin/orientacoes/principiostrabalho.htm), em que a CNPD faz várias recomendações e estabelece princípios na utilização das novas tecnologias - Princípios Genéricos; Princípios relativos ao tratamento de dados nas centrais telefónicas; Princípios gerais relativos à utilização e controlo do e-mail e Internet; Princípios específicos em relação ao e-mail; Princípios relativos à Internet; Procedimentos a adoptar pelas entidades empregadoras;

No Brasil salienta-se uma jurisprudência no sentido da admissibilidade de utilização pela entidade empregadora de prova obtida mediante acesso ao "e-mail corporativo"[1], por se tratar de instrumento de trabalho, que a entidade patronal tem *direito de fiscalização* para aferir se está a ser utilizado correctamente e para os fins a que é destinado.

[1] Como também é admitido em decisões dos Tribunais portugueses, conforme supra mencionado, nomeadamente se tal estiver vertido em regulamento da empresa. Em sentido contrário, conforme acima citado, Joana Vasconcelos in "O Contrato de Trabalho. 100 Questões", 2004, págs. 91 a 93.

Entre outros veja-se[2]:

TST[3], Relator Vieira de Mello Filho, AIRR[4]-1640/2003-051-01-40.0, Julgado em 15/10/2008:

"Consoante entendimento consolidado neste Tribunal, o e-mail corporativo ostenta a natureza jurídica de ferramenta de trabalho, fornecida pelo empregador ao seu empregado, motivo pelo qual deve o obreiro utilizá-lo de maneira adequada, visando à obtenção da maior eficiência nos serviços que desempenha. Dessa forma, não viola os arts. 5º, X e XII, da Carta Magna *a utilização, pelo empregador, do conteúdo do mencionado instrumento de trabalho,* uma vez que cabe àquele que suporta os riscos da atividade produtiva zelar pelo correto uso dos meios que proporciona aos seus subordinados para o desempenho de suas funções."

TRT4[5], Rel. Flavio Portinho Sirangelo, RO nº 00168-2007-203-04-00-3 (RO), Julgado. 03/09/2008:

"Prova que evidencia a utilização do email funcional, pelo empregado, para difundir informações tendentes a denegrir a imagem da empregadora. Constitui justa causa para a despedida o uso indevido do correio eletrônico fornecido pelo empregador, não se podendo cogitar de infração ao disposto no artigo 5º, inciso XII da CF, já que o serviço de "e-mail" é ferramenta fornecida para uso estritamente profissional."

[2] Consultado em "Análise dos últimos 10 anos do Direito Digital no Judiciário Brasileiro. II Consolidado de Jurisprudência - Direito Digital, "Patrícia Peck Pinheiro, Vivian Pratti, Rogério Martes: http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=8396&revista_caderno=17.

[3] Tribunal Superior do Trabalho. O Tribunal Superior do Trabalho (TST) é a instância mais elevada de julgamento para temas envolvendo o direito do trabalho no Brasil. Consistindo na instância máxima da Justiça Federal especializada do Trabalho brasileiro que por sua vez organiza-se em Tribunais Regionais do Trabalho (TRT) e que por sua vez coordenam as Varas do Trabalho. É um dos Tribunais Superiores brasileiros, ao lado do Supremo Tribunal Federal (STF), do Superior Tribunal Militar (STM), do Tribunal Superior Eleitoral (TSE) e do Superior Tribunal de Justiça (STJ). Informação disponível em http://pt.wikipedia.org/wiki/Tribunal_Superior_do_Trabalho.

[4] Autos de Agravo de Instrumento em Recurso de Revista.

[5] Tribunal Regional de Trabalho da 4.ª Região (Rio Grande do Sul)

TST, Rel.Min. João Batista Brito Pereira, AIRR - 426540-10.2007.5.12.0036, Julgado em 25/08/2010:

(...) No entanto, a jurisprudência somente vem admitindo a possibilidade de o empregador monitorar e rastrear a atividade do empregado no ambiente de trabalho, em `e-mail-corporativo.(…) Saliento que o e-mail pessoal ou particular do empregado desfruta da proteção constitucional e legal de inviolabilidade, sendo ilícitas as provas por ele obtidas.

TST, Rel.Min. Ives Gandra Martins Filho, RR[6] - 9961/2004-015-09-00, Publicado em 20/02/2009:

"O art. 5º, XII, da CF garante, entre outras, a inviolabilidade do sigilo da correspondência e da comunicação de dados. 2. A natureza da correspondência e da comunicação de dados é elemento que matiza e limita a garantia constitucional, em face da finalidade da norma: da pessoa física ou jurídica diante de terceiros. 3. Ora, se o meio de comunicação é o institucional da pessoa jurídica -, não há de se falar em violação do sigilo de correspondência, seja impressa ou eletrônica, pela própria empresa, uma vez que, em princípio, o conteúdo deve ou pode ser conhecido por ela. 4. Assim, se o e-mail é fornecido pela empresa, como instrumento de trabalho, não há impedimento a que a empresa a ele tenha acesso, para verificar se está sendo utilizado adequadamente. Em geral, se o uso, ainda que para fins particulares, não extrapola os limites da moral e da razoabilidade, o normal será que não haja investigação sobre o conteúdo de correspondência particular em e-mail corporativo. Se o trabalhador quiser sigilo garantido, nada mais fácil do que criar seu endereço eletrônico pessoal, de forma gratuita, como se dá com o sistema gmail do Google, de acesso universal. 5. Portanto, não há dano moral a ser indenizado, em se tratando de verificação, por parte da empresa, do conteúdo do correio eletrônico do empregado, quando corporativo, havendo suspeita de divulgação de material pornográfico, como no caso dos autos."

TST, Rel. Min. Vieira de Mello Filho, Ag. Instr. em RR[7] nº 1130/2004-047-02-40, Julgado em 31/10/2007:

[6] Recurso de revista.

"Correio eletrônico. Monitoramento. Legalidade. Não fere norma constitucional a quebra de sigilo de e-mail corporativo, sobretudo quando o empregador dá a seus empregados ciência prévia das normas de utilização do sistema e da possibilidade de rastreamento e monitoramento de seu correio eletrônico. (...) Comungo do entendimento a quo no sentido de afastar a alegada ofensa aos incisos X, XII, LVI do art. 5º constitucional, por não ferir norma constitucional a quebra de sigilo de e-mail fornecido pela empresa, sobretudo quando o empregador avisa a seus empregados acerca das normas de utilização do sistema e da possibilidade de rastreamento e monitoramento de seu correio eletrônico. Também o julgado recorrido consignou ter o empregador o legítimo direito de regular o uso dos bens da empresa, nos moldes do art. 2º da CLT, que prevê os poderes diretivo, regulamentar, fiscalizatório e disciplinar do empregado, inexistindo notícia acerca de excessiva conduta derivada do poder empresarial."

2. A internet e a acção de divórcio. A prova ilícita no direito da família. Efeito à distância. A teoria da proporcionalidade.

Caso hipotético:

"Ana "liga" o computador pessoal do seu marido Alberto, acede ao correio electrónico através de password que conseguiu descobrir sorrateiramente quando Alberto usava o computador, e abre vários e-mails remetidos por Filipa, no qual descobriu que "namoriscavam" (Filipa e seu marido) pela internet. Fez download das mensagens e instaurou acção de divórcio onde juntou como prova as mesmas. Fez ainda uma pesquisa na Internet e descobriu a página pessoal de Filipa no facebook, onde tinha fotos com o seu marido. Por sua vez António usando um computador portátil e uma webcam que colocou no veículo de Ana, captou imagens desta com Manuel, enquanto se beijavam, gravação que utilizou para em sede de reconvenção também ele deduzir pedido de divórcio."

[7] Agravo de instrumento em recurso de revista.

Este exemplo hipotético "expõe" como o uso da internet levanta novas questões no âmbito do direito da família, como seja nas acções de divórcio, nomeadamente sobre a violação dos deveres conjugais e valoração de prova digital.

Quanto à questão dos ***flirts***, através das comunicações eletrónicas tem sido entendido como violação de dever conjugal, embora alguns entendam estarmos no domínio da infidelidade (virtual) e outros no domínio da violação do dever de respeito. Ou seja, um relacionamento amoroso através da Internet, quer seja através de e-mails, chats de conversação, facebook, webcam, etc. consiste na denominada infidelidade moral que o STJ já salientava em decisões[8] da década de 90. Entre outros:

Ac. do STJ, de 2.12.1992, proc. n.º 082820

"A infidelidade moral ao cônjuge pode resultar de relações sexuais sem cópula, "flirt", ligação sentimental ou namoro com outra mulher."

Ac. do STJ, 10.12.1996, proc 96A349

"I - O dever de fidelidade recíproca tem por objectivo a dedicação exclusiva e sincera, como consorte, de cada um dos cônjuges ao outro, envolvendo a proibição de qualquer dos cônjuges ter relações sexuais com terceira pessoa (adultério ou infidelidade material) ou ter com ela mera ligação sentimental ou platónica (infidelidade moral).

II - O dever de respeito tem por objecto a "honra e o bom nome solidário do casal" além de abranger o dever que recai sobre cada um dos cônjuges de não atentar contra a integridade física ou moral do outro."

Ou seja, na hipótese que levantamos, a relação amorosa que tenha sido iniciada na internet entre António e Filipa, por exemplo, através de um chat (sala de conversação), e que prossiga com troca de e-mails, mesmo que ainda não consumada, pode pois consistir na violação do dever

[8] Consultadas em www.dgsi.pt.

de respeito ou fidelidade (art. 1762.º do CC), e determinar a procedência do divórcio, caso tal ligação encetada através da internet demostre a ruptura definitiva do casamento.

Outra questão é a possibilidade de utilização da prova digital obtida nos termos acima apontados. Quanto às fotografias que Ana encontrou de Filipa com António na página pessoal dela da internet, tratava-se de acesso público, pelo que nenhum óbice a que fosse junto ao processo (ou juntando em papel cópia da página da internet onde se encontrava a foto com o link de acesso ou exibindo essa mesma foto em audiência através de recurso do computador), uma vez que nenhuma infracção se vislumbra, nomeadamente ao disposto no art. 79.º do Código Civil e 199.º do Código Penal.

Já quanto à acesso não consentido da correspondência de António pela mulher Ana e da gravação feita por António através da webcam, seria controverso a utilização de tal prova obtida na, ou através, da internet.

Estão aqui em causa bens jurídicos como seja a reserva da vida privada, direito à imagem e palavra, bem como segredo da correspondência e das telecomunicações, que estão tutelados quer no nosso Código Civil (artigos 70.º, 75.º, 78.º e 79.º do CC), quer no Código Penal (cfr. artigos 194.º e 199.º do Código Penal).

Vejamos como a jurisprudência tem resolvido algumas destas questões e outras similares, tais como:

- *Intercepções e gravações de sons e imagens, invasão da correspondência do outro cônjuge e o seu valor probatório em acção de divórcio.*
- *Do valor do testemunho com conhecimento com base na prova acima referida.*
- *Da responsabilidade criminal e civil do cônjuge que juntar prova ilícita ao processo de divórcio.*

A propósito da utilização de uma carta endereçada a um cônjuge numa acção de divórcio (mas que, pelo paralelismo das situações, é aplicável ao e-mail), e da responsabilização criminal

que daí pode "derivar" para o cônjuge que a junta como prova no referido processo, veja-se ac. da RG, proc. 718/04-2, de 28.06.2004, consultado em www.dgsi.

Estava em causa a análise do art. 194.º, nºos 1 e 3 do Código Penal que, relembre-se, estatuem que:

"Artigo 194º

(violação de correspondência ou de telecomunicações)

1. Quem, sem consentimento, abrir encomenda, carta ou qualquer outro escrito que se encontre fechado e lhe não seja dirigido, ou tomar conhecimento, por processos técnicos, do seu conteúdo, ou impedir, por qualquer modo, que seja recebido pelo destinatário, é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias.

2. …..

3. Quem, sem consentimento, divulgar o conteúdo de cartas, encomendas, escritos fechados, ou telecomunicações a que se referem os números anteriores, é punido com a pena de prisão até 1 ano ou com pena de multa até 240 dias."

No processo de divórcio o arguido juntou aos autos uma carta enviada por uma irmã da sua mulher para a casa de morada de família do casal, embora nessa altura o cônjuge já ali não vivesse, em que era criticada a conduta desta, principalmente de abandono do filho. O arguido, em sua defesa, invocou a exclusão da ilicitude, porque estava a exercer um direito de defesa, pelo que não actuou com dolo aquando da junção da carta aos autos de divórcio para prova dos factos alegados na contestação, para além de que a missiva circulou num círculo restrito de indivíduos, não consubstanciando qualquer conceito de "terceiros".

Para o que ora interessa, escreveu-se naquele acórdão:

"Assim, os elementos gramatical, sistemático, histórico e teleológico não autorizam nem legitimam a interpretação que o recorrente faz do preceito, antes reclamam e impõem a interpretação dada pelo Ministério Público, na 1ª e 2ª instâncias, que vai de encontro ao enquadramento jurídico dado aos factos pelo tribunal recorrido. Inequivocamente, o arguido, ao juntar ao processo de divórcio, sem consentimento da ofendida, uma carta que a esta tinha sido dirigida para a sua morada, divulgou ilicitamente o seu conteúdo, ainda que num universo

restrito de pessoas, pelo que esse seu comportamento integra o tipo legal de crime previsto no nº3, do artigo 194º, mesmo não se tendo provado ter sido ele autor da violação dessa correspondência. A circunstância de a carta ter sido recebida na casa de morada de família que a destinatária anteriormente tinha abandonado, não obsta a que se considere que a missiva tenha entrado na esfera de disponibilidade fáctica da ofendida, nem legitima o arguido a considerá-la como sua.

O recorrente pretende, em vão, justificar o seu comportamento com o chamado "estado de necessidade probatório". É que os interesses particulares do arguido em provar, com a carta, factos alegados na acção de divórcio contra ele instaurada pela ofendida, não se podem sobrepor nem justificam o sacrifício dos direitos de personalidade desta, tanto mais que o arguido não demonstrou a impossibilidade de substituir esse meio de prova, designadamente a convocação como testemunha do autor da missiva. Ou seja, como refere o Ministério Público na resposta às motivações de recurso, no caso não existiu uma sensível superioridade do interesse a salvaguardar pelo arguido relativamente ao interesse sacrificado da ofendida, o que desde logo afasta a verificação de um direito de necessidade, como causa de exclusão da ilicitude (cfr. artigo 34º, al. b), do Código Penal)."

Em suma, conclui-se pela prática do crime, mas deixa-se em aberto a possibilidade de, em determinadas circunstâncias, quer por ser o único meio de prova, quer atento aos valores e ao processo em questão, a exclusão da ilicitude poder operar nos termos do art. 34.º. al. b) do Código Penal.

De igual modo, o facto de em determinados casos se dever dar prevalência ao direito à prova para lograr justiça material no caso em concreto[9], em detrimento de direitos tutelados criminalmente pelas partes, também poderá determinar justificação do ilícito penal, pelo facto de estarmos perante um exercício de direito, apenas justificável caso seja necessário, adequado, proporcional e não excessivo, para tutelar aqueles outros valores (cfr. art. 31.º,n.º 1 e n.º 2, al. b) do CP e 18.º da CRP). E por isso de poderá dizer que em princípio a admissão de provas em

[9] Conforme alguns acórdãos supra citados.

processo civil à luz da já referida teoria da proporcionalidade ou tese intermédia (que melhor analisaremos) deverá justificar o ilícito penal, tudo dependendo do caso em concreto.

No processo 2465/08-2, de 07.05.2009, ac. da RL, consultado em www.dgsi, entendeu-se não ser admissível a junção à acção de divórcio, no caso concreto, de e-mail obtido através de acesso não consentido ao correio electrónico de um dos cônjuges, escrevendo-se no sumário que *"Não devem ser admitidos no processo documentos que tenham sido obtidos por forma ilícita, sendo que esta poderá decorrer da violação do estipulado no art.º 32.º, n.º 8 da Constituição da República Portuguesa, aplicável analogicamente ao processo civil."*.

Considerou-se ser uma abusiva intromissão na correspondência, tratando-se de prova ilícita que não poderia ser valorável, aplicando pois o referido art. 32.º, n.º 8 da Constituição, segundo o qual "São nulas todas as provas obtidas mediante tortura, coacção, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações."

Afastou a aplicabilidade do art. 519.º, n.º 3 do CPC, referindo que surge *"como um afloramento de inadmissibilidade indirecta, pois que concretamente se dirige aos que, sendo ou não partes na acção, podem recusar-se a prestar a sua cooperação para a descoberta da verdade, com fundamento na invocação da violação da integridade física ou moral das pessoas, da intromissão na vida privada ou familiar, no domicílio, na correspondência ou nas telecomunicações ou da violação do sigilo profissional ou de funcionários públicos, ou do segredo de Estado, (...) não se trata de norma dirigida directamente ao juiz no âmbito do seu poder vinculado de admissão ou não de provas."*

Também admite que a lei processual civil não tem solução legal para o efeito, *"importando saber em que medida é que sendo uma prova ilícita na sua obtenção tal possa levar à sua inadmissibilidade de aceitação, pois que ao contrário do que sucede no processo penal, (vide designadamente o disposto no art.º 126.º, n.º 3 do Código de Processo Penal) a lei processual civil não estatui directamente a nulidade das mesmas."*

Conclui pois que a solução para tal questão deverá ser encontrada no âmbito da nossa lei fundamental e nos princípios nela enunciados, afastando a admissibilidade de tal prova por via do referido art. 32.º, n.º 8 da Constituição[10].

