MINISTÉRIO PÚBLICO
PORTUGAL
PROCURADORIA-GERAL DA REPÚBLICA
GABINETE CIBERCRIME

JURISPRUDÊNCIA SOBRE CIBERCRIME

Nota Prática nº 15/2020

24 de fevereiro de 2020

NOTA PRÁTICA nº 15/2020
24 de fevereiro de 2020

Jurisprudência sobre cibercrime

ÍNDICE

Esta nota prática sumaria as referências jurisprudenciais dos tribunais superiores referentes a cibercriminalidade e a outras criminalidades cometidos por via de sistemas informáticos. Pretendeu-se que incluísse todas as decisões publicadas e disponíveis na Internet em fonte aberta, até ao final do ano de 2019.
Na prática, recolhe uma década de decisões – no decurso de 2019 celebraram-se os dez anos da publicação, em 2009, da Lei do Cibercrime –, embora se considere também uma que outra decisão mais antiga, por se manter pertinente e por o escopo da Nota não se limitar aos tipos de crime da Lei 109/2009.

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

1 – LEI DO CIBERCRIME

FALSIDADE INFORMÁTICA

É sobre o crime de falsidade informática a mais rica e consistente jurisprudência, no contexto da Lei do Cibercrime. Em geral, as decisões incidem sobre a interpretação estrita e literal dos seus complexos elementos, mas também sobre o interesse jurídico protegidos pelo tipo de crime, tendencialmente mais identificado com a integridade dos sistemas de informação.
Anota-se preocupação da jurisprudência de correlacionar este tipo de crime, por um lado, com crimes "analógicos", ou do mundo real e, por outro, com crimes contra o património.

Acórdão do Tribunal da Relação de Lisboa de 9 de janeiro de 2019

Para que ocorra o crime de falsidade informática, os dados informáticos têm de ser alterados com o propósito de desvirtuar a demonstração dos factos que com aqueles dados podem ser comprovados.
O bem jurídico tutelado por este crime de falsidade informática não é o património, mas antes a *integridade dos sistemas de informação* através da 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.
Os crimes de peculato e de falsidade informática protegem bens jurídicos diferentes – por isso, não existe entre eles um concurso de normas ou aparente, à semelhança do que jurisprudencialmente se tem entendido no caso, esse sim paralelo, do concurso entre burla e falsificação.

Acórdão do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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.

DANO INFORMÁTICO

É ainda escassa e pouco significativa a jurisprudência específica sobre dano informático. No acórdão referenciado de seguida interpreta-se de forma lata o elemento "tornar dados informáticos não acessíveis", presente no tipo de crime do Artigo 5º, nº 1, da Lei do Cibercrime.

Acórdão do Tribunal da Relação de Lisboa de 27 de junho de 2019

Vedar o acesso da vítima à sua própria conta de correio eletrónico, com a intenção de assim a obrigar a agir de determinada forma ou a puni-la por não o fazer, basta para se considerarem verificadas as intenções de lhe causar prejuízo e de obter um benefício ilegítimo (crime de dano relativo a dados ou programas informáticos – Artigoº 5º da Lei do Cibercrime).

ACESSO ILEGÍTIMO

Desde a prolação das decisões mais antigas conhecidas sobre acesso ilegítimo que o tipo de crime vem sendo definido e delimitado pela jurisprudência de forma consistente, quanto à sua essência. Importa reter a leitura assertiva que a jurisprudência fez da evolução legal do tipo de crime de acesso ilegítimo (previsto no Artigo 6º da Lei do Cibercrime e anteriormente no Artigo 7º da Lei nº 109/91).
Da jurisprudência mais recente, anota-se um acórdão que explorou a difícil temática do local da ocorrência (consumação) de crimes cometidos em ambiente digital.

Acórdão do Tribunal da Relação de Lisboa de 27 de junho de 2019

Aceder a contas de correio eletrónico para as usar e se apresentar perante terceiros como se se tratasse do seu dono revela intenção de alcançar, para si, um benefício ou vantagem ilegítimos – indo ao encontro do tipo de crime de acesso ilegítimo (Artigo 6º da Lei do Cibercrime).

