MINISTÉRIO PÚBLICO
PORTUGAL

PROCURADORIA-GERAL DA REPÚBLICA

GABINETE CIBERCRIME

JURISPRUDÊNCIA SOBRE CIBERCRIME

Nota Prática nº 11/2017

2 de novembro de 2017

gabinete cibercrime
novembro 2017

cibercrime@pgr.pt
http://cibercrime.ministeriopublico.pt/

ÍNDICE

NOTA PRÁTICA nº 11/2017
2 de novembro de 2017

Jurisprudência sobre cibercrime

Pretende-se com esta nota prática atualizar as referências jurisprudenciais de tribunais superiores sobre crimes informáticos e crimes cometidos por via de sistemas informáticos, publicadas e disponíveis na Internet. Além dos arestos mais recentes, recuperam-se os acórdãos já incluídos em anteriores Notas Práticas.

Como aconteceu com Notas Práticas anteriores, não se faz a análise detalhada dos acórdãos, os quais se referem apenas com um curto sumário. Além deste, fazem-se apenas muito brevíssimos comentários genéricos, de enquadramento, que somente pretendem dar pistas sobre a extensão e o sentido da jurisprudência.

O período temporal coberto termina na presente data e recua até 2009, ano da publicação da Lei do cibercrime, embora se incluam algumas decisões anteriores, por se manterem pertinentes.

1. ACESSO ILEGÍTIMO

Das decisões mais antigas conhecidas sobre acesso ilegítimo, uma delas é já muito desatualizada, por ser anterior à Lei do Cibercrime (publicada em 15 de setembro de 2009) e a outra versa sobre a evolução do tipo descrito na lei anterior para o atual. Este último confirma as conclusões que o acórdão mais antigo formula, quanto à essência do tipo de crime, apesar de o tipo de crime de acesso ilegítimo da Lei do Cibercrime (Artigo 6º) ter substanciais alterações em relação ao seu congénere da Lei nº 109/91 (Artigo 7º). Por outro lado, o acórdão mais recente clarifica o intuito do tipo de crime, indo no sentido dos outros dois acórdãos.

Acórdão da Relação de Coimbra de 17 de fevereiro de 2016

Comete o crime de acesso ilegítimo (Artigo 6º, nºs 1 e 4, al a, da Lei nº 109/2009), o inspetor tributário que, por motivos estritamente pessoais, acede ao sistema informático da Autoridade Tributária, consultando declarações de IRS de outrem. O tipo subjetivo daquele ilícito penal não exige qualquer intenção específica (como seja o prejuízo ou a obtenção de benefício ilegítimo), ficando preenchido com o dolo genérico de intenção de aceder a sistema)

Acórdão da Relação do Porto de 8 de janeiro de 2014

O crime de acesso ilegítimo, previsto no Artigo 6º da Lei do Cibercrime (Lei nº 109/2009) incrimina exatamente a mesma factualidade que era incriminada pelo crime correspondente (Artigo 7º da Lei nº 109/91). Todavia, na lei nova, não se exige qualquer intenção específica (por exemplo, a de causar prejuízo ou a de obter qualquer benefício

ilegítimo), apenas se exigindo dolo genérico. O bem jurídico protegido é a segurança dos sistemas informáticos.

Acórdão da Relação de Coimbra de 15 de outubro de 2008
O bem jurídico protegido do crime de acesso ilegítimo é a segurança do sistema informático – a proteção ao designado "domicílio informático" algo de semelhante à introdução em casa alheia.

2. FALSIDADE INFORMÁTICA

A generalidade das decisões publicadas sobre o crime de falsidade informática faz uma interpretação estrita e literal dos seus complexos elementos. Noutra vertente, não é pacífico o entendimento jurisprudencial quanto aos interesses jurídicos protegidos pelo tipo de crime. A decisão mais recente, porém, avança nesse domínio, delimitando o interesse protegido, tomando como referência o crime comum de falsificação
Também quanto à falsidade informática se anota a virtude, que as decisões de tribunais superiores sempre têm, de discutir a inserção de casos concretos no tipo de crime. Neste caso é particularmente interessante a confrontação do tipo de crime (e de outros correlacionados) com atuações ilícitas relacionadas com cartões bancários.

Acórdão da Relação do Porto de 14 de setembro de 2016
Os bens jurídicos violados pela burla e pela falsificação são, respetivamente, o património do burlado e a fé pública dos documentos necessária à normalização das relações sociais – portanto, diversos e autónomos. Por isso, entre os crimes de burla informática (Artigo 221º do Código Penal) e o crime de falsidade informática (Artigo 3º da Lei Cibercrime), existe concurso real de infrações.

Acórdão da Relação do Porto de 26 de maio de 2015
No crime de falsidade informática (Artigo 3º nº 1, da Lei do Cibercrime), os dados informáticos têm de ser alterados com o propósito de desvirtuar a demonstração dos factos que com aqueles dados podem ser comprovados. Comete tal crime quem introduzir no sistema informático de um hospital episódios de cirurgias realizadas em regime de ambulatório como se tivessem sido levadas a cabo em regime de internamento, quando tal não correspondia à realidade. A relação jurídica que com este comportamento se cria não corresponde à verdade, sendo certo que os dados assim vertidos no sistema informático produzem os mesmos efeitos de um documento falsificado, pondo em causa o seu valor probatório e consequentemente a segurança nas relações jurídicas.