Este acórdão assume a denominada ***tese restritiva da admissibilidade das provas ilícitas no domínio do processo civil***, como é perceptível ao se escrever *"não havendo aqui um poder discricionário do juiz que o leve a não admitir esta ou aquela prova."* Pugnam os defensores desta tese que toda e qualquer prova ilícita não pode ser valorada no processo civil, independentemente de qual seja a ilicitude em causa e os contornos do caso concreto.

No ac. da R.G., processo n.º 595/07.8TMBRG, de 30.04.2009, abordou-se a questão da valoração das declarações de uma testemunha cujo conhecimento assentou numa gravação ilícita feita pelo cônjuge, instalando um gravador no veículo utilizado pela sua mulher para prova da sua infidelidade (e que pelo paralelismo das situações poderia ser aplicável ao nosso caso hipotético, em que António usando um computador portátil e uma webcam que colocou no veículo de Ana, via internet, também comprovou a sua infidelidade). Escreveu-se, assim, no seu sumário:

"I – A CRP garante o direito à reserva da intimidade da vida privada.

II – Tal direito é directamente aplicável e exequível por si mesmo, sem necessitar da intervenção da lei ordinária, e vincula entidades públicas (a começar pelos tribunais) e privadas.

III - Nos termos da CRP é nula – logo necessariamente ilícita e proibida – a prova obtida mediante abusiva intromissão na vida privada.

[10] A propósito da aplicabilidade do art. 32.º, n.º 8 da CRP ao processo civil, dado a regra desse artigo não ser excepcional, nem as suas razões justificativas serem válidas apenas para o processo penal, Isabel Alexandre (Provas Ilícitas em Processo Civil – 1998 – Almedina, págs. 190-191, 192-195 e pág. 287) entende que nas situações em que se comprove ter havido uma abusiva intromissão na vida privada, no domicílio, na correspondência ou nas comunicações, estará o juiz obrigado a não admitir a prova apresentada que tenha sido obtida através desses meios. Também sobre o tema José João Abrantes ("Prova Ilícita – da sua relevância no Processo Civil", in Revista Jurídica n.º 7, Julho - Setembro 1986 edição da AAFDL, onde a fls. 35) "Pensamos, aliás, que a garantia de processo criminal do n.º 6 (hoje n.º 8) do art.º 32.º da Lei Fundamental (…) é aplicável ao processo civil. Com efeito, aquele preceito nada mais faz do que especificar alguns direitos previstos genericamente nos artgs. 25.º (integridade pessoal) 26.º (reserva da intimidade da vida privada e familiar) e 34.º (inviolabilidade do domicílio e da correspondência), direitos que, face ao nosso ordenamento constitucional (art.º 18.º - 1), são directamente aplicáveis

IV - Esta regra, conquanto formalmente prevista para o processo penal, deve ser tida como aplicável em todo e qualquer processo, e reporta-se tanto à prova obtida tanto pelas entidades públicas como pelas entidades particulares.

V - As proibições de prova produzem, na sua atendibilidade e valoração, aquilo a que se costuma chamar "efeito à distância", no sentido (que porém não esgota o conteúdo da figura) de que da mesma maneira que não é admissível a prova proibida directa, também não é tolerável a prova mediata, fundada naquela outra.

VI – O cônjuge não está legitimado a interceptar e gravar, para efeitos de acção de divórcio, conversa telefónica ou outros sons provenientes do outro cônjuge em interacção com terceiro a partir do espaço do automóvel que tal cônjuge utiliza.

VII - O casamento, pese embora as variáveis mais ou menos morais, filosóficas e societárias que lhe estão associadas, não pode ser visto como implicando a demissão de uma certa privacidade, aí onde os cônjuges a queiram preservar.

VIII - Verificado que uma testemunha adquiriu o seu conhecimento a partir de prova obtida mediante violação do direito à reserva da vida privada da ré – gravação audio - deverá o seu depoimento ser recusado ou, se prestado, ser tido como nulo."

De todo o modo, há que destacar que este acórdão não arreda a possibilidade de utilização da prova ilícita, se tal for imperioso para acautelar o direito do acesso ao direito e aos tribunais, pelo que sempre que exista colisão de direitos entre o direito à reserva da vida privada e aquele outro direito, ambos valores constitucionais, há que fazer tal ponderação, escrevendo a propósito *"que o critério a usar em caso de colisão de direitos conferidos pela CRP deve passar, em primeira linha, não pela hierarquização abstracta dos bens envolvidos nesses direitos fundamentais, mas por uma ponderação em função das circunstâncias concretas em que se põe o problema, de forma a encontrar a solução mais conforme à ordem constitucional. Pois bem: nada encontramos no caso vertente que autorize a pensar que o recurso probatório em causa seja imperioso e insubstituível em ordem à demonstração dos factos a que se destina e, como*

aos particulares, o que significa que podem fundamentar a inadmissibilidade de certos meios de prova, sejam obtidos

assim, que sem ele o direito de acção judicial (rectius, de acesso aos tribunais) do autor seja posto em causa. Já ao contrário, é a todos os títulos evidente que o direito da ré à reserva da intimidade da vida privada fica completamente desguarnecido. A ser assim, como é, não deve este último direito ser posto em crise no confronto daquele outro, como fez o tribunal recorrido."

Já no processo n.º 1488/09.0TAMTS.P1, da RP, de 12.10.2011, consultado em www.dgsi, se admitiu como prova num processo de divórcio fotografias tiradas por telemóvel ao cônjuge que estava na companhia, num casamento, de outra mulher que não a sua esposa, sumariando-se que "Exerce um direito subjetivo, sem lesão dos bens jurídico-penalmente tutelados pelo artº 199º do C. Penal, quem, na posse de fotografias, as usa, ainda que presuntivamente contra a vontade da pessoa nelas visada, como prova de factos que alegou em processo de divórcio e cujo ónus de prova lhe competia." Ali se escreveu que "a junção a um processo de divórcio das ditas fotografias constitui um acto lícito, praticado no exercício de um direito, o direito de produzir prova num processo em que se é parte, acto cuja ilicitude está excluída por força do disposto no artigo 31º/1 e 2 alínea b) C Penal."

Retomando o nosso caso concreto, resulta pois divergente a admissibilidade da prova obtida por Ana através da invasão do correio electrónico no seu marido e as filmagens feitas por este através de uma webcam, que tinham como finalidade a prova da infidelidade na acção de divórcio.

Quanto a nós, neste tema, mais abrangente e profundo, da utilização da prova ilícita em processo civil, defendemos a denominada pela doutrina brasileira teoria da proporcionalidade ou tese intermédia, ou seja, casuisticamente, caso a caso, atento à importância do processo, dos direitos que se pretendem valer, e dos meios de prova existentes, é preciso aferir se é proporcional, não excessivo, adequado e necessário, considerando o direito à prova e o direito ao acesso ao direito e aos tribunais, permitir a utilização de tais provas, designadamente para o que

por autoridades públicas ou particulares, em processo criminal ou em processo civil."

aqui tratamos, obtidas através de recurso a novas tecnologias, não obstante violarem a reserva da vida privada ou outros valores fundamentais da contraparte no processo.

Na verdade, o processo civil é omisso quanto à valoração de provas que atentem contra valores como seja o segredo da correspondência, a imagem, ou a reserva privada. Repare-se que se trata de prova obtida por particulares, e não por autoridades públicas, para o qual está vocacionada a tutela do art. 32.º, n.º 8 da CRP e 126.º do CPP. E quanto a provas obtidas por particulares não existe no processo civil uma norma similar ao art. 167.º, n.º 1 do CPP, que faz depender as reproduções por qualquer meio electrónico como meio de prova caso não sejam ilícitas nos termos da lei penal. Em processo civil rege o art. 515.º do CPC que dispõe que o Tribunal deve tomar em consideração **todas** as provas produzidas.

Trata-se de um direito à prova, que tem também tutela constitucional nos artigos 20.º, n.ºs 1 e 4 da Constituição da República Portuguesa (CRP) – direito de acesso aos tribunais para defesa dos seus direitos e interesses legalmente protegidos e a um processo equitativo. Em termos civilísticos pode-se chamar à colação como base legal para a possibilidade de utilização de tais provas, o art. 79.º, n.º 2 do CC, ao afastar o consentimento do visado para efeitos de utilização da sua imagem no caso de **"exigências de justiça".** Ou seja, em princípio uma prova que seria ilícita por filmar ou fotografar o visado sem o seu consentimento, será contudo admissível se razões de justiça o impuserem.

Assim sendo, as restrições ou compressões no direito à imagem, reserva privada, ou segredo de correspondência, devem ser proporcionais, adequadas e não excessivas, para efeitos da tutela do acesso ao direito e à prova (cfr. Art. 18.º, n.º 2 do CRP), e se assim for, entendemos que, em princípio se exclui o ilícito criminal (por exemplo, dos tipos legais de gravações e fotografias ilícitas ou violação de correspondência ou telecomunicações p. e p. pelo artigos 194.º e 199.º do CP), por força da aplicação do art. 31.º, n.º 2, al. b) do Código Penal ou em virtude de um estado de necessidade probatório (cfr. Art. 34.º, al. c) do mesmo diploma).

Deverá pois analisar-se caso a caso se a utilização da referida prova é essencial e proporcional ao fim que se prossegue, para efeitos de valoração ou não no processo. Relativamente ao efeito à distância da prova ilícita no âmbito do processo civil não cremos poder

aqui vigorar sem mais a "tese da árvore envenenada", pelo que neste caso, devem operar as restrições para o meio de prova em causa.

3. O processo electrónico (Citius) e questões que se levantam na sua aplicabilidade prática.

O Citius (do latim mais rápido, mais célere), trata-se do nome do denominado projecto de desmaterialização de processos nos tribunais judiciais, que foi desenvolvido no Ministério da Justiça, em vigor nos processos de natureza cível ou similar, elencados no art. 2.º da Portaria n.º 114/2008, de 6 de Fevereiro, com as alterações introduzidas pela Portaria n.º 1538/2008, de 30 de Dezembro e 471/2010, de 8 de Julho, Portaria que regula vários aspectos da tramitação electrónica dos processos judiciais nos tribunais judiciais de 1.ª instância (como seja a apresentação de peças processuais e documentos por transmissão electrónica de dados, comprovação do prévio pagamento da taxa de justiça ou da concessão do benefício do apoio judiciário, distribuição por meios electrónicos, notificações por transmissão electrónica de dados, prática de actos processuais por meios electrónicos por magistrados e funcionários judiciais e a consulta dos processos).

Esta tramitação electrónica colocou já várias questões sobre as quais os tribunais se tiveram que debruçar.

Uma das situações prende-se em apurar **se a notificação à parte, na pessoa do seu mandatário, quando realizada por transmissão electrónica de dados, beneficia da mesma dilação prevista, no artigo 254º, nº 3, do Código de Processo Civil.**

Ou seja, no que se reporta às notificações em processos pendentes, estabelece o artigo 254.º, n.º 2 do CPC que os mandatários poderão ser notificados electronicamente. Considerando, contudo, que o n.º 5 do referido artigo estabelece que a notificação por transmissão eletrónica de dados se presume feita na data da expedição, coloca-se pois a questão se a presunção de notificação no terceiro dia posterior, ou no primeiro dia útil seguinte a esse, quando o não seja, previsto no n.º 3, terá *aplicabilidade.*

Entendemos que a Portaria n.º 114/2008, de 6 de Fevereiro, com as alterações introduzidas pela Portaria n.º 1538/2008, de 30 de Dezembro e 471/2010, de 8 de Julho

(conjugado com o CPC) permitiria numa interpretação interligada lograr a resposta, já que é expresso o seu art. 21.º-A, n.º 5, a propósito das notificações electrónicas, que o *"sistema informático CITIUS assegura a certificação da data de elaboração da notificação, presumindo-se feita a expedição no terceiro dia posterior ao da elaboração, ou no primeiro dia útil seguinte a esse, quando o final do prazo termine em dia não útil."* Embora a norma mencione a presunção da expedição, afigurava-se-nos que tal não pretendia precludir para as transmissões electrónicas a presunção de notificação existente no CPC para as notificações por via postal.

De todo o modo, o "novo" CPC (proposta de Lei n.º 113/XII que aprovou o código de processo civil) retira qualquer dúvida que houvesse ao dispor no artigo 248.º, a propósito das formalidades das notificações aos mandatários, que o ***"o sistema informático certifica a data da elaboração da notificação, presumindo-se esta feita no terceiro dia posterior ao da elaboração, ou no primeiro dia útil seguinte a esse, quando o não seja."***

É esta a jurisprudência dos Tribunais Superiores, e mesmo nos casos em que no sistema Citius consta que o acto processual foi "lido" pelo mandatário.

Neste sentido, Ac. da RL, processo n.º 79-B/1994.L1-4, 22.06.2011, consultado em www.dgsi.pt, no qual se escreveu *" I- A notificação à parte, na pessoa do seu mandatário, quando realizada por transmissão electrónica de dados, beneficia da mesma dilação prevista, no artigo 254º, nº 3, do Código de Processo Civil, para a notificação postal, presumindo-se feita no terceiro dia posterior ao do registo, ou no primeiro dia útil seguinte a esse, quando o não seja. II- Trata-se uma presunção que apenas pelo notificado pode ser ilidida, provando ele que não foi efectuada a notificação ou que ocorreu em data posterior à presumida, para tanto não servindo o critério da leitura efectiva, por tal desiderato se não encontrar elencado no texto legal."* Igualmente, ac. da RL, de 19.10.2010, processo n.º 277/08.3TBSRQ-F.L1-7, consultado em www.dgsi.pt: *"A notificação ao mandatário por transmissão electrónica de dados presume-se efectuada no 3º dia seguinte ao da sua elaboração no sistema informático CITIUS, ou no 1º dia útil posterior a esse, quando o não seja (arts. 254º, nº 5, do CPC, e 21º-A, nº 5, da Portaria nº 114/2008, de 6 de Fevereiro, redacção da Portaria nº 1538/2008, de 30 de Dezembro); (...) Para esse efeito, de determinação da data de realização da notificação, não releva o momento em que, efectivamente, o mandatário haja procedido à consulta e leitura da decisão notificanda, junto do*

sistema informático CITIUS." Também com a mesma posição o ac. da Ac. da RL, processo n.º 1479/09.0TJLSB-A.L1-1, 23.02.2010, consultado em www.dgsi.pt, que se sumariou nos seguintes moldes: *"1- Nos termos do nº.5 deste art. 254ºdo CPC., a notificação por transmissão electrónica de dados presume-se feita na data da expedição e face ao nº. 6 do mesmo, as presunções estabelecidas nos números anteriores só podem ser ilididas pelo notificado provando que a notificação não foi efectuada ou ocorreu em data posterior à presumida, por razões que lhe não sejam imputáveis. 2- Há que conjugar duas presunções para efeitos de determinação de datas de notificações, ou seja, a presunção de que a notificação por transmissão electrónica se presume feita na data da expedição e a de que esta se presume feita no terceiro dia posterior ao da elaboração, ou no primeiro dia útil seguinte a esse, quando o final do prazo termine em dia não útil. 3- Não houve uma preocupação de redução de prazos aos advogados, ou seja, não se fez qualquer alteração para contemplar uma diferenciação entre a notificação postal e a electrónica. 4- A expedição na via electrónica beneficiará da mesma dilação correspondente à do registo na via postal."*. Do mesmo modo, ac. da RP, processo n.º 257/09.0TVPRT.P1, 4.03.2013, em www.dgsi.pt: *"I- Determina o artigo 150º, 1, do CPC (redação do DL303/2007, de 24-8), que os atos processuais que devam ser praticados por escrito pelas partes são apresentados a juízo preferencialmente por transmissão eletrónica de dados, nos termos definidos na portaria prevista no n.º 1 do artigo 138º-A (Portaria é a n.º 114/2008, de 6-2). II- O artigo 254º, 5, do CPC determina que a notificação por via eletrónica se presume feita na data da expedição e a expedição presume-se feita no 3º dia posterior ao da elaboração, ou no primeiro dia útil seguinte a esse, quando o final do prazo termine em dia não útil – ver artigo 21º-A, 5, da referida Portaria. III- São duas presunções que é necessário combinar, sendo certo que só o notificado pode elidir essas presunções em duas situações: alegando que não recebeu a notificação ou que esta ocorreu em data posterior à presumida. IV- Como se sabe, não é aplicável a Portaria n.º 114/2008 aos tribunais superiores, pela simples razão da peculiaridade da forma como é levado a cabo o trabalho dos seus Magistrados, que em grande parte trabalha em casa o que não tornou viável que a sua intervenção nos autos oferecesse garantias de segurança e praticabilidade ao sistema CITIUS. V - Assim, tem de ser interpretada em termos*

hábeis essa exclusão, não tendo lógica a existência de uma contagem de prazos na Relação diferente da do Tribunal de 1ª Instância."