Acórdão do Tribunal da Relação de Lisboa de 26 de março de 2019

Um crime de acesso ilegítimo (Artigo 6º da Lei do Cibercrime) à caixa de correio eletrónico de uma pessoa coletiva deve ter-se como consumado na sua sede, apesar do agente ter executado o crime noutro local, através da internet.

Apesar da desmaterialização característica da sociedade moderna, as pessoas (singulares ou coletivas), continuam a ter um local onde concentram e armazenam o seu património e direitos, mesmo aqueles direitos que só se manifestam de forma desmaterializada, o que coincide, sociologicamente, com o local da residência ou da sede.
E se é verdade que se pode aceder ilegitimamente à caixa de correio eletrónico de outra pessoa a partir de qualquer sítio, dispondo de equipamento informático, ligação à internet e coordenadas de acesso, a pessoa que criou e usa uma caixa de correio eletrónico não é uma entidade virtual: é ela em concreto quem vê atingida a segurança e confidencialidade da sua correspondência.

Acórdão do Tribunal 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 do Tribunal 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 do Tribunal 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 – DIREITO DE AUTOR

Sobre esta temática geral, avultam decisões respeitantes a dois grandes núcleos temáticos: o crime de reprodução de programa protegido, previsto na Lei do Cibercrime e o crime de usurpação, previsto no Código de Direito de Autor e Direitos Conexos.
Noutra vertente, assinala-se um recente aresto sobre tema mais raro: a titularidade do direito de autor existente sobre um programa informático.

Acórdão do Tribunal da Relação de Coimbra de 10 de julho de 2019
O direito de autor de um programa informático desenvolvido por um técnico informático por conta de um empregador, pertence a este último.

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 do Tribunal 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 do Tribunal 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 do Tribunal 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.

USURPAÇÃO

A discussão jurisprudencial mais abundante 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 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).

Esta última problemática, cuja discussão foi, durante anos, balizada pelo Acórdão de fixação de Jurisprudência do STJ de novembro de 2013, sofreu recentemente uma alteração drástica, uma vez que, neste aspeto particular (da comunicação pública não autorizada de fonogramas e videogramas), por força da Lei nº 92/2019, de 4 de outubro, o crime foi convertido em contraordenação[1].

Acórdão do Tribunal da Relação de Lisboa de 5 de dezembro de 2019

A distribuição de sinal radiodifundido através de aparelhos de televisão, nos quartos e nas zonas comuns dos hotéis, constitui comunicação ao público de obras radiodifundidas.

[1] A este propósito foi emitida a Nota Prática nº 13/2019 do Gabinete Cibercrime, de 13 de dezembro de 2019, disponível no Portal do Ministério Público (http://cibercrime.ministeriopublico.pt/notas-praticas).

Acórdão do Tribunal da Relação de Lisboa de 21 de novembro de 2019

A distribuição dos canais televisivos pelos diversos quartos dos estabelecimentos hoteleiros constitui comunicação ao público e não retransmissão, independentemente de a distribuição ser feita por cabo coaxial.

Acórdão do Tribunal da Relação de Coimbra de 22 de maio de 2019

A difusão de música, em estabelecimento comercial, através de altifalantes (para ampliação do som), provinda de um canal de televisão especializado na vertente musical, inserir-se apenas no domínio da mera *receção* e não no da *recriação*. Por isso, não carece de autorização do autor da obra em causa.

Acórdão do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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.

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 e também com o crime (como) de burla, previsto no Artigo 217º do Código Penal.

Acórdão do Tribunal da Relação do Porto de 14 de dezembro de 2017

Comete crime de burla (Artigo 217º do Código Penal) quem coloca um anúncio de venda de um objeto no *Facebook*, acorda e recebe antecipado o pagamento do preço respetivo e não entrega tal objeto ao comprador – nunca tendo tido a intenção de o entregar.

Acórdão do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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.