Acórdão da Relação de Évora de 19 de maio de 2015
O tipo objetivo do crime de falsidade informática previsto no nº 1 do Artigo 3º da Lei do Cibercrime supõe que a interferência no tratamento informático de dados produza, como resultado, dados ou documentos não genuínos. O tipo supõe dolo, nas formas gerais e ainda, enquanto elemento subjetivo especial do tipo, a intenção de provocar engano nas relações jurídicas, bem como, relativamente à produção de dados ou documentos não genuínos, a particular intenção do agente de que tais dados ou documentos sejam considerados ou utilizados para finalidades juridicamente relevantes como se fossem genuínos. Este crime visa proteger a segurança das relações jurídicas enquanto interesse público essencial que ao próprio Estado de Direito compete assegurar e não a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e de dados informáticos. O uso de documento não genuíno (nº 3 do Artigo 3º) apenas é punido se o for por pessoa distinta da que praticou a "falsificação". A utilização de nome de outrem

para criar endereço de correio eletrónico traduz a produção de dados ou documentos não genuínos (mediante a introdução de dados informáticos) e é idóneo a fazer crer que foi a pessoa a quem respeita o nome quem efetivamente criou aquele endereço.

Acórdão da Relação do Porto de 17 de setembro de 2014
Constitui o crime de contrafação de moeda falsa (Artigos 262º, nº 1 e 267º, nº 1, c) do Código Penal), o fabrico de cartão de crédito falso com inserção de banda magnética clonada de um cartão verdadeiro, por bastar para o preenchimento do tipo a interferência na banda magnética do cartão de crédito clonado. Constitui o crime de falsidade informática (Artigo 3º, nºs 1 e 2 da Lei 109/2009) a captura, em ATM, da informação existente na banda magnética de cartão de crédito.

Acórdão da Relação do Porto de 24 de abril de 2013
O bem jurídico tutelado pelo crime de falsidade informática (Artigo 3º, nºs 1 e 3 da Lei do Cibercrime), não é o património, mas antes a integridade dos sistemas de informação, através do qual se pretende impedir os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados.

Acórdão da Relação do Porto de 21 de novembro de 2012
O crime de passagem de moeda falsa e o crime de falsidade informática estão em relação de concurso efetivo, porque protegem interesses diferentes: o primeiro, a fé pública na moeda, a segurança e funcionalidade do tráfego monetário e a integridade do sistema monetário; o crime de falsidade informática visa proteger a integridade dos sistemas de informação e a sua confidencialidade, integridade e disponibilidade.

Acórdão da Relação de Lisboa de 10 de julho de 2012
O crime de falsidade informática previsto no Artigo 3º da Lei do Cibercrime não veio esvaziar de sentido a alínea c) do nº 1, do Artigo 267º, do Código Penal, continuando este preceito a abranger a conduta que se traduza em adulteração de cartões de crédito, uma vez que no crime de contrafação de moeda o bem jurídico protegido é a integridade ou intangibilidade do sistema monetário legal em si mesmo considerado, aqui representado pelos cartões de crédito por via da sua equiparação àquela.

Acórdão da Relação de Lisboa de 30 de junho de 2011
O bem jurídico protegido pelo crime de contrafação de moeda é a intangibilidade do sistema monetário, incluindo a segurança e credibilidade do tráfego monetário; o bem jurídico protegido pelo crime de falsificação informática é a integridade dos sistemas de informação. Se a ação consiste em duplicar e utilizar cartões bancários, com acesso a dados que neles se encontravam, produzindo com estes dados documentos não genuínos para os utilizar no levantamento de dinheiro ou pagamento de bens, ocorrem, em concurso efetivo, aqueles dois crimes.

3. BURLA INFORMÁTICA

Com exceção das situações de facto relacionadas com levantamento de dinheiro em utilização indevida de cartões bancários, a jurisprudência sobre burla informática ainda é escassa. A referência legislativa é o Artigo 221º do Código Penal, introduzido em 1995 e alterado em 1998. Em geral, as decisões conhecidas incidem sobre a essência do tipo de crime, quer na sua generalidade, quer na relação com o tipo de crime de falsidade.

Esta última vertente é a questão primordial da mais recente decisão, delimitando o interesse protegido da falsidade informática tomando como referência o crime comum de falsificação.

Acórdão da Relação do Porto de 14 de setembro de 2016
Os bens jurídicos violados pela burla e pela falsificação são, respetivamente, o património do burlado e a fé pública dos documentos necessária à normalização das relações sociais – portanto, diversos e autónomos. Por isso, entre os crimes de burla informática (Artigo 221º do Código Penal) e o crime de falsidade informática (Artigo 3º da Lei Cibercrime), existe concurso real de infrações

Acórdão da Relação do Porto de 3 de fevereiro de 2016
A burla informática consiste num erro consciente provocado por intermédio da manipulação de um sistema de dados ou de tratamento informático. Não se exige um qualquer engano ou artifício por parte do agente, mas sim a introdução e utilização abusiva de dados no sistema informático.

Acórdão da Relação de Évora de 19 de novembro 2015
A manipulação de dados de uma máquina ATM com o propósito de que a mesma, sem motivo legítimo, ejete uma grande quantidade de notas, preenche o tipo de crime de burla informática.