Questão diversa, prende-se com "problemas" de notificação no âmbito do processo electrónico, por exemplo quando a secção notifica o mandatário, mas não segue em anexo o despacho a notificar, considerando-se neste caso ilidida a presunção de notificação prevista no art.º 254º, n.º 5, do Código de Processo Civil e 21º-A, n.º 5, da Portaria n.º 114/2008, de 6-2, na redacção introduzida pela Portaria n.º 1538/2008, de 30-12. Trata-se pois de um caso em que tem plena aplicabilidade o art. 254.º, n.º 6 do CPC, que considera ilidida a presunção de notificação *"pelo notificado provando que a notificação não foi efetuada ou ocorreu em data posterior à presumida, por razões que lhe não sejam imputáveis."* Decidiu-se, a este propósito, no Ac. da RL, processo n.º 986/09.0TBBNV-A.L1-2, 10.12.2009, consultado em www.dgsi.pt que "*Sendo os próprios serviços do CITIUS a dar conta de que os Srs. funcionários não faziam correctamente as notificações electrónicas, confirmando ainda que efectivamente em finais de Julho de 2009 foram feitas alterações no sistema de visualização dos anexos, sendo agora possível saber se com a notificação segue algum anexo, e que o advogado da parte participou o incidente (não visualização do anexo com o despacho notificando) aos serviços do CITIUS, dois dias depois de notificado do despacho subsequente, é de considerar ilidida a presunção de notificação estabelecida na conjugação dos art.ºs 254º, n.º 5, do Código de Processo Civil e 21º-A, n.º 5, da Portaria n.º 114/2008, de 6-2, na redacção introduzida pela Portaria n.º 1538/2008, de 30-12.*"

A propósito da elisão da presunção de notificação do mandatário dos actos transmitidos electronicamente no 3.º dia útil após a expedição, ou no 1.º dia útil seguinte, se o último dia não o for, a mesma apenas poderá ser feita pelo notificado, não cabendo pois ao Tribunal considerá-lo notificado anteriormente ao decurso do referido prazo (Ac. da RC, de 30.04.2012, processo n.º 420/11.5TBSRT-A.C1, consultado em www.dgsi.pt: *"1. A notificação ao mandatário por transmissão electrónica presume-se efectuada no 3º dia seguinte ao da sua elaboração no sistema informático CITIUS ou nº 1º dia útil posterior a esse, quando o não seja (art. 254 nº5 CPC, art.21-A nº5 da Portaria nº 114/2008 de 6/2, redacção da Portaria nº 1538/2008 de 30/12). 2. Não releva, para o efeito, a data em que o mandatário procedeu à*

consulta e leitura da decisão notificanda no sistema informático CITIUS. 3. A presunção de notificação pode ser ilidida (art.254 nº6 CPC), mas só para alargamento do prazo e não para o seu encurtamento."; Ac. da RC, processo n.º 30-D/2002.C1, de 21.06.2011, www.dgsi.pt: "*1. Face ao disposto no n.º 5 do artigo 21.º-A da Portaria n.º 114/2008, de 6 de Fevereiro, na redacção que lhe foi conferida pela Portaria n.º 1538/2008, de 30 de Dezembro, a notificação por transmissão electrónica de dados presume-se feita no terceiro dia posterior ao da elaboração, ou no primeiro dia útil seguinte a esse quando o final do prazo termine em dia não útil. 2. Perante a presunção legal enunciada, a contagem do prazo para a impugnação do despacho objecto da notificação (ou para a prática de qualquer outro acto que a lei preveja), não pode ficar dependente da averiguação casuística por parte do tribunal, acerca da data em que efectivamente o correio electrónico foi aberto pelo destinatário. 3. Torna-se assim irrelevante a verificação pelo tribunal, da menção inserta no histórico do processo, no sistema citius, de que o destinatário da notificação a leu no mesmo dia em que foi emitida. 4. É aplicável à notificação por transmissão electrónica de dados a regra prevista no n.º 6 do artigo 254.º do CPC, segundo a qual só ao notificado é legalmente reconhecida a faculdade de ilidir a referida presunção, provando que a notificação não foi efectuada ou ocorreu em data posterior à presumida, por razões que lhe não sejam imputáveis."; Acórdão TRE, Processo:404/06.5TBTVR-A.E1, de 13-09-2012, www.dgsi.pt: I - Nos termos do disposto art. 254° do Código de Processo Civil, "a notificação por transmissão electrónica de dados presume-se feita na data da expedição" e tal presunção só pode ser ilidida "pelo notificado provando que a notificação não foi efectuada ou ocorreu em data posterior à presumida, por razões que lhe não sejam imputáveis" (n.º 5 e 6).).*

Contudo, entendendo que poderá ilidir-se a presunção <u>no sentido do encurtamento do prazo</u> ac. da RC, de 7.02.2012, processo n.º 5964/10.3TBLRA-Q.C1, www.dgsi.pt:*"1 - O artº 21º-A nº5 da Portaria 114/2008 de 06 de Fevereiro consagra uma mera presunção iuris tantum, passível de ilisão nos termos gerais e para além dos limites do nº6 do artº 254º do CPC, pelo que, se ilidida, a data da notificação é a data – <u>anterior ou posterior à consagrada na presunção</u> -, na qual se provar ter a expedição sido feita – artº 254º nº5 do CPC. 2 - Este entendimento não é discriminatório e prejudicial, relativamente à via postal, antes evita discriminação para com*

esta, pois que a adesão dos mandatários à notificação via electrónica não é impositiva, mas opcional e é certo que os seus meios são muito mais céleres e fidedignos, sendo consabido que com a expedição o conhecimento do ato notificado fica imediatamente ao alcance do notificando, o que já não se verifica com a via postal."

A prova da elisão da presunção deve ser suficiente para abalar a credibilidade adveniente da certificação informática via Citius de que a mesma foi feita *(Ac. da RC, de 20.06.2012, processo n.º 4054/07.0TBLRA.C1, consultado em www.dgsi.pt , 1. As notificações de mandatários por transmissão eletrónica de dados provenientes do tribunal têm-se por presumidamente feitas na data de expedição (art.º 254, nº 5 do CPC), presumindo-se, por sua vez, esta feita no terceiro dia após a elaboração ou no primeiro dia útil seguinte (art.º 21-A, nº 5, da Portaria nº 114/2008 de 6 de Fevereiro), certificando o CITIUS quanto aos restantes atos processuais a data e hora de expedição, nos termos do art.º 13, a) da dita Portaria, e estas presunções também são ilidíveis (como se colhe do nº 6 do art.º 254 do CPC e da 2ª parte do nº 5 do art.º 21-A da Portaria mencionada). 2. Só que uma tal ilisão não pode naturalmente ser levada a cabo porqualquer tipo de prova. 3. Nomeadamente não pode ser um mero documento particular interno que pode destruir a força probatória que deve ser ligada a um documento oficial - que tem a força de um documento autêntico, nos moldes do art.º 371, nº 1 do CPC - como é o emanado do CITUS. 4. Principalmente quando esse sistema confirma ou atesta que a notificação não só foi disponibilizada como lida em determinado momento.5. Só a demonstração de que tal atestação é material ou ideologicamente falsa, ou eventualmente decorre de um erro do próprio CITIUS, parece poder ter impacto bastante para destruir o seu efeito, que é o de se ter a notificação por efetuada".).*

Nos casos em que deverá praticar-se um acto processual em determinado prazo, e o mandatário se vê impedido de anexar o ficheiro com o conteúdo material de tal peça, por "problemas" no Citius, tem entendido a jurisprudência que se deverá aplicar analogicamente ou por interpretação extensiva o disposto no art. 10.º Portaria n.º 114/2008, de 6 de Fevereiro, com as alterações introduzidas pela Portaria n.º 1538/2008, de 30 de Dezembro e 471/2010, de 8 de Julho. Na verdade, a norma prevê casos em que o sistema Citius não permite o envio da peça processual ou o conjunto da peça processual e dos documentos por

exceder os 3Mb, permitindo o envio das mesmas através de outros meios previstos no CPC. Ora, também nas outras situações em que o sistema Citius inviabiliza a transmissão electrónica por motivo não imputável ao mandatário, por maioria de razão, terá aplicabilidade o disposto no art. 10.º da dita Portaria, podendo pois proceder-se ao envio da peça processual e documentos através dos outros meios previstos no CPC. Assim se decidiu no ac. da RL, processo n.º 1960/10.9TTLSB.L1-4, 30.06.2011, consultado em www.dgsi.pt: *"I- Se ao pretender praticar um acto processual sujeito a prazo, por exemplo contestação, através do CITIUS, a parte se depara com qualquer obstáculo à anexação dos ficheiros com o conteúdo material da peça processual, deve, por interpretação extensiva do disposto no art. 10º nºs 2 a 5 da P. 114/2008, de 6/2, na redacção da P. 1538/2008 de 30/12, proceder à entrega através dos restantes meios previstos no nº 2 do art. 150º do CPC."*

Situações como estas e outras similares ficam abarcadas pelo art. 144.º, n.º 3 do NCPC ("novo" código de processo civil), que dispõe *"A apresentação por transmissão eletrónica de dados dos documentos previstos no número anterior não tem lugar, designadamente, quando o seu formato ou a dimensão dos ficheiros a enviar não o permitir, nos termos definidos na portaria prevista no n.º 1 do artigo 132.º."*

Deve pois o mandatário fazer prova da impossibilidade de ter praticado o acto atempadamente por razões imputáveis ao sistema Citius (Ac. da RP, processo 129/05.9FAVNG-A.P1, consultado em www.dgsi.pt: *"Relativamente à transmissão de dados por via electrónica, o legislador parte do princípio de que os equipamentos são, por regra, fiáveis e asseguram, na esmagadora maioria dos casos, a perfeita recepção do documento. Quando tal não acontece, incumbe ao apresentante demonstrar que o acto não foi atempadamente praticado por razões que não lhe são imputáveis."*).

A não indicação de informação relativa às testemunhas e peritos, no campo respectivo do formulário facultado aos advogados no sistema Citius não obsta a que se considere e admita tal prova se constar do ficheiro anexo remetido (Ac. da RL, processo n.º 6/09.4TBSCF-A.L1.8, de 14.02.2010, consultado em www.dgsi.pt: *"Não tendo sido indicada informação relativa às testemunhas e peritos, no campo respectivo do formulário facultado ao advogados no sistema Citius, para a comunicação electrónica do requerimento probatório,*

apesar de a mesma informação constar do ficheiro anexo, não deve ser rejeitado tal requerimento, no que aos referidos meios de prova diz respeito."; Ac. da RP, p*rocesso n.º 823/08.2TBCHV-A.P1,* 12.04.2010, www.dgsi.pt, *I- Decorre do art. 6º da Portaria nº 114/2008 de 06/02 que existe uma lacuna no que concerne às consequências jurídicas do não preenchimento de campo específico do formulário referente à apresentação dos meios de prova (testemunhal e pericial) quando a peça processual é apresentada em juízo por via electrónica, através do sistema informático CITIUS.II- Assim, caso o rol de testemunhas tenha sido inserido na contestação anexa como ficheiro ao formulário disponibilizado no endereço electrónico necessário, mas não tenha sido inserido no campo específico do formulário relativo à apresentação dos meios de prova, deve ser admitido o rol de testemunhas, uma vez que a peça processual em causa passa a fazer parte integrante do ficheiro único, de formato digital, criado pelo referido sistema informático; Acórdão do Tribunal da Relação de Guimarães, processo: 5834/09.8TBBRG-C.G1, de 11-05-2010: Deve ser admitido o rol de testemunhas constante do requerimento probatório anexo ao formulário de requerimento probatório disponibilizado pelo sistema informático CITIUS, apesar da omissão de preenchimento do campo daquele formulário destinado ao arrolamento de testemunhas.).* **E nada impede que existindo um evidente lapso de escrita, entre o conteúdo do formulário do Citius e o ficheiro anexo, se determine a rectificação, nos termos do art. 249.º do CC –** que passará a estar previsto expressamente no art. 146.º, n.º 1 do "novo" código de processo civil que preceitua: "É admissível a retificação de erros de cálculo ou de escrita, revelados no contexto da peça processual apresentada" – (a este propósito, Ac. da RL, processo n.º 576/10.4TJLSB-8, 25.11.2010, consultado em www.dgsi.pt: "Existindo divergência, por lapso de escrita revelado no contexto do documento escrito, entre os elementos de identificação do Réu constantes do formulário do Citius e o conteúdo dos ficheiros anexos, é licito ao juiz proceder à rectificação do erro material, nos termos do art.249º do CC e ordenar o prosseguimento dos autos em conformidade com o conteúdo do suporte de papel.").

No caso de discrepância entre a data da certificação do citius (data da elaboração) e a data da expedição para efeitos de presunção da notificação, considera-se esta última (Ac. da RL, processo n.º 4261/07.6TTLSB.L1-4, 6.04.2011, consultado em www.dgsi.pt: *"1- Não pode haver discrepância entre data da elaboração da notificação e a data da sua expedição,*

dado que a certificação do citius se destina precisamente a certificar a data de expedição da notificação. 2- Mas se existir essa a discrepância entre a data da certificação do citius (data da elaboração) e a data da expedição deve ser esta a ter em conta para efeitos da presunção da notificação, pelo que, no caso, tendo a expedição electrónica ocorrido em 21.10.2009 (terça-feira) a notificação presume-se feita no terceiro dia posterior ou primeiro dia útil seguinte, ou seja no dia 26.10.2009.").

A partir do momento em que o mandatário faça uso do Citius (bastando para tanto o envio de taxa de justiça, como decidiu o Ac. da R.E., proc. n.º 156/07.1TBARL-A.E1, de 6.12.2012, www.dgsi.pt: "A remessa pelo sistema CITIUS do comprovativo do pagamento da taxa de justiça preenche a previsão da al. b) do nº 4 do art. 21º-A da Portaria nº 114/2008 de 6 de Fevereiro, pelo que, a partir daí devem as notificações passar a ser realizadas nos termos do referido nº 4") **todas as notificações serão por transmissão electrónica, sendo que neste caso não há lugar a notificações por qualquer outro meio** (Ac. da RL, processo n.º 119831/09.3YIPRT.L1-2, de 24.06.2010, consultado em www.dgsi.pt: *"1- As notificações às partes em processos pendentes são realizadas por transmissão electrónica de dados, na pessoa do seu mandatário, nomeadamente, quando o mandatário tenha enviado, para o processo, qualquer peça processual ou documento através do sistema informático CITIUS. E, sendo as notificações realizadas por transmissão electrónica de dados, não há lugar a notificações por qualquer outro meio."*). **A transmissão electrónica das peças processuais e documentos não impede que o juiz se o entender determine a apresentação dos originais, conforme resulta do art. 150.º, n.º 8 do CPC – art. 144.º, n.º 5 do "novo" CPC** (Ac. da RL, processo n.º 12977/08.3YYLSB.L1-8, 14.12.2010, consultado em www.dgsi.pt *"- Nos termos do art. 150º nº8, do C.P.Civil, o disposto no aludido nº3 do mesmo artigo não prejudica o dever de exibição das peças processuais em suporte de papel e dos originais dos documentos juntos pelas partes por meio de transmissão electrónica de dados, sempre que o juiz o determine, nos termos da lei de processo.- Sendo para o efeito notificado, acha-se, assim, o exequente obrigado à apresentação dos originais do requerimento executivo e respectivos documentos.").* Contudo, com o "novo" CPC – art. 724.º, n.º 5 - quando a execução se funde em título de crédito e o requerimento executivo tiver sido entregue por via eletrónica, o exequente deve sempre enviar o

original para o tribunal, dentro dos 10 dias subsequentes à distribuição; na falta de envio, o juiz, oficiosamente ou a requerimento do executado, determina a notificação do exequente para, em 10 dias, proceder a esse envio, sob pena de extinção da execução.

O artigo 12.º, n.º 3 da Portaria 114/2008, com as ulteriores alterações, disciplina os casos em que um dos mandatários não manifesta a sua adesão via Citius, estabelecendo que nos *"casos de não adesão por parte dos mandatários indicados no formulário no prazo fixado na alínea b) do número anterior, considera-se que a peça processual não foi apresentada e anula-se a respectiva distribuição nos casos de requerimento, petição inicial ou petição inicial conjunta.".* Contudo, a jurisprudência tem interpretado restritivamente esta norma, à luz da teleologia e escopo da mesma. Assim, no ac. da RL, processo n.º 1256/10.6YXLSB-A.L1-6, de 17.11.2011, consultado em www.dgsi.pt, decidiu-se que a "falta de "adesão" de um dos mandatário a uma contestação que deva ser subscrita por mais que um advogado não pode dar lugar à aplicação automática da sanção prescrita no n.º 3 do art.º12.º da Portaria 114/2008, antes deve dar lugar, como deu, a um convite ao mandatário "faltoso" para que venha dar a sua "adesão" (como ali se escreveu, este *"preceito radica a sua essência os requerimentos conjuntos, apresentados pelos mandatários das várias partes, como sejam, por exemplo, transacções, pedidos de suspensão da instância, de alteração de datas de diligência, etc. Nestes casos, que envolvem as várias partes, bem se compreende que se uma das partes não dá a sua "adesão", o requerimento não possa ser atendido, não se vendo que outro tratamento pudesse ser dado. Agora, daqui a aplicar-se o mesmo tratamento a uma contestação vai "um passo de gigante", o qual não podemos acolher. E atendendo ao elemento literal do preceito vemos que não se faz qualquer expressa referência ao caso da contestação, contrariamente ao caso da petição. Se o legislador tivesse expressamente previsto e enunciado a situação da contestação, não temos qualquer dúvida em afirmar que não teria retirado da dita falta de "adesão" a consequência que parece ressaltar do texto e que é a defendida pelo recorrente. Em resumo: a falta de "adesão" de um dos mandatário a uma contestação que deva ser subscrita por mais que um advogado não pode dar lugar à aplicação automática da sanção prescrita no n.º 3 do art.º12.º da Portaria 114/2008, antes deve dar lugar, como deu, a um convite ao mandatário "faltoso" para que venha dar a sua "adesão""*. No mesmo sentido, ac. da RE, processo n.º 60/11.9TTEVR.E1, de

6.03.2012, consultado em www.dgsi.pt : "I- Não é correcta a leitura linear do artigo 12.º da Portaria n.º 114/2008, de 6 de Fevereiro, com ulteriores alterações, face ao disposto no artigo 9.º do Código Civil e à razão de ser da norma em referência – que radica, essencialmente, na apresentação de requerimentos conjuntos, apresentados pelos mandatários das diferentes partes e em relação aos quais bem se compreende que não possam ser atendidos se uma delas omite a respectiva "adesão". II- Não se verifica tal situação e não pode acolher-se a consideração da falta de apresentação de articulado quando este foi tempestivamente apresentado e por quem tinha poderes suficientes para o exercício do mandato.").

O **"regime jurídico estabelecido na Portaria n.º 114/2008, de 6 de Fevereiro (com as alterações que lhe foram sendo introduzidas, nomeadamente, pelas Portarias n.º 457/2008, de 20 de Junho e 1538/2008, de 30 de Dezembro), para a tramitação electrónica de processos, é aplicável aos processos pendentes à data da sua entrada em vigor (artigo 11.º, n.º 2 do Decreto-Lei n.º 303/2007, de 24.08) (…) Porém (…) a aplicação do referenciado regime jurídico, tendente à progressiva (mas ainda não concluída) desmaterialização dos processos judiciais (…), vigora apenas para os processos judiciais nos tribunais de 1.ª instância, mas já não nos tribunais superiores, nomeadamente nas Relações e no Supremo Tribunal de Justiça." (Ac. do STJ, proc. n.º 4495/05.8TTLSB.S1, de 13.03.2013, consultado em www.dgsi.pt –** o que implica cautela dos mandatários, no sentido de que caso mudem de escritório comuniquem aos Tribunais Superiores, pois caso não seja usada a notificação electrónica, opera a presunção de notificação prevista no CPC para a via postal).

4. Breves considerandos sobre o valor probatório da prova digital:

No que se reporta ao processo digital "Citius" cabe relembrar que os documentos apresentados por transmissão electrónica têm a força probatória dos originais, nos termos definidos para as certidões (cfr. Art. 150.º, n.º 7 do CPC).

Quanto ao valor probatório da prova digital, muitas vezes se levantam questões tais como o *valor probatório do correio electrónico ou o valor probatório das filmagens e imagens colocadas na internet.*

Importa chamar à colação nesta temática o Decreto-Lei n.º 290-D/99, de 2 de Agosto, com as alterações introduzidas pelos Decretos-Leis n.º 62/2003, de 3 de Abril, n.º 165/2004, de 7 de Junho, 116 -A/2006, de 16 de Junho e DL 88/2009, de 9 de Abril [11], diploma que regula a validade, eficácia e valor dos documentos electrónicos (cfr. art. 1.º), quer para efeitos de processo civil, quer para efeitos do processo penal. Documento electrónico será o documento elaborado mediante processamento electrónico de dados (art. 2.º. al. a)). **O art. 3.º estabelece a forma e força probatória do documento electrónico.** O documento electrónico satisfaz o requisito legal de forma escrita quando **o seu conteúdo seja susceptível de representação como declaração escrita** (art. 3.º, n.º 1). Quando lhe seja aposta uma assinatura electrónica qualificada certificada por uma entidade certificadora credenciada, **o documento electrónico com o conteúdo referido no número anterior** tem a força probatória de documento particular assinado, nos termos do artigo 376.º do Código Civil (art. 3.º, n.º 2). Quando lhe seja aposta uma assinatura electrónica qualificada certificada por uma entidade certificadora credenciada, **o documento electrónico cujo conteúdo não seja susceptível de representação como declaração escrita** tem a força probatória prevista no artigo 368.º do Código Civil e no artigo 167.º do Código de Processo Penal (art. 3.º, n.º 3). O disposto nos números anteriores não obsta à utilização de outro meio de comprovação da autoria e integridade de documentos electrónicos, incluindo outras modalidades de assinatura electrónica, desde que tal meio seja adoptado pelas partes ao abrigo de válida convenção sobre prova ou seja aceite pela pessoa a quem for oposto o documento (art. 3.º, n.º4). **Sem prejuízo do disposto no número anterior, o valor probatório dos documentos electrónicos aos quais não seja aposta uma assinatura electrónica qualificada certificada por entidade certificadora credenciada é apreciado nos termos gerais de direito (art. 3.º, n.º 5).**

[11] Pode ser consultado em http://dre.pt/pdfgratis/2009/04/07000.pdf.

Nos termos do art. 4.º as cópias de documentos electrónicos, sobre idêntico ou diferente tipo de suporte, são válidas e eficazes nos termos gerais de direito e têm a força probatória atribuída às cópias fotográficas pelo n.º 2 do artigo 387.º do Código Civil e pelo artigo 168.º do Código de Processo Penal, se forem observados os requisitos aí previstos.

O art. 6.º reporta-se à comunicação de documentos electrónicos, estabelecendo que o documento electrónico comunicado por um meio de telecomunicações considera-se enviado e recebido pelo destinatário se for transmitido para o endereço electrónico definido por acordo das partes e neste for recebido (art. 6.º, n.º 1). São oponíveis entre as partes e a terceiros a data e a hora da criação, da expedição ou da recepção de um documento electrónico que contenha uma validação cronológica emitida por uma entidade certificadora (art. 6.º, n.º2). A comunicação do documento electrónico, ao qual seja aposta assinatura electrónica qualificada, por meio de telecomunicações que assegure a efectiva recepção equivale à remessa por via postal registada e, se a recepção for comprovada por mensagem de confirmação dirigida ao remetente pelo destinatário que revista idêntica forma, equivale à remessa por via postal registada com aviso de recepção (art. 6.º, n.º 3). Os dados e documentos comunicados por meio de telecomunicações consideram-se em poder do remetente até à recepção pelo destinatário (art. 6.º, n.º 4). Os operadores que assegurem a comunicação de documentos electrónicos por meio de telecomunicações não podem tomar conhecimento do seu conteúdo, nem duplicá-los por qualquer meio ou ceder a terceiros qualquer informação, ainda que resumida ou por extracto, sobre a existência ou sobre o conteúdo desses documentos, salvo quando se trate de informação que, pela sua natureza ou por indicação expressa do seu remetente, se destine a ser tornada pública (art. 6.º, n.º 5).

A este propósito salienta-se que o projecto do novo código de processo civil brasileiro[12] prevê várias normas a disciplinar tal matéria. Assim, no art. 412.º, parágrafos 3.º e 4.º estatui-se "§ 3º A fotografia digital e as extraídas da rede mundial de computadores, se impugnada sua autenticidade, só terão força probatória quando apoiadas por prova testemunhal ou pericial. § 4º Aplica-se o disposto no artigo e em seus parágrafos à forma impressa de mensagem eletrônica."

E quanto à utilização de documentos electrónicos dispõe o art. 425.º que a "utilização de documentos eletrônicos no processo convencional dependerá de sua conversão à forma impressa e de verificação de sua autenticidade, na forma da lei.", sendo que nos termos do art. 426.º "O juiz apreciará o valor probante do documento eletrônico não convertido, assegurado às partes o acesso ao seu teor."

Em Portugal, como assinalámos, o regime que estabelece o valor probatório da prova digital é o Decreto-Lei n.º 290-D/99, de 2 de Agosto, com as alterações introduzidas pelos Decretos-Leis n.º 62/2003, de 3 de Abril, n.º 165/2004, de 7 de Junho, 116 -A/2006, de 16 de Junho e DL 88/2009, de 9 de Abril.

Assim, atento tal diploma, por exemplo uma mensagem de correio electrónico, com assinatura electrónica certificada por entidade credenciada, caso seja escrita, tem o valor de um documento particular assinado, caso contrário trata-se de prova sujeita à livre apreciação da prova (cfr. art. 127.º do CPP e 655.º, n.º 1 do CPC). Nestes casos poderá existir outra prova para demonstrar a autoria do emitente e receptor do e-mail, que pode ser prova testemunhal, ou o facto do e-mail ter sido dado como forma de contacto, ou através da análise dos teores dos e-mails, ou a identificação do IP e utilizador.

No que se reporta à valoração de imagens e filmagens da internet deve atender-se a nível do processo civil ao art. 368.º do CC, ou seja, as mesmas fazem prova plena dos factos e coisas que representam, se a parte contra quem os documentos são apresentados não impugnar a sua exactidão (por ex. imagem retirada do Google earth numa acção de acidente de viação ou de reais).

A nível do processo penal determina o art. 167.º, n.º 1 do CPP que só valerão como prova dos factos ou coisas reproduzidas se não foram ilícitas nos termos da lei penal (por exemplo, filmagem de um turista numa via pública que capta a actuação de um terrorista). Assim, em princípio as fotografias e filmagens obtidas na Internet e que consistam em devassa da vida privada (art. 192.º do Código Penal), devassa por meio informático (art. 193.º do Código Penal) ou gravações ou fotografias ilícitas (art. 199.º do Código Penal), em princípio não serão passíveis

[12] Consultado em http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=831805&filename=

de ser utilizadas como prova em processo penal, excepto caso se verifique uma causa de exclusão da ilicitude prevista nos artigos 31.º e ss do Código Penal, excludentes que poderão ser as previstas no art. 79.º, n.º 2 do Código Civil, nomeadamente quando "exigências de polícia ou de justiça" o imponham.

Muito recentemente se discutiu tal a propósito de um processo-crime em que duas jovens batiam numa outra jovem, acto filmado pelos colegas e depois colocado na rede mundial.

Compartilha-se aqui a posição do Sr. Juiz Desembargador Rui Rangel (Correio da Manhã, 9.06.2011) *"não existindo qualquer obstáculo à sua utilização como meio de prova, porque foi gravado no espaço público, o que exclui qualquer intromissão na vida privada. Não validar essa prova única, num crime grave, e deixar a vítima desprotegida, seria um absurdo e a negação de um processo penal moderno ao serviço da paz e da ordem social."*

Acrescente-se que as autoras do ilícito bem sabiam estar a ser filmadas, sendo que a queixa feita pela vítima dá o seu consentimento à investigação e implicitamente à utilização das filmagens.

5. Crimes praticados através da Internet e a obtenção de prova em ambiente digital:

Existem crimes[13] que apenas podem ser praticados ou cometidos por meio de sistema informático, como sejam os previstos naquela Lei 109/2009 (falsidade informática, dano relativo a programas ou outros dados informáticos, sabotagem informática, acesso ilegítimo, intercepção ilegítima, reprodução ilegítima de programa protegido) e crimes "comuns", em que um dos meios de acção pode ser (mas não necessariamente) a utilização de sistema informático, nomeadamente através da Internet, como por exemplo, crimes de injúrias, difamação, ameaças, de pornografia de menores, etc [14].

PL+8046/2010.

[13] De referir que também as queixas-crime em Portugal podem ser feitas on-line.

[14] Na doutrina brasileira faz-se tal distinção. Assim JESUS, Damásio E. de apud ARAS, Vladimir. Crimes de Informática. Jus Navigandi, Ed. 12, out. 2001, www1.jus.com.br/doutrina/texto.asp?id=2250 , classificando os crimes informáticos em crimes informáticos puros ou próprios e crimes informáticos impuros ou impróprios. Os primeiros são aqueles praticados por meio de um sistema eletrônico, onde o resultado da

Determinado tipo de criminalidade pode ser potenciada, exarcebada ou acentuada pelo uso da Internet, como seja o denominado *stalking*[15], que consubstancia uma forma de perseguição que prejudica a paz do visado e pode culminar em diversos crimes de maior ou menor gravidade. O crime de stalking não está expressamente previsto na nossa legislação, podendo enquadrar-se numa panóplia de crimes, como sejam os crimes de ameaças, coacção, maus tratos ou violência doméstica. Neste acto de perseguição um dos meios usados pelo stalker pode ser justamente a internet, o denominado cyberstalking, por exemplo, através do envio de mensagens para o correio electrónico da vítima ou por meio de redes sociais, publicando fotografias do visado num blog, ou descrevendo o que essa pessoa fez durante o dia, tudo demonstrações de assédio e perseguição, perpetrados pela Internet.

Outro dos fenómenos criminais que devem merecer atenção, pela gravidade que pode gerar nas vítimas, perpetrado através da Internet é o *cyberbullying*. Conforme nos dão conta Juan Calmaestra, Rosario del Rey, Rosario Ortega e Joaquín A. Mora-Merchá [16] *o "caso mais famoso de cyberbullying foi, talvez, o de Megan Meier, uma rapariga americana de 13 anos que se suicidou em 2006, depois de um ataque de cyberbullying no MySpace, cometido por alguém que fingiu ser um adolescente."* Socorrendo-nos ainda de tal estudo poderemos delimitar um conjunto de actuações por Internet usadas pelos pelos cyber-agressores contra os seus alvos. Assim, como ensinam Juan Calmaestra, Rosario del Rey, Rosario Ortega e Joaquín A. Mora-Merchá [17] existe o " **Bashing (insulto)**, quando os cyber-agressores colocam comentários em blogues ou roubam fotos de uma fonte da Internet para alterar as fotografias de forma prejudicial ou adicionam comentários difamatórios" para que sejam vistos online "por outras pessoas, ou filmam alunos a serem espancados por outros", vídeos colocados online. A **Exclusão (Exclusion)** consiste em

conduta se opera em meio eletrônico, sendo o sistema informacional o bem jurídico protegido. Os crimes informáticos impuros ou impróprios são aqueles em que o sistema funciona como ferramenta para a prática de condutas lesivas a bem jurídicos já protegidos por outras normas penais incriminadoras, não relacionados com a os bens informacionais.

[15] Sobre este tema a dissertação de mestrado de Nuno Miguel Lima Luz, Tipificação do Crime de Stalking no Código Penal Português, Introdução ao problema. Análise e proposta de lei criminalizadora, Abril de 2012, consultado em http://repositorio.ucp.pt/bitstream/10400.14/8952/1/TESE.pdf.

[16] Introdução ao cyberbullying, pag. 4, consultado em http://www.cybertraining-project.org/book/printerfriendly/pt/Module%203%20-%20Portuguese.pdf.

"ser excluído de participar em actividades online com os seus pares, o que pode causar um sentimento de rejeição, exclusão que pode ser de jogos online, de blogues de grupo, num ambiente de mensagens instantâneas". **O Flaming (manifestar ódio)** "inclui linguagem vulgar, rude e ofensiva, insultos e por vezes ameaças que pode ocorrer através de mensagens instantâneas ou em blogues de sites de redes sociais, salas de conversação, fóruns de discussão, ou sites de jogos online". A **revelação de segredos (Outing)** "privadas ou pessoais sobre o sujeito-alvo, provocando vergonha ou humilhação. Uma forma comum de revelação de segredos é o reencaminhamento de uma mensagem do sujeito-alvo que contém informação pessoal e íntima". Por fim a **dissimulação (Posing),** na qual um "cyber-agressor cria sites na Internet, fingindo ser o sujeito-alvo. Outra alternativa é a utilização da informação de acesso do utilizador-alvo para iniciar uma situação de abuso, tal como colocar comentários difamatórios. Quando o cyber-agressor finge ser o sujeito-alvo e diz coisas más sobre os amigos deste, pode fazer com que esses amigos o rejeitem."

A nível das relações laborais o *mobbing* pode ser praticado através da Internet. Referimo-nos ao assédio indesejado ao trabalhador pela entidade patronal, previsto no art. 24.º do Código de Trabalho, quer para destabilizar o mesmo, ou com conteúdo sexual, por exemplo através de envio de mensagens para o correio electrónico do trabalhador.

Mas centrando-nos na questão da obtenção de prova em ambiente digital, antes de mais cumpre dizer que a Lei n.º 109/2009, de 15 de Setembro (que aprovou a Lei do Cibercrime) estabelece as disposições processuais relativa à recolha da prova em suporte electrónico, que deve ser conjugado com o previsto no art. 187.º, 188.º e 190.º do CPP, bem como a Lei n.º 32/2008, de 17 de Julho [18] (transpõe para a ordem jurídica interna a Directiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações) e a Lei 41/2004, de 18 de Agosto[19] (transpõe para a ordem jurídica nacional a Directiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12

[17] Introdução ao cyberbullying, pag. 8 e 9, consultado em http://www.cybertraining-project.org/book/printerfriendly/pt/Module%203%20-%20Portuguese.pdf.
[18] Que pode ser consultado em http://dre.pt/pdf1sdip/2008/07/13700/0445404458.PDF.

de Julho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas).