Acórdão da Relação do Porto de 30 de setembro de 2009
Na burla informática a lesão do património produz-se através da intromissão nos sistemas e da utilização em certos termos de meios informáticos - é um crime de resultado, exigindo-se que seja produzido o prejuízo patrimonial de alguém.

Acórdão da Relação do Porto de 30 de abril de 2008
Se a burla se realizou mediante a introdução de dados incorretos/falsos no sistema informático da Segurança Social, existe concurso efetivo de burla e falsidade informática.

4. BURLA INFORMÁTICA – CARTÕES MULTIBANCO

*No final da década de 1990, o Tribunal Constitucional (Acórdão nº 48/99, de 19 de janeiro de 1999) e o Supremo Tribunal de Justiça (Acórdãos de 2 de outubro de 1996 e de 19 de dezembro de 2001) deixaram entender que o levantamento indevido de dinheiro com cartões bancários ilegitimamente obtidos consubstanciava a prática de crime de furto (furto do cartão, primeiro, mas igualmente furto do dinheiro, depois). O "*pin*" do cartão ilegitimamente obtido era assim equiparado à chave de um cofre, que permitia a quem furtasse ou roubasse o cartão, também, furtar dinheiro.*
*Na sequência da posição assumida na anotação ao Código Penal de Leal Henriques e Simas Santos, a ulterior jurisprudência das Relações passou a tender para considerar que esta atuação preenche o tipo de crime de burla informática, na medida em que supõe "*utilização não autorizada de dados*".*
A jurisprudência mais recente é quase unânime nesse sentido, havendo, todavia, ainda alguma resistência do Supremo Tribunal de Justiça.

Acórdão da Relação de Évora de 29 de novembro de 2016
Incorre na prática de um crime de burla informática aquele que, sem autorização e com vista a obter um enriquecimento ilícito, utiliza um cartão Multibanco de terceiro, cujo *pin* era do seu conhecimento, e procede a várias operações bancárias (levantamentos e transferências monetárias) sobre a conta associada a esse cartão.

Acórdão da Relação de Évora de 20 de janeiro de 2015
Quem subtraí um cartão multibanco alheio e, de seguida, levanta quantias em dinheiro de caixa de ATM, comete em concurso efetivo, dois crimes: um de furto e outro de burla informática.

Acórdão da Relação do Porto de 5 de junho de 2013
Comete o crime de burla informática (Artigo 221º do CP) quem utiliza um cartão bancário de débito para pagamentos, sem autorização do legítimo titular do cartão, ainda que para o efeito não seja necessária a marcação de qualquer código. Este crime tutela a utilização correta dos meios informáticos e também o património de outrem.

Acórdão da Relação de Guimarães de 18 de dezembro de 2012
O levantamento de dinheiro em caixas ATM com utilização do cartão de outrem e digitação do respetivo código de acesso sem autorização, com intenção de obter enriquecimento ilegítimo, causando a outra pessoa prejuízo patrimonial, integra uma das modalidades da ação típica do crime de burla informática.

Acórdão da Relação de Évora de 26 de junho de 2012
A burla informática, consiste na manipulação dos sistemas informáticos, ou utilização sem autorização ou abusiva determinando a produção dolosa de prejuízo patrimonial; o tipo pretendeu abranger a utilização indevida de máquinas automáticas de pagamento.

Acórdão da Relação do Porto de 14 de março de 2012
Uma das modalidades da ação típica do crime de burla informática, é a apropriação de dinheiro através da introdução e utilização no sistema informático das ATM de dados sem autorização (introdução do cartão e digitação do código de acesso), com intenção de obter enriquecimento ilegítimo, causando a outra pessoa prejuízo patrimonial.

Acórdão do Supremo Tribunal de Justiça de 5 de novembro de 2008
A utilização de um cartão Multibanco obtido por via de violência ou coação, para levantamento de dinheiro é ainda parte da prática do crime de roubo, perdendo qualquer autonomia, ou estando mesmo tipicamente excluída, a integração do crime de burla informática).

Acórdão do Supremo Tribunal de Justiça de 29 de maio de 2008
Se o agente do crime força a vítima a revelar o código secreto (PIN) do seu cartão de débito ou de crédito que lhe retira, para depois se apoderar dos proventos económicos que a utilização desse cartão obtém através do sistema bancário, em prejuízo da vítima, há uma consumpção de normas entre os crimes de roubo e os de burla informática.

5. REPRODUÇÃO ILEGÍTIMA DE PROGRAMA PROTEGIDO

Existia rica jurisprudência sobre o crime de reprodução ilegítima de programa protegido ao abrigo da antiga Lei da Criminalidade Informática, atualmente revogada (Lei nº 109/91). Talvez por se terem firmado, nesse tempo, orientações claras e, ainda também, por o tipo de crime não ter sofrido, da versão de 1991 para a de 2009, alteração substancial, é mais diminuta a jurisprudência sobre a lei vigente (a Lei do Cibercrime – Lei nº 109/2009). Os acórdãos referenciados abordam, todavia, três ideias basilares:

por um lado, a de que é ilícito, quanto a um programa informático que se comprou licitamente, reproduzi-lo em número superior ao contratualmente previsto; por outro lado, a de que o crime não exige intenção lucrativa; por último, a de que os seus elementos típicos fulcrais (reprodução, divulgação e comunicação ao público) não são cumulativos, bastando-se o tipo de crime com apenas um de entre eles.

Acórdão da Relação de Lisboa de 8 de setembro de 2015
De acordo com o Decreto-Lei nº 252/04, que criou o direito de autor sobre programas de computador, a autorização de utilização do programa não implica a transmissão dos direitos atribuídos ao autor do programa de computador - designadamente os direitos de reprodução, transformação e colocação em circulação.

Acórdão da Relação de Coimbra de 30 de outubro de 2013
O tipo de crime de reprodução ilegítima de programa protegido não exige que, cumulativamente, haja reprodução, divulgação e comunicação ao público, bastando-se, por exemplo, com a instalação não autorizada de um programa informático protegido.

Acórdão da Relação de Coimbra de 12 de julho de 2006
A instalação de um único programa informático licenciado em vários computadores de uma empresa traduz-se numa reprodução de programa não autorizada. O tipo de crime de reprodução de programa protegido não exige intenção de lucro.

6. USURPAÇÃO

A discussão jurisprudencial mais recente sobre a violação de direito de autor, na vertente criminal, incide sobre dois aspetos práticos: um deles é o da incriminação, ou não, de agentes que, apesar de terem sido encontrados na posse de com cópias ilegítimas de obras, não venderam as mesmas; o outro respeita à reprodução por sistemas de som (altifalantes), de obras (nomeadamente música), em áreas públicas (sobretudo cafés, bares, esplanadas ou similares).
A respeito desta última problemática, a discussão jurisprudencial portuguesa está balizada pelo Acórdão de fixação de Jurisprudência do STJ de novembro de 2013, mas a questão não está encerrada nas instâncias da União Europeia.
É interessante aperceber as diversas opções da jurisprudência mais recente, quer seguindo a jurisprudência do STJ, quer, pelo contrário, reconhecendo a autoridade do TJUE – e até mesmo pragmaticamente assumindo que, mesmo consubstanciando os factos em causa um crime, pelas circunstâncias em que decorre esta discussão, os mesmos não poderão traduzir dolo dos seus agentes.

Acórdão da Relação de Coimbra de 28 de junho de 2017
A jurisprudência fixada pelo Supremo Tribunal de Justiça através do Acórdão Uniformizador nº 15/2013 é incompatível com a interpretação que uniformemente vem sendo dada pelo Tribunal de Justiça da União Europeia ao conceito de «comunicação ao público» de obra. Segundo aquela deliberação do STJ, não constitui crime de usurpação a difusão, através de aparelhagem sintonizada em emissora de rádio, de música ambiente em estabelecimento comercial porque tal difusão não configura nova utilização das obras transmitidas. À luz da jurisprudência0 do TJUE esta atuação, sem autorização, é ilícita. Porém, neste complexo contexto jurídico-penal e jurisdicional é manifestamente desrazoável considerar dolosa tal atuação.

Acórdão da Relação de Coimbra de 22 de fevereiro de 2017
A simples atividade de audição/visionamento de canal televisivo, em cafés, restaurantes, bares, e outros estabelecimentos abertos ao público em geral, não dependendo de prévia

autorização dos autores das obras transmitidas, não é idónea à verificação do crime de usurpação.

Acórdão da Relação de Lisboa de 4 de fevereiro de 2016
A transmissão de fonogramas através de aparelho de televisão e rádio com amplificador num estabelecimento comercial de café constitui execução pública, a que se refere o artigo 184º do Código do Direito de Autor e dos Direitos Conexos, que necessita de autorização dos respetivos produtores. Não estando autorizada a execução pública dos fonogramas, procede a providência cautelar com a imposição da proibição de continuação da execução e com a condenação de uma sanção pecuniária compulsória, mas já não procede na parte em que é pedido o encerramento do estabelecimento, por ser uma medida desproporcionada e desnecessária, nem a apreensão dos bens em causa e o livre acesso ao estabelecimento para fiscalização, por serem medidas também desnecessárias, já que se trata de um estabelecimento aberto ao público em que facilmente se controla o cumprimento ou não da medida de proibição decretada.

Acórdão da Relação de Coimbra de 20 de janeiro de 2016
Constitui mera receção e não reutilização da obra transmitida, a difusão de música ambiente de determinada estação emissora de rádio, através de várias colunas de som. Esta difusão não constitui crime de usurpação (Artigo 195º do Código do Direito de Autor e dos Direitos Conexos) e não carece de autorização dos autores das obras radiodifundidas por aquela estação emissora.

Acórdão da Relação de Guimarães de 11 de janeiro de 2016
Quem adquire um conjunto de obras contrafeitas com o propósito de as vir a vender, preenche o tipo de crime do Artigo 199º do Código do Direito de Autor e dos Direitos Conexos na forma tentada. Porém, tendo em conta a moldura penal abstratamente aplicável para o crime consumado a prática deste ilícito típico na forma tentada não é punível (Artigos 22º, 23º do Código Penal e 197º nº1 CDADC).

Acórdão da Relação de Évora de 19 de novembro de 2013
Pratica o crime de usurpação e/ou aproveitamento de obra usurpada quem colocar à venda cópias não autorizadas de fotogramas ou videogramas; mesmo que não tenha sido vendida nenhuma cópia, o crime consuma-se se o agente estava em local de venda, com intenção de venda e na posse de cópias ilegais.