Atentemos em duas questões (entre outras) que têm levantado celeuma na jurisprudência.

A primeira prende-se em apurar se será possível por exemplo obter dados de tráfego ou de conteúdo quando está em causa um crime de difamação[20]. A segunda se a apreensão de uma mensagem de correio electrónico aberta fica submetido ao regime da apreensão de correspondência, ou se pelo contrário, deve ser "encarada" como prova documental e como tal passível de ser apreendido sem intervenção do juiz.

Analisemos alguns exemplos a propósito da primeira das questões decididas pela jurisprudência.

Crime de difamação, em que um médico fez uma denúncia contra terceiros, em virtude de em dois fóruns de conversação na internet terem sido proferidas expressões de cariz difamatório por três utilizadores. Foi então solicitada pela PJ a identificação dos referidos utilizadores de contas que participaram nos fóruns associados aos mencionados sites, com recurso a endereços de IP pertencentes a ISP's (internet service provider) sedeados em Portugal. Ainda em ordem a apurar o registo da realização das mencionadas intervenções, bem como a identificação dos respectivos autores, a PJ solicitou à Portugal Telecom a identificação dos Protocolos de Internet, com referência ao grupo data-hora, associados à colocação dos comentários no site X, bem como relativos à criação das contas referidas, assim como a identificação e contacto do responsável do fórum. Foi recusada a informação pela Portugal Telecom invocando o sigilo das telecomunicações.

Não obstante ser um crime de difamação, não expressamente previsto no catálogo do art. 187.º do CPP, será admissível autorizar o fornecimento de tais dados?

No ac. da RG, de 12.04.2010, processo n.º 1341/08.4TAVCT, consultado em www.dgsi, que analisou decidiu que *"Tendo no decurso do inquérito sido participado contra desconhecidos um crime de difamação agravada praticada através da Internet, e visando-se apurar dados de*

[19] Que pode ser consultado em http://dre.pt/pdf1sdip/2004/08/194A00/52415245.pdf.

tráfego de comunicações electrónicas (dados relativos às ligações do computador de um agente a um fornecedor de serviço de acesso à Internet), cujo acesso só é possível, nos termos legais, através de autorização do JIC, o regime aplicável é o prevenido no artº 187º, por remessa do artº 189º do C.P.Penal". E *"tal conclusão decorre exactamente da equiparação do crime de difamação ao crime de injúria, sob pena de, doutra forma, a prática dum crime de injúrias por via telemática só ser possível aquando duma videoconferência, situação completamente restritiva e injustificada quando num qualquer crime de difamação em causa estão precisamente os mesmos bens jurídicos que no crime de injúrias. O correio electrónico nunca seria possível de interceptar e gravar porque, por natureza, lhe falta a "presencialidade", elemento crucial para a verificação do mencionado crime de injúrias"*. E sendo assim, decidiu-se que *"deverá o Mº juiz a quo (JIC) solicitar à PT os elementos pretendidos pelo MPº, após o que, ante uma eventual escusa, haverá de ser accionado mecanismo procedimental previsto no artº 135º, n.ºs 2 e 3 do CPP."*

Também no ac. da RL, processo n.º 3142/09.3PBFUN-A.L1-5, 18.01.2011, consultado em www.dgsi.pt, num caso de crime de difamação, através da colocação de um "post" num blog, e pretendendo-se apurar a identificação completa, morada e endereço de correio electrónico do titular de determinado blog, bem como o IP de criação desse blog e o IP onde foi efectuado determinado "post" (elementos essenciais para prosseguir a investigação), embora entendendo tratarem-se de dados base, para o caso de se entender ser dados de tráfego, poderia igualmente ser solicitado pelo JI, considerando *"que o bem jurídico protegido pelos crimes de injúria e difamação é o mesmo, deve entender-se que este é abrangido pela al.e, do nº1, do art.187, CPP, integrando, assim, os crimes de "catálogo" referidos nesse preceito";*

Em sentido contrário, entendendo que não é possível autorizar a informação sobre dados de tráfego ou conteúdo relativamente ao crime de difamação por ex. ac. da R.E., processo n.º 12/12.1YREVR, 5 de Junho de 2012, consultado em www.dgsi.pt, sumariando-se que *"1.Estando em causa investigação por crime de difamação através da internet, não é admissível*

[20] A questão não se coloca quanto aos dados de base, que na fase de inquérito podem ser solicitados pelo MP, ao contrário dos dados de tráfego ou conteúdo, que apenas podem ser ordenados pelo JI, verificados os requisitos legais previstos no art. 187.º do CPP E na Lei n.º 109/2009, de 15 de Setembro (que aprovou a Lei do Cibercrime).

o acesso a dados de tráfego, por via de autorização judicial, dado que tal ilícito não consta, nem do catálogo previsto no art. 187.º do CPP, nem da definição de crime grave do art. 2.º, n.º 1, alínea g), da Lei n.º 32/2008, de 17.07. 2. O princípio da legalidade obsta a que, para esse efeito, se equipare ao crime de injúria incluído nesse catálogo.". Defende-se pois não ser possível uma interpretação extensiva desta norma por ser compressora de direitos individuais e excepcional. Entendeu-se neste acórdão serem dados de tráfego a informação relativa aos "dados do utilizador de IP 188.80.239.206, entre as 10h43m54s e as 10h4521s (GTM) do dia 21 de Janeiro de 2011." No mesmo sentido ac. da RE, proc. n.º 315/11.2PBPTG-A.E1, de 13.12.2012, "Estando em causa investigação por crime de difamação através da internet, não é admissível o acesso a dados de tráfego, por via de autorização judicial, dado que tal ilícito não consta, nem do catálogo previsto no art. 187.º do CPP, nem da definição de crime grave do art. 2.º, n.º 1, alínea g), da Lei n.º 32/2008, de 17.07."(caso em que o MP requereu ao abrigo do disposto nos arts. 2º, al. c) e 18º, nº 1, als. a) e b) e nºs 2 e 3 da Lei nº109/2009 de 15 de Setembro (Lei do Cibercrime), ao Juiz de Instrução que fosse solicitado a "Google Inc" as seguintes informações: Os elementos de identificação que foram indicados por quem criou o blogue com o endereço http://xxxxxblogspot.py; O endereço do IP da criação do blogue e correspondente grupo data/hora/fuso horário; Os endereços de IP e correspondentes grupos data/hora/fuso horário dos acessos ao blogue, ocorridos nos dias 24, 25 e 28 de Fevereiro de 2012; O endereço de correio electrónico associado ao blogue - Os endereços de IP e correspondentes grupos data/hora/fuso horário, dos últimos dez acessos à caixa de correio electrónica que se encontrar associada ao blogue, "esclarecer, que com excepção dos elementos, de identificação indicados sobre quem criou o blogue aqui em causa e, bem assim, o endereço do correio electrónico associado a esse mesmo blogue, os outros elementos pretendidos pelo MºPº, constituem dados de tráfego, enquanto aqueles são dados relativos à conexão à rede, vulgarmente designados por "dados de base"." (…) "Porém, não podendo, pelos motivos expostos, o crime de difamação, integrar o catálogo taxativo e fechado do nº1 do art.187º do CPP, aplicável por remissão do art.18º, nº1, al. b) da Lei do Cibercrime, o acesso e a recolha aos pretendidos dados de tráfego, é legalmente inadmissível. Convirá ainda realçar que o art.18º tem o seu campo de aplicação à intercepção de dados de conteúdo e/ou de tráfego, mas sempre no que respeita a diligência de intercepção da

comunicação em tempo real, ou seja, em transmissão, o que não é o caso em apreço, não tendo aplicação essa norma, enquanto a injunção prevista no art.14º respeita ao acesso mas de dados armazenados. Aliás, a Lei do Cibercrime assenta, não numa estruturação tripartida de dados como tradicionalmente, em dados de base, dados de tráfego e de conteúdo, mas sim numa separação dos momentos em que se dá a intromissão nos dados informáticos. Ainda assim, convirá examinar agora a questão na perspectiva isolada do pedido do MºPº no que concerne aos dados de base – elementos de identificação sobre quem criou o blogue e o endereço de correio electrónico associado ao blogue.Vejamos. Dispõe o art.11º, nº1, al. b) da mencionada Lei do Cibercrime que com excepção do disposto nos arts.18º e 19º, as disposições processuais previstas nesse capítulo aplicam-se a processos relativos a crimes cometidos por meio de sistema informático. Como já dissemos anteriormente está aqui em causa um crime de difamação cometido por meio de sistema informático, entendido este, na acepção da al.a) do art.2º da citada Lei do Cibercrime. Nos termos do disposto no art.14º, nº1 e 3 desse diploma, quando no decurso do processo se tome necessário à descoberta da verdade obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha a disponibilidade ou controlo desses dados que os comunique ao processo, sob pena de punição por desobediência, permitindo assim que essa ordem seja dada pelo Ministério Público, na fase inquérito, excluindo-se, no n.°4, dessa informação, quer os dados de conteúdo, quer os dados de tráfego, quando refere que pode ser ordenado a fornecedores de serviços "que comuniquem ao processo dados relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo". Ou seja, relativamente aos mencionados dados de base atrás referidos, o Mº Pº nesta fase de inquérito pode/deve, se entender necessários para a investigação em curso, sem intervenção do JI, solicitá-los directamente à entidade por ele referida, e se porventura esta se escusar a fornecer esses dados escudando-se no estatuído no art.182º do CPP, é que deverá então ser suscitado nos termos do art.135º do mesmo código o incidente de levantamento do sigilo invocado. Para finalizarmos, acresce ainda dizer, que no âmbito da citada Lei nº32/2008, de 17 de Julho, apesar dos dados de base se inserirem na categoria abstracta dos dados de tráfego, pois nela está consagrado que cabem na categoria de "dados necessários para encontrar e identificar a fonte de uma

comunicação" o nome e endereço do assinante ou do utilizador registado, bem como o nome e endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP, o código de identificação de utilizador ou o número de telefone que estava atribuído no momento da comunicação, o certo é que não sendo o crime de difamação, "crime grave" nos termos definidos na al. g) do art.2º da Lei nº32/2008, de 17 de Julho, também não seria admissível a solicitação feita pelo JI, a requerimento daquele, para transmissão no âmbito da investigação daquele crime, de qualquer um dos dados da pretensão formulada pelo MºPº no seu requerimento. Nesta conformidade e sem mais desenvolvidas considerações por desnecessárias, impôs-se negar provimento ao recurso, mantendo-se o despacho recorrido).

A este propósito diga-se, é pois fulcral existir uma correcta distinção entre dados de base e dados de tráfego ou conteúdo, já que os primeiros podem ser solicitados pelo MP, já os segundos sempre precisarão da autorização de um JI.

A propósito desta destrinça veja-se, entre outros, Ac. da RE que considerou ser dados de tráfego a informação relativa aos "dados do utilizador de IP 188.80.239.206, entre as 10h43m54s e as 10h4521s (GTM) do dia 21 de Janeiro de 2011." Já o ac. da RE, de 7.12.2012, processo n.º 72/11.2DFTR-A.E1, consultado em www.dgsi.pt, entendeu num caso em que se investigava a prática de um crime de difamação cometido através de um comentário anónimo inserido num blogue, que a solicitação de informação junto do fornecedor das comunicações electrónicas nacionais, a PT, da identificação completa, morada e endereço de correio electrónico do comentador, se tratam dados de base, razão pelo qual não seria aplicável os artigos 187.º a 190.º do CPP, já que estas "normas, como do respectivo teor literal resulta, têm em vista exclusivamente a intercepção e a gravação de conversações ou comunicações telefónicas e a localização celular ou registo da realização de conversações ou comunicações". Concluiu pois que se devia ordenar à PT o envio de tais informações, sendo que caso fosse invocado o segredo profissional, oportunamente suscitar-se-ia o art. 135.º, n.º 3 do CPP.

O ac. da RE, processo n.º 1276/09.3TAPTM-B.E1, de 27.01.2011, consultado em www.dgsi.pt faz uma distinção entre a identificação do utilizador de um IP estático ou de um IP dinâmico, decidindo-se que «Perante um IP (Internet Protocol) dinâmico, a obtenção de dados

relativos à identificação do seu utilizador só pode ser facultada mediante ordem prévia do juiz, porquanto tal operação pressupõe uma prévia consulta de dados de tráfego»[21]. Trata-se de uma situação em que num site após a colocação de uma notícia terão sido feitos comentários difamatórios, apurados os IP's (Internet Protocol) usados pelos autores de comentários assinados com os nicknames previamente colhidos do site em questão e, bem assim, os respectivos ISP (Internet Service Provider), foi solicitado às diversas operadoras de telecomunicações a identificação dos titulares/utilizadores, bem como as moradas completas dos mesmos pelo MP. Respondeu a Sonaecom que "a informação acerca da identificação do utilizador do IP numa determinada data/hora constitui, neste caso, dado de tráfego, uma vez que o IP é dinâmico.", pelo que solicitou autorização do JI. Como ali se escreve "o IP cuja identificação de utilizador se pretende é dinâmico, isto é, trata-se de um número, ou melhor, de uma sequência de números composta de 32 bits (4 grupos de 8 bits), que é dado a um computador sempre que ele se liga à rede, mas que muda de cada vez que é efectuada uma conexão. Isto é: se um determinado utilizador se ligar à internet neste momento, é-lhe atribuído um determinado endereço de IP; se terminar a sua ligação e a retomar dentro de alguns momentos, ser-lhe-á atribuído um IP distinto. Basicamente, é como se o ISP (Internet Service Provider) fizesse a gestão dos IP's que tem disponíveis e que, a cada momento, atribuísse um deles, nesse momento livre, a cada utilizador que pretenda efectuar uma ligação. Distintamente, um IP estático (ou fixo) é um número dado permanentemente a um computador, de tal forma que sempre que o utilizador se ligar à internet, usará sempre o mesmo IP."

Salienta pois tal acórdão tratarem-se de situações distintas, pois quando o IP é estático "o acesso à identificação e morada do seu utilizador se pode fazer sem recurso a qualquer dado de

[21] Para a distinção entre dados de base, de tráfego e de conteúdo e citado nesse acórdão Armando Veiga e Benjamim Silva Rodrigues, "A monitorização de dados pessoais de tráfego nas comunicações electrónicas", http://raizesjuridicas.up.edu.br/arquivos/raizesjuridicas/Revista%205/ a%20monitorizaçã o.pdf, "os dados de base consistem nos elementos fornecidos pelo utilizador à empresa que fornece o acesso à rede e ou ao serviço de comunicações electrónicas, v.g., nome, morada, e os dados que aquela empresa fornece, em sentido inverso, ao utilizador para efeito de interligação à rede e ou ao serviço de comunicações electrónicas, v.g., número de acesso, nome de utilizador, password. Os dados de tráfego dizem respeito aos elementos funcionais da comunicação e permitem o envio da comunicação através de uma rede de comunicações electrónicas, v.g., data e hora do início da sessão (log in) e do fim (log off) da ligação ao serviço de acesso à Internet, endereço de IP atribuído pelo operador,

tráfego, recorrendo apenas aos elementos constantes em arquivo e relativos aos dados fornecidos pelo cliente aquando da celebração do contrato com a empresa fornecedora do acesso. São dados existentes a montante das comunicações propriamente ditas, analisáveis e consultáveis sem recurso à própria comunicação. Quando, porém, estamos perante um IP dinâmico, a obtenção de dados relativos à identificação do seu utilizador não pode ser feita sem, simultaneamente, se proceder a uma consulta de dados de tráfego. Quer dizer: há que saber não apenas a identificação de um determinado utilizador constante de um qualquer contrato mas, essencialmente, quem, em determinado momento, era o utilizador de determinado IP." Assim sendo, seriam dados que necessitariam de autorização do JI, e em caso de invocação do segredo das comunicações, acionar o incidente da quebra do mesmo.

Outra questão discutida na jurisprudência prende-se com a valoração em processo penal da leitura de mensagens de telemóvel ou correio electrónico.

As mensagens de telemóvel ou correio electrónico permitem distinguir três situações. Se tiverem em trânsito aplica-se as regras das intercepções telefónicas, devendo ser validadas e autorizadas por um juiz. Se recebidas e não abertas são aplicadas as normas de apreensão de correspondência. Se abertas trata-se de prova documental, não competindo ao juiz validá-las, mas sim ao MP.

A este propósito e neste sentido ac. da RP, de 27.01.2010 , em cujo sumário se escreve, "(…) II - A mensagem via telemóvel já recebida deverá ter o mesmo tratamento da correspondência escrita, que circula através do tradicional sistema postal: recebida mas ainda não aberta pelo destinatário, aplicar-se-á, à respectiva apreensão, o estabelecido no artigo 179º do CPP; recebida, aberta e guardada pelo destinatário, já não beneficiará do regime de protecção da reserva da correspondência e das comunicações, podendo ser apreendida para valer como mero documento escrito". Com a mesma posição, Ac. R. Lisboa, de 15/07/08, Proc. nº 3453/2008: "na sua essência, a mensagem mantida em suporte digital depois de recebida e lida terá a mesma protecção da carta em papel que tenha sido recebida pelo correio e que foi aberta e guardada em arquivo pessoal". Note-se a presunção a que alude o Ac. da RC, de 29/03/06, Proc. nº 607/06: "a

volume de dados transmitidos, entre outros. Os dados de conteúdo baseiam-se no conteúdo da comunicação

mensagem recebida em telemóvel e guardada na respectiva memória, atenta a natureza e finalidade do aparelho, é de presumir, segundo as regras da experiência comum e da natureza das coisas que, uma vez recebida, foi lida pelo seu destinatário."