Acórdão de fixação de jurisprudência do Supremo Tribunal de Justiça nº 15/2013, de 13 de novembro de 2013
A aplicação, a um televisor, de aparelhos de ampliação do som, difundido por canal de televisão, em estabelecimento comercial, não configura uma nova utilização da obra transmitida, pelo que o seu uso não carece de autorização do autor da mesma, não integrando consequentemente essa prática o crime de usurpação (Artigos 149º, 195º e 197º do Código do Direito de Autor e dos Direitos Conexos).

Acórdão da Relação de Évora de 15 de outubro de 2013
A emissão de programa televisivo, em estabelecimento aberto ao público, através de um televisor ligado a uma box da Cabovisão (e a nenhum outro dispositivo), sem que os titulares dos direitos de autor tivessem concedido uma autorização específica para este efeito, não preenche o tipo de ilícito de usurpação dos Artigos 195º e 197º do Código dos Direitos de Autor e dos Direitos Conexos.

Acórdão da Relação de Coimbra de 30 de março de 2011

O crime de usurpação (Artigos 195º, 197º e 199º do CDADC) tutela o exclusivo de exploração económica da obra, que a lei reserva ao respetivo autor; o crime verifica-se quando ocorre uma utilização não autorizada, independentemente de o agente se propor obter qualquer vantagem económica; a utilização ou reprodução sem expressa autorização do autor apenas é permitida para fim exclusivamente privado, sem prejuízo para a exploração normal da obra e sem injustificado prejuízo dos interesses legítimos do autor.

7. PHISHING

A jurisprudência sobre phishing *disponível é, toda ela, da jurisdição cível e respeita a casos em que aquilo que se discutia era a responsabilização, ou não, da instituição bancária, pela perda resultante de um ato criminoso. É colateral a esta a questão da culpa – e eventual responsabilidade – do "dono" da conta bancária, a qual apenas é reservada para casos de negligência grosseira.*

Acórdão do Supremo Tribunal de Justiça de 14 de dezembro de 2016

Recai sobre o banco prestador do serviço bancário online o risco das falhas e do deficiente funcionamento do sistema, impendendo ainda sobre o mesmo o ónus da prova de que a operação de pagamento não foi afetada por avaria técnica ou qualquer outra deficiência. Se o banco não demonstrar, como é seu ónus, que o utilizador teve um qualquer comportamento suscetível de pôr em causa a segurança do sistema, desconhecendo-se o modo como terceiros possa0m ter acesso aos dispositivos de segurança e efetuar operações não autorizadas, tem aquele banco a obrigação de reembolsar o ordenante do montante daquela operação de pagamento não autorizada.

Acórdão da Relação do Porto de 13 de outubro de 2016

Existe presunção de culpa da entidade bancária na má utilização fraudulenta de sistemas bancários por via da Internet. Em todo o caso, o banco pode ilidir aquela presunção, afastando a sua culpa ou demonstrando mesmo a culpa do cliente pela deficiente utilização daqueles meios expeditos, designadamente, alegando e demonstrando que o cliente violou o contrato, divulgando na internet dados pessoais, secretos e intransmissíveis relativos ao seu acesso, em benefício de hackers.

Acórdão da Relação de Lisboa de 15 de março de 2016

O *phishing* constitui uma fraude eletrónica cuja consequência é a obtenção ilícita de dados de acesso a contas bancárias e a sua utilização subsequente em proveito do autor da fraude. Apenas há responsabilidade da vítima, se se determinar que ela, com negligência grave, permitiu ao defraudador o acesso às credenciais de acesso. Negligência grave (ou grosseira) corresponde à falta grave e indesculpável, consistente na omissão dos deveres a que se está adstrito, que só uma pessoa especialmente desleixada, descuidada e incauta deixaria de observar. Não se provando como o agente do crime obteve as credenciais, não pode qualificar-se a atuação da vítima como gravemente negligente.

Acórdão da Relação de Coimbra de 2 de fevereiro de 2016

Não se tendo provado que o cliente forneceu a terceiros as chaves de acesso ao serviço de *homebanking* nem que, ao navegar na Internet, permitiu que outrem tenha capturado as credenciais de acesso e validação, recai sobre o banco a responsabilidade pela movimentação fraudulenta da sua conta bancária, através da internet (por via dos serviços de *homebanking*).

Acórdão da Relação de Évora de 25 de junho de 2015

No âmbito do *homebanking*, em regra recai sobre o Banco depositário o ónus da prova de que a falta de cumprimento de regras de segurança não procede de culpa sua. Mas o Banco pode elidir aquela presunção, demonstrando a culpa do cliente, por exemplo, provando que o cliente beneficiário violou o contrato, divulgando na internet dados pessoais, secretos e intransmissíveis relativos ao seu acesso, em benefício de *hackers*. Age com culpa o utente que fornece todo o conteúdo do cartão matriz perante uma solicitação numa página idêntica à do Banco, uma vez que contraria toda a lógica do sistema de segurança que não pode ser desconhecida por parte do utilizador.

Acórdão da Relação de Lisboa de 3 de março de 2015

Não se tendo apurado ter o cliente permitido o acesso de terceiros às suas credenciais, não se pode concluir ser imputável ao mesmo a quebra da confidencialidade dos dispositivos de segurança de acesso à sua conta bancária na Internet.