Lidas e abertas as mensagens de correio electrónico ou telemóvel (mesmo que de voz) deverá equiparar-se à situação das "cartas abertas", e guardadas em arquivo, sujeitas ao regime normal de apreensão de documentos. "As mensagens recebidas em telemóvel e mantidas em suporte digital, depois de recebidas e lidas, não têm mais protecção do que as cartas recebidas, abertas e guardadas pelos seus destinatários." (…) "se a mensagem foi de voz, não sendo ilícita, pode ser valorada, desde que transcrita nos autos (199.º, 167.º e 101.º, n.º 2 do CPP)" - ac. da RG, de 24.01.2011 .

Em sentido contrário ac. da RG, proc. 735/10.0GAPTL – A.G1, de 29.03.2011: "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."

6. Responsabilidade civil. Da prova ilícita no processo civil. De novo da teoria da proporcionalidade. Da migração da prova obtida em processo criminal para o processo disciplinar e para o processo civil.

Conforme fomos abordando, através da internet poderão praticar-se ilícitos criminais, civilísticos ou de cariz disciplinar, cujos pressupostos para despoletar a responsabilidade civil, criminal ou disciplinar são iguais aos ilícitos não praticados por meio da internet.

Ora, nomeadamente a nível do processo civil poderá colocar-se a questão de apurar se determinado tipo de prova obtida **ilicitamente** em ambiente digital (a companheira que lê indevidamente o mail do companheiro, a colega de trabalho que acede ao mail de outrem, onde para além de se deparar que tem sido alvo de difamação, logra apurar que a trabalhadora cujo

transmitida pela rede de comunicações electrónicas".

mail é invadido tem subtraído dinheiro à empresa ou, por exemplo, a colocação abusiva de programa no computador de outrem que lhe dá acesso aos seus documentos, permitindo-lhe comprovar as ameaças que tem sido alvo), poderá ser valorado num processo civil.

A segunda questão é se **obtida de forma válida em processo criminal prova em ambiente digital a mesma poderá ser valorada num processo civil.**

A nível da valoração de prova ilícita em processo civil, chamamos aqui à colação um acórdão, cujos considerandos são igualmente aplicáveis se a prova em causa tivesse sido obtida digitalmente, por via da internet (através por ex. de intercepção ilegal em chat de conversação ou leitura indevida de correio electrónico), e que aborda esta problemática.

Sumariou-se assim, no ac. da RL, processo n.º 1107/2004-6, de 3.06.2004, consultado em www.dgsi.pt:

" A ilicitude na obtenção de determinados meios de prova não conduz necessariamente à sua inadmissibilidade, mas também não implica a garantia do seu aproveitamento. Numa acção em que se pretende a indemnização decorrente de ofensas ao bom nome imputadas ao ex-cônjuge é pertinente a junção de uma gravação áudio referente a uma conversa mantida entre a R. e outra pessoa mediante a qual o autor pretende demonstrar a inveracidade de alegadas cenas de violência domésticas que a R. lhe imputou. Ao invés, por falta de pertinência relativamente ao objecto da acção de indemnização, deve ser indeferida a junção de uma gravação vídeo reportando factos integrantes de uma situação de adultério em que foi interveniente a R., ainda que a gravação tenha sido feita através de um sistema instalado na casa de morada do ex-casal com o conhecimento de ambos. A tal junção obstaria ainda o facto de a gravação abarcar não apenas a pessoa do ex-cônjuge, mas ainda uma terceira pessoa."

Trata-se de um processo em que o ex-marido peticiona os danos patrimoniais e não patrimoniais que a conduta da ex-mulher lhe causou, e em que juntou uma cassete áudio e vídeo com gravações de voz e imagem da ex-cônjuge. No caso a veracidade das palavras e da imagem eram admitidas pela R., tratando-se de gravações particulares, colocando-se a tónica na sua admissibilidade, licitude e ilicitude. Relembrou-se neste arresto as três teses sobre a admissibilidade da prova ilícita: uma tese ampla que defende a admissibilidade sem restrições de tal prova tendo em vista a descoberta da verdade material, uma intermédia *"caso a caso,*

mediante a apreciação das circunstâncias concretas e consoante os valores em jogo" (João Abrantes, Rev. Jurídica, nº 7, Julho/Setembro 1986, AAFDL, pags. 15/16) e uma restrita, vedando em qualquer caso a utilização de prova ilícita (Marcelo Caetano in Manuel de Direito Administrativo, 9ªed., TII, Lisboa, 1972, pag. 827 e Parecer nº 12/66, de 13/5/1966, da PGR, in BMJ 163º-137).

Optou-se aqui, na esteira do defendido por Salazar Casanova (Salazar Casanova, Provas Ilícitas em Processo Civil, Sobre a Admissibilidade e Valoração de Meios de Prova Obtidos por Particulares", Março de 2003, publicação da Biblioteca do TRL, pag. 53), *"que a orientação que admite a prova com algumas restrições, consoante o caso concreto e os interesses em conflito, independentemente de se aceitar com maior ou menor reserva a aplicação analógica do art. 32º da Constituição, é a mais razoável e a que melhor se ajusta aos princípios e normas em vigor, sem olvidar, obviamente, a relevância que a prova, cuja junção se pretende, tem no caso concreto. Ou seja, a ilicitude na obtenção de determinado meios de prova não conduz necessariamente à proibição da sua admissibilidade, mas também não implica, a garantia do seu aproveitamento. De facto, como conclui Salazar Casanova, uma protecção sem limites a certos direitos fundamentais "deixaria em muitos casos sem efectiva tutela o próprio direito de acção" e os direitos fundamentais poderiam vir a ser invocados em claro abuso de direito."*

E antes de avançar com a análise do caso concreto, abre-se um parêntesis para afirmarmos a nossa concordância, como já salientamos, com a tese intermédia, entendendo-se que o julgador deverá ponderar a "dimensão" do processo, os valores em jogo, a necessidade da prova, a possibilidade da prova sem estes meios, os direitos "em jogo", para depois, decidir-se, ou não, pela valoração de tal prova.

É a igualmente a tese maioritária defendida no Brasil e denominada tese da proporcionalidade, e que inclusivamente consta do projecto de lei do novo código de processo civil brasileiro [22] (redacção original do projeto de Lei do Senado n.º 166, de 2010):

[22] Consulte-se http://www.senado.gov.br/senado/novocpc/pdf/anteprojeto.pdf e http://www.senado.gov.br/atividade/materia/getPDF.asp?t=84496.

"Art. 257. As partes têm direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar fatos em que se funda a ação ou a defesa e influir eficazmente na livre convicção do juiz.

Parágrafo único. A inadmissibilidade das provas obtidas por meio ilícito será apreciada pelo juiz à luz da ponderação dos princípios e dos direitos fundamentais envolvidos."

Mas retomando o caso concreto, e no que se reporta à cassete de áudio, considerou-se justificada a junção aos autos tendo em vista o A. provar da inveracidade de situações de violência doméstica que a R. descreveu em livro que publicou, sendo que essa gravação consistia numa entrevista que serviu de base ao livro e que o A. pretendia demonstrar que não tinham correspondência com o que foi escrito, gravação essa que a R. invocava que não era para ser de conhecimento público. Admitiu-se a mesma por ser considerada uma prova fundamental para demonstrar a inveracidade do escrito no livro, para além de que a divulgação visava um fim específico que era o exercício do direito à prova, direito este com assento constitucional. Entendeu-se, pois, que a *"ponderação de interesses justifica(-se) a divulgação em tribunal dos relatos feitos pela aqui Agravante e que constam da gravação"*.

No que se reporta à cassete de vídeo o A. pretendia demonstrar o adultério praticado pela sua ex-cônjuge com uma gravação que contém imagens captadas por um sistema de segurança existente na casa da Agravante, sendo que a R. admitia ter conhecimento da gravação, mas que a mesma se destinava a fins de segurança e não a divulgação das mesmas.

Quanto a esta o tribunal afastou a sua admissibilidade, por não sequer estar em causa o direito à prova, já que visando a acção provar a inveracidade de cenas de violência doméstica, o adultério praticado em casa de morada de família relevaria para a acção de divórcio e a introdução de terceiros em casa, se colocasse em causa a segurança dos filhos, para a acção de regulação de poder paternal, para além de se ter pressuposto que a terceira pessoa, "o amante"m desconheceria essa gravação, pelo que seria uma inadmissível intromissão na vida privada.

De todo o modo, o que há que extrair desta jurisprudência é a necessidade de uma ponderação de valores e interesses, para aferir se é proporcional, não excessivo e adequado valorar a prova, mesmo que ilícita.

Como se escreveu na conclusão do acórdão:

Em suma,

"No processo civil a regra continua a ser a afirmação do princípio dispositivo, pelo que, como se referiu, uma protecção sem limites de certos direitos fundamentais, como o direito à imagem ou à palavra que não podem deixar de se considerar como relativos na sua oponibilidade à produção de prova, ao direito à prova, seria vista como uma desprotecção dos meios de prova mais valiosos a favor dos mais falíveis.

Por isso, mesmo quando estão em causa certos direitos fundamentais, não pode pretender-se uma transposição automática do disposto no art. 32º da Constituição, respeitante às garantias do processo criminal, para o processo civil.

Não decorrendo da lei a proibição absoluta de admissibilidade da prova, é em função das circunstâncias como foi obtida e da relevância que possa ter, que será ou não admitida pelo Tribunal."

Ora, como já referimos esta abordagem às teses sobre a admissibilidade da prova ilícita em processo civil aplica-se mutatis mutandis à prova digital (imagine-se uma situação de invasão do correio electrónico ou intercepção ilegal de conversa via net, que não foi considerado válida em processo crime de homicídio, mas em que o familiar da vítima interpõe acção de indemnização contra o alegado homicida, apresentando para comprovar a conduta ilícita e culposa do alegado homicida, tal prova).

Questão diversa é se quando a prova digital é obtida em processo penal, com respeito dos normativos processuais, e ali validamente usada para a condenação do arguido, poderá ser usada em processo civil, por exemplo numa situação de acção de indemnização interposta pelo ofendido em tribunal civil contra o arguido ou contra terceiro que garante a indemnização, como seja uma seguradora.

Estamos aqui perante uma situação de **migração de prova obtida em processo criminal, para o processo civil**, sendo que a mesma questão se coloca sobre a utilização de tal prova em outros processos como seja o laboral, administrativo ou o disciplinar.

Tal tem sido analisado essencialmente a nível das escutas telefónicas, mas como dissemos, será aplicável à prova criminal obtida através de intercepção em ambiente digital ou mediante a apreensão de correio electrónico, por exemplo.

Vejamos, contudo, uma decisão relativa à possibilidade de valorar prova criminal em sede disciplinar.

Assim, no ac. do S.T.A., Processo n.º 0878/08, de 30.10.2008, consultado em www.dgsi.pt, decidiu-se:

"III – A transposição das escutas telefónicas legalmente obtidas um processo crime para o processo disciplinar instaurado contra o arguido e a sua manutenção e valoração neste processo é ilegal porque, nos termos do citado art.° 187.° do CPP, as mesmas só podem ser colhidas e utilizadas quando esteja em causa a investigação e punição de um dos crimes previstos no seu n.° 1."

Neste processo estava em causa a intimação para protecção de direitos, liberdades e garantias, pedindo-se que a Federação Portuguesa de Futebol desentranhasse de um processo disciplinar onde o requerente, presidente de um clube de futebol, era arguido, certidões passadas pelo DIAP pelos Serviços do Ministério Público, constituídas por transcrições das conversas telefónicas que foram interceptadas no âmbito de processos-crime onde estava indiciado por crimes de corrupção desportiva e que foram arquivados. No processo disciplinar estava acusado da prática de infracção disciplinar de corrupção na forma tentada p. e p. pelo art.º 100.º, n.º 1 e 3 do Regulamento Disciplinar da LPFP. A questão a apurar era de saber se a transposição e a sua posterior valoração para o processo disciplinar onde o Requerente foi punido das escutas licitamente efectuadas nos processos crimes instaurados contra ele foi legal.

Nesse acórdão decidiu-se pelo menos relativamente a escutas que os mesmos não poderão servir de prova em qualquer outro processo, escrevendo-se *"o recurso a escutas telefónicas só é legal quando elas se destinem a obter prova para crimes que constem do citado normativo o que quer dizer que em todos os demais processos onde se investigue a prática de outros ilícitos, quer de natureza penal quer de outra natureza, designadamente disciplinar, o recurso a esse meio de obtenção de prova é ilegal e, consequentemente, é ilegal a sua utilização e valoração. Por outro*

lado, o mesmo preceito é claro ao proibir a transposição da gravação de conversas ou comunicações de um processo penal para outro e a sua posterior utilização se este último respeitar a crime que não admita escutas telefónicas (vd. n.º 7 do transcrito art.º 187.º do CPP), o que só pode querer significar que a proibição de obtenção da prova por meio de escutas telefónicas abrange todos os processos que não os respeitantes aos crimes de catálogo e, por maioria de razão, os processos de natureza não penal como são os processos disciplinares. Com efeito, se os comportamentos sociais perseguidos nestes processos são menos graves e menos danosos do que os perseguidos nos processos penais, seria de todo incompreensível que se aceitasse a utilização das escutas telefónicas naqueles processos quando as mesmas eram proibidas na grande maioria dos processos-crime."

Saliente-se, contudo, o voto vencido no sentido de que o está aqui em causa á a admissibilidade da divulgação das escutas, designadamente com a junção de certidões de transcrições a outros processos, como por exemplo de índole disciplinar, pelo que é a autoridade judiciária que remete as certidões que deve a ou sindicar a legalidade e proporcionalidade da divulgação que o envio dessas certidões implica.

Vejamos.

No processo penal inexiste qualquer norma que discipline tal matéria, sendo que em 2007 foi introduzida uma norma relativa aos conhecimentos fortuitos, mas que tem como escopo fixar os pressupostos de admissibilidade de valoração de intercepção, em outros processos criminais[23].

No que se reporta ao valor extraprocessual das provas no processo civil rege o art. 522.º do CPC.

No entanto, cremos que tal norma está pensada para as provas obtidas em outro processo civil, e não em processo criminal. Entendemos, contudo, que perante esta lacuna, deverá atender-se aos princípios ali vertidos, pelo que na nossa óptica será de valorar tal prova como documento, desde que as partes (no processo civil) tenham intervindo no processo criminal, já que as

[23] Dispõe o art. 187.º, n.º 7 do CPP, que a "gravação de conversações ou comunicações só pode ser utilizada em outro processo, em curso ou a instaurar, se tiver resultado de intercepção de meio de comunicação utilizado por pessoa referida no n.º 4 e na medida em que for indispensável à prova de crime previsto no n.º 1."

garantias conferidas neste processo não são inferiores ao processo civil, pelo contrário. Cremos que se trata de norma criadora, admissível ao abrigo do art. 9.º do CC, e que se coaduna e é coerente com aquela norma processual, bebendo dos fundamentos que lhe subjazem.

Sobre esta matéria de denominada "prova emprestada" na doutrina brasileira, e sobre as problemáticas ali suscitadas, veja-se, entre outros, o escrito [24] "*DAS PROVAS ILÍCITAS NO ORDENAMENTO JURÍDICO BRASILEIRO O PRINCÍPIO DA PROPORCIONALIDADE FRENTE ÀS PROVAS ILICITAMENTE OBTIDAS",* onde se escreveu a propósito da utilização da prova colhida mediante interceptação telefónica no processo civil: "*Questão relevante diz respeito à possibilidade ou não de utilização da prova colhida da interceptação telefônica no processo civil por meio da denominada prova emprestada. Em primeiro lugar, é forçoso reconhecer que o juiz da área civil não possui competência para autorizar o procedimento de intercepção, porque tal atribuição compete exclusivamente ao juiz criminal(...) A prova emprestada é aquela produzida num processo e transportada para outro, no intento de surtir efeitos jurídicos, sendo considerada pela doutrina brasileira como prova documental no plano formal, porém, não perdendo a natureza originária. Concluindo: a prova emprestada, formalmente, obedece às prescrições legais, para a prova documental, por ser trazida aos autos mediante um meio gráfico de reprodução, um documento; quanto à essência, conserva a natureza jurídica primitiva e será avaliada e considerada segundo as normas que regem tal natureza. Quanto aos efeitos, valor e avaliação, a prova emprestada possui quatro princípios norteadores que precisam ser observados conjuntamente: o primeiro é que ela tenha sido produzida em processo formado pelas mesmas partes ou, pelo menos, naquela ação judicial em que uma das partes suportou seus efeitos; o segundo princípio exige que na demanda anterior e na qual era primitivamente destinada, tenham sido observados todos os aspectos legais atinentes a sua natureza; outro requisito afirma que os fatos necessitam semelhança e, por último, que no processo o qual foi transportada, devem ser cumpridos os comandos legais acerca da prova documental. Nelson Nery Júnior é favorável à utilização da prova colhida da interceptação telefônica no processo civil, mediante prova emprestada, conforme se depreende do seu*

pensamento, in verbis: A dúvida existirá quando se pretender utilizar, no processo civil, como prova emprestada, essa prova obtida licitamente. Sendo norma de exceção, o disposto no inciso XII do artigo 5º da CF deve ser interpretado restritivamente. Quer isto dizer que somente o juiz criminal pode autorizar a interceptação telefônica, quando ocorrerem as hipóteses previstas na Constituição Federal. O juiz do cível não pode determinar escuta telefônica para formar prova direta no processo civil. Entretanto, entendemos ser admissível a produção da prova obtida licitamente (porque autorizada pela CF) para a investigação criminal ou instrução processual penal, como prova emprestada no processo civil. A natureza da causa civil é irrelevante para a admissão da prova. Desde que a escuta tenha sido determinada para servir de prova direta na esfera criminal, pode essa prova ser emprestada ao processo civil. Outro aspecto confirmador do posicionamento do aludido jurista é que tendo ocorrido a quebra do sigilo, não há que se falar mais em preservação da intimidade do interlocutor da comunicação telefônica. Entretanto, existem doutrinadores discordantes do ensinamento adotado por Nelson Nery Júnior, defendendo que, como a finalidade da interceptação telefônica restringe-se à investigação criminal e à instrução processual penal, somente neste âmbito pode a mesma ser utilizada. E poderia a prova obtida dentro de uma investigação criminal ou instrução penal ser utilizada em outro processo (civil, administrativo, constitucional etc.)? Pode haver prova emprestada nessa hipótese? Nelson Nery Júnior responde afirmativamente. Nosso pensamento, no entanto, é divergente. O legislador constitucional ao delimitar a finalidade da interceptação telefônica (criminal) já estava ponderando valores, sopesando interesses. Nisso reside também o princípio da proporcionalidade. Segundo a imagem do legislador, justifica-se sacrificar o direito à intimidade para uma investigação ou processo criminal, não civil. Isso tem por base os valores envolvidos num e noutro processo. Não se pode esquecer que a proporcionalidade está presente (deve estar, ao menos) na atividade do legislador (feitura da lei), do Juiz (determinação da medida) e do executor (que não pode abusar). Mais uma vez divide-se a doutrina brasileira em duas correntes, conforme exposto. O certo é que a admissibilidade da prova no processo civil

[24] Consultado em http://www.pge.ac.gov.br/site/arquivos/bibliotecavirtual/revistas/revista03/DAS_pROVASIlicitas.pdf.

dependerá do entendimento do magistrado, que se filiará a uma das defensáveis posições doutrinárias."

Ainda mais controverso será a valoração de tal prova "emprestada" em processo disciplinar, por se tratar se processo sancionatório (e que foi analisado no acórdão acima citado), sendo nosso entendimento que a aproveitabilidade de prova de intercepções em outros processos sancionatórios só é admissível nos casos previstos no processo penal para os conhecimentos fortuitos, ou seja, apenas em outro processo-crime, estando em causa crime do catálogo.

7. Filmagens, fotografias e gravações colocadas na internet vs reserva da privada e direito à imagem. Brevíssimos apontamentos sobre a responsabilidade do provedor de serviços na Internet.

a) As questões da privacidade, imagem, reserva da vida privada e o Google street view.

A este propósito comecemos com uma situação bastante actual que se prende com o Google street view, funcionalidade que permita ter conhecimento visual de várias ruas. Sucede, contudo, que tal empresa utiliza veículos com aparelhos fotográficos, captando a imagem de várias pessoas sem o seu consentimento e colocando as imagens acessíveis na internet.

Os problemas relacionados com a violação da privacidade do Google street view têm sido recorrentes desde o seu lançamento.

O Street View, é um programa que disponibiliza fotos interactivas e a 360 graus das ruas das grandes cidades, foi lançado em 2009 no Reino Unido, após ter sido lançado pela primeira vez em Maio de 2007 nos Estados Unidos.

Mas apenas 24 horas após o seu lançamento, a Google teve de retirar várias imagens consideradas embaraçosas, como a de um homem a sair de uma sex-shop no Soho, bairro de luxo em Londres.[25]

Também os suíços consideram que a empresa norte-americana não está a respeitar as condições de privacidade fixadas. Em apenas uma semana de funcionamento na Suíça, o "Street

[25] Notícia consultada em http://aeiou.visao.pt/street-view-do-google-poe-em-causa-a-vida-privada=f501065).

View" recebeu 300 reclamações. O Comissariado Federal de Protecção de Dados da Suíça exigiu que a empresa norte-americana Google, retirasse imediatamente o serviço "Street View" que abrange também aquele país, considerando que atenta contra a vida privada dos seus habitantes.

Argumenta-se que vários rostos e matrículas não foram adequadamente disfarçados. Segundo adianta o jornal brasileiro "A Folha", foram recebidas 300 queixas, tanto de particulares, como de empresas e repartições públicas, pedindo que os rostos capturados pelas máquinas da Google sejam desfigurados ou as imagens eliminadas[26].

Também na Bélgica se investiga se a Google violou a privacidade de moradores com Street View. A procuradoria belga investiga a captação de dados pessoais pelo Google durante a criação de seu arquivo de fotos de ruas "Street View". O objetivo é determinar se a empresa cometeu alguma infração contra a proteção da vida privada.

Para além da captação de imagens outra invasão da privacidade se tem questionado. É que os automóveis do Google, que percorreram as ruas de todo o mundo para construir esse aplicativo, podem ter captado e-mails e outras informações pessoais enviadas por meio de redes sem fios não protegidas por senhas[27].

Em Portugal existiu pelo menos notícia de uma acção motivada por tal circunstância. Foi interposta queixa-crime por fotografia ilícita e devassa da vida privada, que deu entrada no DIAP (Departamento de Investigação e Acção Penal) e um pedido de indemnização civil, em que um casal surge na imagem, alegadamente sendo perceptível de quem se trata[28].

b) Colocação de imagens e filmagens de pessoa com notoriedade pública no youtube. O caso Cicarelli na jurisprudência brasileira. Publicação de imagens em jornais on-line. Responsabilidade dos prestadores intermediários de serviços na internet.

[26] Notícia consultada em http://www.jn.pt/PaginaInicial/Tecnologia/Interior.aspx?content_id=1342256.
[27] Notícia consultada em http://veja.abril.com.br/noticia/vida-digital/procuradoria-belga-investiga-se-google-violou-direito-privado-com-streetview.
[28] Notícia consultada em http://www.tvi24.iol.pt/sociedade/tvi24-processo-street-view-privacidade-casal-google/1085130-4071.html.

Outras das situações que têm colocado questões sobre a violação da privacidade prende-se com a colocação de vídeos e imagens no youtube (ou em outras páginas na internet), principalmente de pessoas com notoriedade.

No Brasil, tem sido recorrentes acções interpostas contra esta empresa para que sejam retirados vídeos considerados violadores da reserva da vida privada.

Destacamos aqui o "caso Cicarelli", uma modelo brasileira e apresentadora de TV, que em praias do sul de Espanha, é filmada por um paparazzi a namorar no mar com o seu companheiro, que depois coloca tal vídeo no youtube.

Assim em acção interposta, entre outros, contra o youtube (Ação inibitória fundada em violação do direito à imagem, privacidade e intimidade de pessoas), APELAÇÃO CÍVEL N° 556.090.4/4-00, foi decidido pelo Tribunal de Justiça do Estado de São Paulo[29] dar provimento para fazer cessar a divulgação dos filmes e fotografias em websites, por não ter ocorrido consentimento para a publicação – Interpretação do art. 461, do CPC e 12 e 21, do CC, preservada a multa diária de R$ 250.000,00, para inibir transgressão ao comando de abstenção.

Aqui a questão que se coloca é se o facto de ser em lugar público, legitimaria a captação de imagens, mesmo sem consentimento dos visados.

Nessa decisão brasileira cita-se JOAQUIM FELIPE SPADONI [Ação inibitória, 2a edição, RT, 2007, P. 104]: *"Não é porque os dois namoraram ou transaram na praia que se legaliza a exploração, na internet e outros meios, das cenas que não foram produzidas para deleite do publico (....) exatamente porque os autores da ação não deram consentimento para devasse de momentos íntimos."*

E escreve-se *"Os apelantes estão suportando violações não somente do direito à imagem, como da intimidade [leia-se vida privada] e convém colocar um fim a essas invasões. As cenas são de sexo, atividade mais íntima dos seres humanos. Ainda que as pessoas tenham errado e errare humanum est quando cederam aos impulsos dos desejos carnais em plena praia, a ingerência popular que se alardeou a partir da comercialização do vídeo produzido de forma ilícita pelo paparazzo espanhol, afronta o princípio de que a reserva da vida privada é absoluta,*

somente cedendo por intromissões lícitas. A notícia do fato escandaloso ainda pode ser admitida como lícita em homenagem da liberdade de informação e comunicação, o que não se dá com a incessante exibição do filme, como se fosse normal ou moralmente aceito a sua manutenção em sites de acesso livre. Há de ser o Judiciário intransigente quando em pauta a tutela da esfera íntima das pessoas que não autorizaram a gravação das cenas e a transmissão delas. É preciso eliminar a confusão que se faz do direito à vida privada, mesmo de pessoa célebre ou notória, com preservação do direito à reserva da intimidade." E essa decisão brasileira cita um jurista lusitano [MENEZES CORDEIRO, Tratado de Direito Civil Português, I, parte geral, Tomo III, Almedina, 2004, p. 211] admite que *a notoriedade de políticos e celebridades implica em restrição da privacidade e adverte: "nunca ao ponto de atingir as esferas secretas e íntima".*

A propósito da responsabilidade do dono do site pelo seu conteúdo, também se debruçou tal decisão escrevendo *"Embora seja duvidosa a responsabilidade do provedor de hospedagem sobre ilicitudes de conteúdo, quando desconhecidas, a responsabilidade é incontroversa quando toma conhecimento da ilicitude e deixa de atuar em prol da restauração do direito violado." (...)o controlador que tem conhecimento da natureza ilegal da informação tem o dever de tomar as medidas necessárias para preveni-la ou retirá-la do sistema, sob pena de ser responsabilizado. Essa exigência de conduta, no entanto, deve ser interpretada mais como uma obrigação de manter-se diligente, de tomar providências que sejam consideradas próprias para fazer cessar a publicação ilícita, do que o dever de intervir diretamente no conteúdo da página eletrônica hospedada em seu sistema".*

Pelo que concluiu que era dever do YOUTUBE "*promover, em trinta dias, medidas concretas de exclusão do vídeo do casal, dos links admitidos, advertindo e punindo, com exclusão de acesso de hospedagem, todos os usuários que desafiarem a determinação com a reinserção do filme, sob pena de pagamento de multa diária de R$ 250.000,00."*

[29] Consultado em https://esaj.tjsp.jus.br/cjsg/getArquivo.do;jsessionid=F0E8B0DC867344DC573A5D657079AFBE?cdAcordao=2701681&vlCaptcha=fUniD.

Em Portugal a responsabilidade dos provedores de serviço depende da verificação dos requisitos do Decreto-Lei n.º 7/2004, de 7 de Janeiro, alterado pelo Decreto-Lei n.º 62/2009[30], de 10 de Março, que transpôs para a ordem jurídica nacional a Directiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho de 2000 (DCE), instituindo assim o RJCE (Regime Jurídico do Comércio electrónico), que também determina que estes responderão, juntamente com aquele que colocou o conteúdo ilícito na internet, se tendo conhecimento da ilicitude do mesmo, não os removeram de forma diligente. Sem nos querendo alongar doutrinalmente neste temática, por não ser o escopo deste trabalho, dir-se-á que o princípio geral está previsto no art. 12.º do RJCE no sentido de que "Os prestadores intermediários de serviços em rede não estão sujeitos a uma obrigação geral de vigilância sobre as informações que transmitem ou armazenam ou de investigação de eventuais ilícitos praticados no seu âmbito", mas têm que cumprir determinados deveres (cuja omissão poderá determinar a sua responsabilização), previstos no art. 13.º do RJCE (De informar de imediato quando tiverem conhecimento de actividades ilícitas que se desenvolvam por via dos serviços que prestam; De satisfazer os pedidos de identificar os destinatários dos serviços com quem tenham acordos de armazenagem; De cumprir prontamente as determinações destinadas a prevenir ou pôr termo a uma infracção, nomeadamente no sentido de remover ou impossibilitar o acesso a uma informação; De fornecer listas de titulares de sítios que alberguem, quando lhes for pedido).

Resulta, pois, que não obstante não tenham um dever geral de vigilância, o conhecimento da ilicitude de um conteúdo impõe o dever de o remover, para que não mais seja disponibilizado, impedindo a perpetuação da ilicitude através do uso dos seus serviços.

Em Portugal, ainda sobre a ilicitude de captação de imagens em locais públicos e sua divulgação sem consentimento do visado, nomeadamente na internet, veja-se o seguintes acórdãos que têm aplicabibilidade no caso, por exemplo, de um jornal com edição on-line.

Assim, o ac. STJ de 24 de maio de 1989 (BMJ 386, 531) [nota 818 da obra de CAPELO DE SOUZA – O direito geral de personalidade, Coimbra Editora, 1995, p. 324]decidiu que *"age*

[30] Que podem ser consultados em dre.pt/pdf1s/2004/01/005A00/00700078.pdf e dre.pt/pdfgratis/2009/03/04800.pdf.

com culpa, praticando facto ilícito passível de responsabilidade civil nos termos dos art. 70 e 483 e segs. do Código Civil, o jornal que, sem o seu consentimento e não ela pessoa pública, fotografa determinada pessoa desnuda e publica essa fotografia numa das edições, não obstante o facto de a fotografia ter sido obtida quando a pessoa em causa se encontra quase completamente nua (em topless) na praia do Meco, considerada um dos locais onde o nudismo se pratica com mais intensidade, número e preferência, mesmo que se admita ser essa pessoa fervorosa adepta do nudismo".

Um outro mais recente em que foi publicada numa revista "cor-de-rosa" fotografias de uma actriz nacional conhecida em Portugal, quando estava na praia, juntamente com outros veraneantes, com um homem, fazendo-se capa de revista com tais imagens como sendo o "romance de verão" (ac. do STJ, processo n.º 4822/06.0TVLSB, de 17.12.2009, consultado em www.dgsi.pt).

Considerou-se que por aplicação do disposto no citado art. 335º do C. Civil, há que entender que a liberdade de expressão não pode (e não deve) atentar contra os direitos à reserva da intimidade da vida privada e à imagem, salvo quando estiver em causa um interesse público que se sobreponha àqueles e a divulgação seja feita de forma a não exceder o necessário a tal divulgação. Entendeu-se que apesar de estar num local público, as imagens não foram captadas estando a visada enquadrada no local público, já que se destacou a sua imagem no meio da multidão, sendo que o interesse visado era apenas o lucrativo, pelo que foi condenada a pagar uma indemnização à referida actriz.

8. Responsabilidade por burla informática bancária.

Existem infelizmente várias situações de intromissão no sistema informático de um utilizador, sendo que o autor do ilícito aproveita para fazer transferências bancárias no sistema home-banking.

Relativamente à responsabilidade criminal (burla informática) e civil (responsabilidade civil extra-contratual) do autor do ilícito dúvidas não existem.

Mais discutida tem sido a responsabilidade do Banco que disponibiliza ao cliente esse serviço de home-banking, através do qual este foi lesado.

A jurisprudência brasileira tem dado acolhimento a indemnizações dos clientes através do código de defesa do consumidor, enquadrando-se como um cumprimento defeituoso da prestação de serviços, presumindo a culpa do banco.

"AÇÃO DE INDENIZAÇÃO - INSTITUIÇÃO FINANCEIRA - FRAUDE - OPERAÇÕES BANCÁRIAS VIA INTERNET - RELAÇÃO DE CONSUMO - FALHA NA PRESTAÇÃO DO SERVIÇO - DANOS MORAIS - CONFIGURAÇÃO - 'QUANTUM'. A responsabilidade do fornecedor, em decorrência de falha na prestação do serviço, é objetiva, nos exatos termos do art. 14 do CDC, bem como do art. 927, parágrafo único, do CC/2002. O valor da reparação não deve constituir enriquecimento sem causa, mas deverá ser desestimulo à repetição da conduta danosa. Recurso não provido. 1.0105.03.080070-7/001(1) Relator: ROBERTO BORGES DE OLIVEIRA Data do Julgamento: 08/04/2008."

Socorre-se pois da responsabilidade objectiva prevista no art. 14 do Código de Defesa do Consumidor segundo o qual "O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos".

O "prestador de serviço (….) "há de responder pelos danos causados por defeitos verificados nessa prestação, independentemente de culpa, pois a responsabilidade decorre do só fato objetivo do serviço, e não da conduta subjetiva do agente" (STOCO, 2007, p. 142 STOCO, Rui. Tratado de Responsabilidade Civil: Doutrina e jurisprudência. São Paulo: Revista dos Tribunais. 2007.).

Claro está que se existir culpa do cliente, por exemplo se culposamente cede a senha, poderá excluir-se a responsabilidade do banco ou existir concorrência de culpas.