Acórdão da Relação de Guimarães de 17 de dezembro de 2014

Num contrato de *homebanking*, o Banco tem a obrigação de assegurar que os dispositivos de segurança personalizados do instrumento de pagamento só sejam acessíveis ao utilizador de serviços de pagamento que tenha direito a utilizar o referido instrumento. O utilizador de serviços de pagamento responde pelas perdas resultantes de operações de pagamento não autorizadas se tiver agido com incumprimento deliberado de uma ou mais das suas obrigações. Pode ainda responder por aquelas perdas se tiver atuado com negligência grave, conceito que se pode definir como "negligência grosseira, erro imperdoável, desatenção inexplicável, incúria indesculpável, vistos em confronto com o comportamento do comum das pessoas, mesmo daquelas que são pouco diligentes".

Acórdão da Relação do Porto de 29 de abril de 2014

No *homebanking*, incumbe ao Banco ilidir a presunção de culpa pelo perecimento de quantias cujo domínio lhe foi transferido por via contratual, ainda que a causa do perecimento resulte de acessos fraudulentos aos meios de movimentação de contas bancárias que disponibiliza aos seus clientes. Não age com culpa o depositante que por via de uma fraude informática levada a efeito por terceiros, na convicção que estava na página online do banco, introduziu numa página falsa, clonada da página daquele Banco, as suas certificações, pessoais e intransmissíveis, que abusivamente vieram a ser utilizadas no acesso, por terceiros, à conta de que era titular.

Acórdão da Relação de Lisboa de 12 de dezembro de 2013

No *homebanking* compete ao banco diligenciar pela segurança, de modo a que o seu utilizador não fique privado dos valores nele depositados pelo abusivo acesso de terceiros; ou seja, o cliente tem de poder confiar nesse sistema de acesso à sua conta bancária e respetiva movimentação. Sobre o Banco impende a obrigação de prestar um serviço eficaz e seguro, correndo por sua conta o risco de acessos fraudulentos. Porém, se o cliente fizer uma utilização imprudente, negligente e descuidada desse serviço, revelando a terceiros, na internet, os seus códigos pessoais de acesso ou outros elementos de acesso ao serviço, não é exigível ao Banco o pagamento das quantias por aqueles indevidamente movimentadas.

Acórdão da Relação de Lisboa de 5 de novembro de 2013

No serviço de *homebanking* é o banco quem tem que diligenciar para que o serviço seja seguro e nele possa o cliente confiar. Ignorando-se como é que os terceiros acederam às

chaves ou códigos de acesso, recai sobre o banco o dever de reembolsar os autores dos montantes das operações de pagamento.

Acórdão da Relação do Porto de 29 de outubro de 2013
Quando ocorre um caso de *phishing*, investe-se o ónus da prova de demonstrar que o computador do cliente defraudado foi infetado com um programa de código malicioso, que abriu uma brecha na respetiva segurança, permitindo a terceiros executar operações bancárias como se fossem os clientes do banco.

8. PORNOGRAFIA DE MENORES

Têm vindo a aumentar as decisões das Relações sobre pornografia de menores, o que espelhará com certeza o número de casos a este propósito instaurados nos tribunais. Uma boa parte dos acórdãos incide sobre aspetos processuais ou, na parte substantiva, sobre aspetos de pormenor. Não obstante, nem por isso deixam de ser relevantes.
É significativa a decisão que diz ser prescindível a concreta determinação da idade do menor/vítima. Já quanto à qualificação como crime do mero download *de ficheiros de pornografia infantil, instalou-se a discussão na jurisprudência.*
*Salienta-se, como "*sinal dos tempos*", a decisão mais recente, sobre partilha de fotografias entre pessoas conhecidas.*

Acórdão da Relação do Porto de 7 de junho de 2017
Se uma jovem de 14 anos tirou fotografias de partes do seu corpo sem vestuário e as enviou a terceiro, através do Facebook, este último pratica o crime de pornografia de menores (Artigo 176º do Código Penal), se remeter tais fotografias a outrem, que as recebeu e visualizou.

Acórdão da Relação de Évora de 25 de outubro de 2016
Constitui pornografia infantil qualquer representação, por qualquer meio, de uma criança em atividades sexuais explicitas, reais ou simuladas ou qualquer representação dos órgãos sexuais de crianças.

Acórdão da Relação de Évora de 2 de fevereiro de 2016
As medidas de coação de "detenção na habitação com vigilância eletrónica" e "proibição de utilização de equipamentos informáticos e de acesso à internet", esta última sem possibilidade efetiva de fiscalização e controlo, revelam-se medidas insuficientes para acautelar o perigo de continuação da atividade criminosa relativamente a arguido acusado da autoria de 977 crimes de pornografia de menores cometidos no domicílio, justificando-se a aplicação de prisão preventiva.

Acórdão da Relação de Lisboa de 15 de dezembro de 2015
Se não se provar intenção de partilha, fazer *download* de pornografia infantil constitui a prática de crime de aquisição ou detenção de pornografia de menores (Artigo 176°, n° 4, alínea d), do Código Penal). O *download* não constitui "importação de pornografia de menores" (crime previsto e punido pelo Artigo 176°, n ° 1 alínea c) do Código Penal).

Acórdão da Relação de Évora de 17 de março de 2015
Tendo os filmes de carácter pornográfico sido objeto de perícia, a sua exibição/visualização em audiência torna-se tarefa sem utilidade detetável. A concreta identificação de vítimas

não constitui elemento do tipo de pornografia de menores, previsto no artigo 176º, nº 1, als. c) e d) do Código Penal.

Acórdão da Relação do Porto de 3 de dezembro de 2014
Fazer *download* de dados de pornografia de menores, de um servidor para o seu dispositivo informático pessoal, relativos a ficheiros de imagens, integra o conceito de importar previsto na alínea c) do nº1 do Artigo 176º do Código Penal.

Acórdão da Relação de Coimbra de 2 de abril de 2014
Preenche o crime de pornografia de menores o arguido que guarda no seu computador imagens de crianças do sexo masculino, nuas e em poses de exibição dos órgãos sexuais.

9. NÃO CUMPRIMENTO DE OBRIGAÇÕES RELATIVAS A PROTEÇÃO DE DADOS

Os processos em que se investigam ou julgam crimes desta natureza não são muito abundantes. Não obstante, as decisões de tribunais superiores sobre a temática são ricas e abordam temas essenciais das mesmas (por exemplo, a sobreposição dos crimes da Lei nº 67/98 com o crime de devassa informática - Artigo 193º do Código Penal –, ou ainda a relação entre os diversos crimes da Lei de Proteção de Dados Pessoais).

Acórdão da Relação do Porto de 22 de abril de 2015
Preenche objetivamente o tipo de crime de não cumprimento de obrigações relativas à proteção de dados pessoais (Artigo 43º, nº 1, c), da Lei nº 67/98) a conduta de quem utiliza dados pessoais recolhidos pela empresa para quem trabalhou como cabeleireira, para promover o seu próprio negócio, também como cabeleireira.

Acórdão da Relação de Évora de 5 de novembro de 2013
O Artigo 193º do Código Penal (devassa por meio da informática) foi revogado e substituído pelos crimes da Lei de Proteção de Dados Pessoais. Entre o crime de não cumprimento de obrigações relativas a proteção de dados (Artigo 43º da LPDP) e o crime de violação do dever de sigilo (do seu Artigo 47º) verifica-se uma situação de concurso efetivo. O número de crimes cometidos não se afere pelo número de pessoas constantes do ficheiro de dados pessoais, o qual é irrelevante.

10. ILÍCITOS EM REDES SOCIAIS

A generalização da utilização da Internet e das redes sociais e, por outro lado, o aumento da capacidade e da conectividade dos equipamentos de computação e comunicação, potenciaram a divulgação, na Internet, de conteúdos suscetíveis de violarem a honra de outrem, ou a privacidade, ou o direito à imagem de terceiros.
Este tipo de atividades tem vindo a dar origem a um número crescente de processos, nos tribunais, o que se tem repercutido nas decisões dos tribunais superiores. Tais decisões têm versado, sobretudo, temáticas relacionadas com a honra. Destaca-se, porém, uma decisão que aborda a divulgação de dados de crianças em redes sociais.

Acórdão da Relação de Évora de 25 de junho de 2015
Em decisão de regulação de responsabilidades parentais, a imposição aos pais do dever de «abster-se de divulgar fotografias ou informações que permitam identificar a filha nas redes sociais» mostra-se adequada e proporcional à salvaguarda do direito à reserva da intimidade da vida privada e da proteção dos dados pessoais e, sobretudo, da segurança da menor no Ciberespaço.

Acórdão da Relação de Guimarães de 18 de março de 2013
A criação, numa rede social, de um perfil em nome de outra pessoa, com inclusão de características de utilizador ofensivas da honra e consideração do "titular" do perfil, constituem crime de difamação.

Acórdão da Relação de Évora de 14 de fevereiro de 2012
Estando em causa a prática de crimes contra a honra por meio de comentários publicados num *blog*, o domínio do facto assiste a duas pessoas, cuja intervenção é imprescindível ao cometimento do crime: aquela que inscreve o comentário e aquela que disponibiliza o *blog* para o efeito e consente na respetiva publicação. O administrador do *blog* gere e seleciona os comentários feitos no mesmo, pelo que tem o pleno domínio do facto. O importante não é quem causa o facto, mas quem domina a execução deste.

11. FOTOGRAFIAS ILÍCITAS

O surgimento de significativos casos de crimes de fotografias ilícitas (incluído filmagens em vídeo), previsto no número 2 do Artigo 199º do Código Penal, pode estar associado à expansão das maquinas fotográficas digitais e, sobretudo, à popularização de telefones que incorporam câmaras. A discussão deste fenómeno na jurisprudência coincidiu com o surgimento de um número expressivo de decisões sobre a admissão deste tipo de imagens como prova, em processo penal. A fronteira entre as duas questões jurídicas nem sempre está clara traçada, já que as duas discussões estão muito relacionadas, como que sendo as duas diferentes faces de uma mesma moeda.
A orientação genérica da jurisprudência é claramente protetora da imagem, reprimindo a utilização de fotografias de quem não consente nessa utilização. Chega mesmo a retirar consequências civis a este respeito, declarando haver responsabilidade de quem, detendo imagens de terceiro, permitir o seu visionamento por outrem.

Acórdão da Relação de Coimbra de 20 de setembro de 2017
O registo da imagem contra a vontade do retratado viola um bem jurídico-penal autónomo, em relação aos direitos à privacidade e intimidade. Para que ocorra o crime de fotografias ilícitas (Artigo 199º, nº 2, do Código Penal), não se exige que a oposição de vontade seja expressa, pois para a conduta ser típica bastará que contrarie a vontade presumida do portador concreto do direito à imagem.