Contudo, a cedência de "senhas" aos hackers, iludidos por estes, só por si não eximem de responsabilidade o Banco. Na verdade, disponibilizando o banco um serviço a um cliente que lhe traz vantagens, nomeadamente de contenção de custos, deve arcar com os riscos daí inerentes, onde se incluem as intromissões por via de internet nos sistemas de homebanking. Estamos

perante um cumprimento defeituoso do contrato, que faz presumir a culpa do banco. Aliás, se estivermos perante relação de consumo, na acepção que consta do Código de Defesa do Consumidor, este diploma também realça a obrigação do fornecedor do serviço o prestar sem quaisquer defeitos.

De toda a maneira, a jurisprudência portuguesa tem resvalado entre uma interpretação mais protectora dos clientes e outra que pende mais para as entidades bancárias, especialmente quando estão em causa a cedência de "senhas" aos hackers.

No sentido de uma jurisprudência que faz sobressair tais situações como um risco da actividade bancária, que deve arcar com as consequências negativas da disponibilização dos serviços de homebanking, já que enquanto contraente mais forte, que coloca on-line o serviço, deve assegurar a segurança do mesmo, acórdãos do TRL, Processo 192119/11.8YIPRT.L1-2, de 24-05-2012, consultado em www.dgsi.pt.

Tratou-se de um caso em que o cliente subscreveu o serviço de homebanking, que lhe permitiu a faculdade de estabelecer relações com o Banco, designadamente, "na aquisição de serviços, realização de consultas e de operações bancárias relativamente às contas de que ele seja o único titular ou co-titular em regime de solidariedade, e que possa livremente movimentar, utilizando para o efeito, canais telemáticos: telefone (serviço telefónico) internet (serviço on-line) Wap (wireless Application Protocol, ITV (interactive TV) ou outras formas de acesso que venham a ser definidas" (tratava-se da cláusula 1ª das "Condições Gerais" do Serviço Homebanking).

Também provado ficou que foram feitos movimentos através do homebanking por terceiro. Quem acedeu à conta bancária do Autor pôde fazê-lo porque conhecia, quer o número do contrato, quer o número do código de acesso, quer todas, ou parte, das 64 combinações de três algarismos que compõem o cartão matriz; As movimentações da conta do Autor foram executadas porque introduzidos os códigos que permitiam o acesso àquela conta bancária;

Posto isto, o acórdão começa por qualificar o contrato de depósito bancário, como um contrato de depósito irregular (sendo certo que existe quem enquadre em contrato de mandato, contrato de mútuo ou uma tese mista), em que cabe ao depositário responder pelo risco de extravio ou dissipação da coisa até ao montante exigível no momento da solicitação da

restituição, cfr. art.ºs 540º, 796º, n.º 1, 799º, n.º 1, 1144º, 1185º, 1205º e 1206º, e 1161º, alínea e), todos do Código Civil, pelo que montantes debitados por actuação fraudulenta de terceiro, não eximem essa responsabilidade.

Salienta tal aresto jurisprudencial que o contrato de homebanking é uma "figura contratual distinta do depósito, e que envolveu uma proposta e uma aceitação" um ""novo" contrato se insere numa relação negocial complexa iniciada através de um contrato de abertura de conta, e da constituição de depósitos de quantias em conta", pelo que nos deparamos com uma "coligação de contratos", sem deixar de também frisar que não obstante este serviço de homebanking passa a interferir normativamente com o contrato de conta bancária, como uma convenção acessória que é necessário cumprir. Como se chama a atenção não obstante se disponibilizar ao cliente um serviço mais cómodo, o certo é que o banco também daí tira benefícios: "Com enormes poupanças de escala, por parte do banco, que, a não ser assim, nunca se interessaria pela disponibilização de tal serviço que, de resto, e como é notório, promove insistentemente junto dos seus clientes."

Mas debruçando-se concretamente sobre o facto do terceiro ter usado "senha" a que apenas o cliente tinha acesso e sobre a cláusula contratual geral que dispunha que a inserção de elementos de segurança pessoais e intransmissíveis do subscritor do serviço pelo terceiro que realizou a operação, se presume que tal foi consentido ou culposamente facilitado pelo aderente, entendeu ser cláusula proibida, por implicar uma prova do contrário – cfr. art.º 350º, n.º 2, do Código Civil – absolutamente diabólica e na prática inalcançável pelo aderente, que "não tem qualquer controlo sobre os sofisticados meios informáticos da entidade bancária, nem dispõe da assessoria técnica de primeira água com que os departamentos respetivos daquela se apetrecham."

Presumindo-se a culpa do Banco nos termos do art. 799.º, n.º 1 do CC, na não restituição de quantia em dinheiro igual à depositada, entendeu-se que deveria provar que não teve qualquer culpa, o que não resulta apenas das movimentações da conta "terem sido "executadas porque introduzidos os códigos que permitiam o acesso àquela conta bancária", "até porque o acesso on line fraudulento aos depósitos bancários conhece uma sofisticação e actualização permanentes, que exigem das instituições de crédito um esforço continuado naquele domínio, ao menos

enquanto persistirem em apresentar-se como guardiãs confiáveis dos valores que lhes são entregues, no pressuposto de assim ficar garantida a salvaguarda daqueles." É crescente a utilização dos chamados Cavalos de Troia na actividade bancária. Como se refere naquela acórdão, citando artigo de Francisco Luís, publicado na inforBANCA 88 • Abr > Jun 2011, da Associação Portuguesa de Bancos,[In http://apb.pt/content/files/Inforbanca_88_Proteger_o_Dinheiro.pdf] "Os ataques de phishing e o malware usados são cada vez mais sofisticados e difíceis de detectar, mesmo para utilizadores alertados para a temática da segurança.".

Tudo isto para concluir que o Banco não elidiu a presunção de culpa estabelecida no art.º 799º, do Código Civil. Mas como bem chama a atenção este acórdão, mesmo ilidindo a presunção de culpa, sempre seria de responsabilizar a título de risco, já que "dificilmente alguém poderá sustentar o razoável de o depositante individual suportar – ainda que em parte – o risco de a instituição de crédito a quem confiou os seus valores, se revelar afinal incapaz de assegurar a intangibilidade daqueles por terceiros. O depositante contrata com o banco no inarredável pressuposto de ser estranho às vicissitudes por que passe a instituição de crédito em matéria de segurança, e para as quais ele não contribua."

A este propósito interessante sentença do 5.º Juízo Cível de Guimarães[31], processo n.º 2869/11.4TBGMR, num caso em que um terceiro se "intrometeu" no sistema de homebanking de um cliente, iludindo este ao pedir os elementos de identificação necessários para fazer o movimento como se tratasse do próprio banco[32], e em que numa interpretação que concordamos, para além do incumprimento contratual do contrato de depósito irregular, também se defende que existe um incumprimento dos deveres acessórios de protecção. Trata-se de uma correcta abordagem que reforça os deveres de segurança que impendem sobre o banco na disponibilização dos serviços de homebanking, nomeadamente dever de evitar intrusões no sistema por hackers.

[31] Inédito, gentilmente disponibilidade pela Sra. Juiz Rita Mota Soares, titular de tal juízo.

[32] Em tal processo provou-se que após o cliente ter introduzido o endereço electrónico do site do Baco, foi-lhe solicitada a introdução dos dados do cartão matriz, o que este fez por não ter detectado nada de estranho na página a que acedera e considerou tratar-se da página verdadeira e fidedigna do site daquela instituição, razão pelo que os dígitos do cartão matriz no local indicado no site para aposição dos mesmos. Através de tal o hacker ficou na posse dos elementos com o qual fez vários movimentos de débito na conta bancária do cliente.

Como se escreveu naquela sentença "ao nível de intrusão sobre que versamos no caso sub judice, a obrigação de oferecer segurança às operações realizadas através da internet não é do utilizador (cliente) mas sim da instituição bancária, a qual deve estar ciente dos riscos que assume quando disponibiliza ao cliente o acesso aos serviços e a realização de operações bancárias que são de molde a fazer claudicar o dever de custódia que assumiu no contrato principal (o que não sucederia se nos reportássemos a uma situação da vida real em que o depositante houvesse fornecido elementos a terceiros de modo consciente e voluntário). Donde, se o Banco não tem condições para garantir a segurança do serviço, então não o deverá prestar. E é aqui que reside o cerne da responsabilidade civil da ré, pois com a não elisão da culpa temos por reunidos todos os pressupostos do instituto (pois quanto ao preenchimento dos demais nenhuma dúvida se coloca): o facto voluntário resulta da autorização da transferência bancária para a conta indicada pelo hacker; o ilícito contratual está circunstância de a ré não cumprir a obrigação de restituição das quantias desviadas às contas bancárias das autoras; o dano consiste nas disponibilidades monetárias perdidas e o nexo causal traduz-se no facto de ter sido aquela transferência que veio a provocar lesão no património das autoras."

E chamado a atenção sobre os deveres de protecção ali se escreve "Mas é ainda de notar que, a mais da via estritamente contratual, a responsabilidade da ré pelo pagamento das quantias desviadas da conta bancária das autoras sempre lhe adviria dos princípios inerentes aos deveres de protecção. Ou seja, ainda que se entendesse que a ré não podia responder contratualmente pela actuação de um terceiro (hacker), pagando à depositária a quantia ilicitamente desviada por este, sempre tal obrigação lhe adviria por via da doutrina dos deveres de protecção", por " omitir os cuidados que poderia e deveria ter levado a cabo na prevenção do ataque do património das autoras por parte de terceiro".

Uma posição da jurisprudência bem mais exigente no que se deve entender por conduta culposa do cliente, bastando a circunstância deste fornecer, ele próprio, as informações essenciais ao hacker para elidir a presunção de culpa do art. 799º, do CPC, poderá "encontrar-se" no Ac. do Tribunal da Relação de Guimarães de 23.10.2012, Rel.: FILIPE CAROÇO, consultado em www.dgsi.pt (tendo-se provado neste processo que a entidade bancária divulga na página inicial

do serviço mensagens a alertar que o banco nunca pede a confirmação dos dados do cartão matriz).

[Este acórdão foi objecto de anotação nos Cadernos de Direito Privado, n.º 41, Janeiro/Março de 2013 por Maria Raquel Guimarães, recomendando-se a sua consulta para melhor apreensão da matéria. Realça-se aqui, contudo, a distinção que esta Autora bem faz entre o phishing (que consiste no envio de mensagens de correio electrónico para o cliente do banco para tentar obter as palavras passe que lhe permitem executar serviços no homebanking, procurando dar a aparência que se trata de informações solicitadas por entidade fidedigna, nomeadamente o banco) e o pharming (situação em que o hacker ataca a própria página do banco, fazendo por exemplo aparecer "janelas" para que o cliente insira os códigos, ou redirecionando o cliente para uma página falsa, quando o cliente procura aceder ao site do banco, em tudo idêntica à deste, onde o cliente introduz as palavras chaves, sem saber que está a ser objecto de burla)].

9. A protecção de programas de computador e responsabilidade pela sua reprodução não autorizada.

Muito sinteticamente, e para terminar, algumas questões a este propósito que os tribunais têm analisado:

Crime de reprodução ilegítima de programa protegido. Violação da propriedade intelectual. Destrinça com o crime de usurpação.

Licitude da utilização ou reprodução de programa protegido sem expressa autorização do autor, no âmbito do CDADC.

A ilicitude da instalação de um único programa informático licenciado em vários computadores de uma empresa.

Da irrelevância pelo facto do programa não ter sido reproduzido em suportes magnéticos móveis, mas apenas instalado noutros computadores.

A divulgação de programa protegido.

Vejamos então os acórdãos que dirimem tais questões:

Ac. da RC, processo n.º 1788/04.5JFLSB.C1, de 20.03.2011, consultado em www.dgsi.pt: *"(...) II – O art. 8º, nº 1, da Lei nº 109/2009, de 15 de Setembro (Lei do Cibercrime), que tipifica o crime de reprodução ilegítima de programa protegido, tutela a propriedade intelectual mediante a criminalização da utilização não autorizada de programa informático protegido por lei. Para a consumação do crime basta a reprodução, divulgação ou comunicação ao público, não se exigindo que a lesão do direito de autor se traduza num prejuízo económico (efectivamente verificado) para este. III – O crime de usurpação p. p. pelos arts. 195º, 197º e 199º do CDADC, tutela o exclusivo de exploração económica da obra, que a lei reserva ao respectivo autor. Este tipo de crime verifica-se, independentemente de qualquer resultado material, desde que ocorra uma utilização não autorizada, independentemente de o agente se propor obter qualquer vantagem económica. IV – No âmbito do CDADC, a licitude da utilização ou reprodução sem expressa autorização do autor apenas se afirma com a demonstração de que essa utilização ou reprodução se destinou a fim exclusivamente privado, sem prejuízo para a exploração normal da obra e sem injustificado prejuízo dos interesses legítimos do autor, sendo esta tripla conjugação que evidencia a verificação da regra dos três passos, decorrente da assimilação dos princípios previstos originariamente na Convenção de Berna para a Protecção das Obras Literárias e Artísticas, ratificada por Portugal e transposta para o direito nacional através da legislação que tutela aquela matéria."*

Tratava-se de um caso em que o arguido efectuou cópias de software – programas de computador – tanto a partir dos respectivos originais como através da utilização do programa de partilha de ficheiros denominado E-mule, sem que para o efeito dispusesse de qualquer autorização dos respectivos autores, e não se provando que tivesse sido para uso privado, pelo que foi condenado pela infracção ao disposto no art. 195.º, n.º 1 do CDADC.

Como se explana nesse acórdão, a propósito do uso particular e apoiando-se no art. 75º, nº 2, al. a), do CDADC, *"a reprodução de obra protegida efectuada no âmbito do uso privado é lícita, independentemente do consentimento do autor da obra ou de quem legalmente o represente. Constituindo ainda uma modalidade de utilização da obra, o uso privado distingue-se por ter em vista a exclusiva satisfação de interesses pessoais de carácter não económico, sejam eles de natureza cultural ou recreativa. A lei apenas excepciona a reprodução de*

partituras. E sendo assim, mesmo o download de obra protegida por direito de autor não traduz violação desse direito, desde que efectuada no âmbito do uso privado, ainda que a obra ou prestação venham a ser fixados num suporte destinado a esse efeito, como um disco rígido ou um CD-R, não havendo lugar à responsabilização criminal ou civil do autor da cópia." Simplesmente, no que tange à cópia, há que ter presente ainda o disposto no art. 81º, al. b), que, desenvolvendo o teor do art. 75º, nº 4, dispõe ser consentida a reprodução "para uso exclusivamente privado, desde que não atinja a exploração normal da obra e não cause prejuízo injustificado dos interesses legítimos do autor, não podendo ser utilizada para quaisquer fins de comunicação pública ou comercialização". Esta forma de utilização lícita tem que ser expressamente demonstrada."

A propósito da ilicitude da instalação de um único programa informático licenciado em vários computadores de uma empresa e da irrelevância pelo facto do programa não ter sido reproduzido em suportes magnéticos móveis, mas apenas instalado noutros computadores, decidiu o ac. da R.C., processo n.º 1161/06, de 12.07.2006, consultado em www.dgsi.pt, em cujo sumário se escreveu *"1. A instalação de um único programa informático licenciado em vários computadores de um empresa traduz-se numa reprodução de programa não autorizada. 2. O tipo legal de crime de reprodução de um programa informático protegido não exige intenção de lucro. 3. Para o preenchimento do tipo legal de crime é irrelevante que o programa não tenha sido reproduzido em suportes magnéticos móveis, mas apenas instalado noutros computadores."*

No caso em análise estava em causa o crime de reprodução ilegítima de programa protegido, p. e p. pelos artigos 9°, n.º 1, da Lei nº 109/91, de 17.08, e 14º nºs 1 e 2, do DL nº 252/94, de 20.10, entre outros de programa antivírus com licença de utilização apenas para um computador da empresa, embora tivessem instalado em vários.

Também, a propósito do crime de reprodução ilegítima de programa protegido, ac. da RC, processo n.º 1159/06, de 5.07.2006, consultado em www.dgsi.pt: No tipo legal de crime de reprodução ilegítima de programas protegidos (crimes informáticos), previsto no art.º 9.º da Lei 109/91, não são cumulativos os elementos contemplados no seu n.º 1, isto é, tanto é punível o acto de reproduzir um programa informático, com é punível o acto de o divulgar ou comunicar ao público.

Aí se escreve *"Sobre a interpretação do artigo 9º confrontam-se duas teses: uma propugnada pelo Prof. José de Faria e Costa que considera ser uma norma de aplicação apenas quando estão reunidos os requisitos de reprodução do software, a sua divulgação ou comunicação ao público e outra, defendida por Manuel Lopes Rocha, mais consentânea com a Recomendação do Conselho da Europa, que considera que tais requisitos não têm que se cumular, bastando para que uma conduta seja criminosa a reprodução ilegítima do software[Lopes Rocha in Direito da Informática – Legislação e Deontologia, Ed. Cosmos, 1994.]. Com a maioria da jurisprudência, e a decisão recorrida, acompanhamos a segunda opção. Interpreta correctamente o preceito. A interpretação contrária contribui para deixar sem punição a esmagadora maioria da reprodução ilegal de software que conhecemos em Portugal."*

Termina-se aqui, sendo que muito haveria por dizer, esperando que o propósito de apresentar, ainda que de forma sintética, uma perspectiva judicial das problemáticas surgidas com o advento da internet tenha sido conseguido.

Muito obrigado,
Coimbra, 21 de Junho 2013