Acórdão da Relação do Porto de 12 de julho de 2017
Constitui o crime de fotografias ilícitas (Artigo 199º do Código Penal), a realização de cópias informáticas de fotografias livremente acessíveis no Facebook e o seu envio posterior por *email*, por ter sido feita contra a vontade de quem elas retratavam. O facto de as fotografias estarem livremente acessíveis no Facebook não confere qualquer legitimidade para fazer cópias informáticas das mesmas e enviá-las por *email*, contra a vontade de quem elas retratavam.

Acórdão da Relação de Guimarães de 21 de novembro de 2016
O crime de fotografias ilícitas (Artigo 199º, nº 2, do Código Penal) proíbe, de forma autónoma, dois tipos de atos suscetíveis de ofender o direito à imagem: o de a registar, que até pode ser lícito, nomeadamente por ter o consentimento da pessoa retratada; outro, bem diferente, o da sua posterior utilização/divulgação contra a vontade do retratado. Preenche este tipo de crime quem divulgar fotografia, mesmo que desta não se

consiga apurar a identidade do retratado, se tal publicação se fizer num perfil do Facebook com o nome desse mesmo retratado.

Acórdão do Supremo Tribunal de Justiça de 3 de novembro de 2016
Se o possuidor de um computador onde está registado um videograma privado violar negligentemente o dever de o conservar (por exemplo, não impedindo que o mesmo seja visto por outrem), poderá ser responsabilizado pelos danos não patrimoniais causados pelo seu visionamento por terceiros.

Acórdão da Relação de Évora de 26 de abril de 2016
Comete o crime de gravações e fotografias ilícitas (Artigo 199º, nº 2 do Código Penal), quem monta e mantém em funcionamento um sistema de videovigilância que procede à gravação sistemática de imagens, nelas se incluindo as do acesso a uma habitação de terceiros que são inevitavelmente filmados sempre que entram ou saem de casa.

Acórdão da Relação do Porto de 14 de outubro de 2015
É legítimo proceder a uma busca domiciliária com vista à apreensão de fotografias ou filmes que se suspeita estarem nesse domicílio, em computador, telemóvel, câmara ou noutro suporte digital, se houver indícios da prática de um crime de gravações e fotografias ilícitas (Artigo 199º, nº 2, a) do Código Penal).

Acórdão da Relação do Porto de 5 de junho de 2015
O direito à imagem constitui um bem jurídico-penal tutelado em si e independentemente do ponto de vista da privacidade ou intimidade retratada. Abrange dois direitos autónomos: o direito a não ser fotografado e o direito a não ver divulgada a fotografia. O visado pode autorizar ou consentir que lhe seja tirada uma fotografia e pode não autorizar que essa fotografia seja usada ou divulgada. Contra vontade do visado não pode ser fotografado nem ser usada uma sua fotografia. Quem, contra a vontade do fotografado, utiliza uma fotografia deste, ainda que licitamente obtida e a publicita no Facebook, comete o tipo legal de crime de gravações e fotografias ilícitas (Artigo 199º nº 2 do Código Penal).

12. JOGO *ONLINE*

A decisão que se inclui em baixo relaciona-se estritamente com a regulamentação do jogo, abordando uma variante muito específica da mesma.

Acórdão da Relação de Guimarães de 2 de novembro de 2015
Não deve ser considerado como "explorador" de jogos (para efeitos do Artigo 108º, nº 1 do Decreto-Lei nº 422/89), aquele que permite que terceiros acedam à Internet, para jogarem *online* jogos de fortuna e azar, mesmo que cobre dinheiro por esse acesso dos jogadores à Internet.

13. QUESTÕES PROCESSUAIS SUBSTANTIVAS

O incremento dos crimes online trouxe com ele a discussão de questões processuais de implicação substantiva. Para já, foram questionados na jurisprudência dois aspetos: por um lado, a do momento de conhecimento, pela vítima, do crime que a atingiu. A questão é relevante, porque muitos dos crimes online são de natureza semipública, dependendo, portanto, a prossecução criminal de apresentação de queixa, em devido tempo. Por outro, foi discutida na jurisprudência a relevância do local da prática física de factos com consequências à distância. Este aspeto também é relevante, não só por razões de

natureza processual, por exemplo de competência do tribunal, mas também pela respetiva implicância substantiva.

Acórdão da Relação do Porto de 17 de fevereiro de 2016

Quando estão em causa factos relacionados com envio de SMS e conversações telefónicas (crimes por via de telemóveis), não é relevante o local onde se encontra o ofendido. Se não for indicado o local onde a ofendida se encontrava quando recebeu cada uma das SMS e cada um dos telefonemas, esse não é fundamento, por desproporcional e excessivo, de rejeição da acusação deduzida.

Acórdão da Relação de Lisboa de 17 de dezembro de 2015

O direito de queixa extingue-se no prazo de 6 meses a contar da data em que o ofendido teve efetiva noção de que poderá estar a ser vítima de um crime. Em caso de burla por meio de vendas *online*, só decorrido algum tempo sobre a compra o comprador percebe que caiu num engano ardilosamente montado e que nunca nada irá receber em troca do que pagou.

(O Gabinete Cibercrime fica grato pela indicação, para cibercrime@pgr.pt de outras decisões sobre cibercrime que não tenham sido elencadas)