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 do Tribunal da Relação de Lisboa de 6 de novembro de 2018
O crime de burla informática e nas comunicações (Artigo 221º, nº1, do Código Penal) protege bens jurídicos distintos dos subjacentes ao crime de roubo, justificando-se a condenação pelos dois crimes, em concurso real.

Acórdão do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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.

4 – PHISHING

A abundantíssima jurisprudência sobre phishing *disponível é, toda ela, da jurisdição cível e respeita a casos em que aquilo que se discute é 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 Tribunal da Relação do Porto de 4 de junho de 2019

Age sem culpa ou negligência o utilizador de conta bancária que, utilizando os serviços de *homebanking*, é vítima de um ataque informático, mediante o qual foram *revelados* inadvertidamente os dispositivos de segurança que haviam sido fornecidos pelo banco, o que veio a permitir uma operação de transferência de fundos não autorizada da sua conta para terceiro.

A entidade bancária 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, pelo que os riscos pela utilização normal do sistema correm por sua conta, devendo por isso suportar o prejuízo resultante da operação não autorizada pelo cliente.

Constitui ónus da prova da entidade bancária provar a ocorrência de comportamento negligente, gravemente negligente ou doloso do utilizador.

Acórdão do Tribunal da Relação de Lisboa de 11 de abril de 2019

Em casos de *phishing* bancário, não havendo um especial juízo de censura que recaia sobre o cliente do banco, é a instituição bancária que deve suportar os prejuízos resultantes da intromissão de um terceiro no sistema de pagamentos que criou.

Uma cláusula contratual geral que transferira para o cliente toda a responsabilidade pelos prejuízos resultantes da utilização indevida de serviço de *homebanking* por parte de terceiros, independentemente de tal utilização resultar do comportamento do cliente, altera as *regras de distribuição do risco* previstas na lei, sendo uma cláusula geral nula, por absolutamente proibida

Acórdão do Tribunal da Relação de Coimbra de 15 de janeiro de 2019

Na utilização de *homebanking* através da internet, não se provando que o cliente agiu com negligência grave, recai sobre o banco a responsabilidade pela movimentação fraudulenta da sua conta bancária, se terceiros vierem a aceder à conta de que é titular.

Em caso de fraude informática, não age com culpa o cliente que introduziu numa página *web* falsa, clonada da página do banco, as suas credenciais de acesso, na convicção que estava a fazê-lo na autêntica página *online* do banco.

Acórdão do Tribunal da Relação de Lisboa de 6 de novembro de 2018

No âmbito do contrato de *homebanking* a responsabilidade por operações de pagamento não autorizadas incumbe, em princípio, ao prestador de serviços de pagamento (o banco), cabendo ao ordenante (o cliente) em caso de sua negligência grave.

Não se tendo apurado ter o cliente permitido, ainda que de forma não intencional, o acesso de terceiros às suas credenciais de acesso à conta, não se pode concluir ser imputável a este a quebra da confidencialidade dos dispositivos de segurança.

Acórdão do Tribunal da Relação de Lisboa de 12 de julho de 2018

Num contrato de *homebanking*, o banco obriga-se a assegurar o acesso seguro e exclusivo do cliente à sua conta bancária.

Tendo o banco comunicado ao cliente, em vários momentos, por vários meios e formas, o modo de corretamente utilizar as credenciais de acesso ao sistema de *homebanking* e, contrariando essas regras, o cliente introduzir os códigos de acesso à conta bancária e de todos os números do cartão matriz numa página *web* com elementos semelhantes à página do banco, mas à qual chegou ao clicar numa hiperligação de um *e-mail*, constitui uma grave violação do dever de manter em segredo as credenciais em causa.

Ou seja, o cliente facultou os códigos necessários à movimentação da conta por terceiros de forma gravemente negligente, devendo por isso suportar as perdas resultantes de tais operações.

Acórdão do Tribunal da Relação de Lisboa de 10 de maio de 2018

Existindo um contrato de *homebanking,* o risco de funcionamento deficiente ou inseguro do sistema de prestação de serviços localiza-se na esfera do banco, seu prestador, a quem incumbe a responsabilidade por operações não autorizadas pelo cliente nem devidas a causa a este imputável.

Só assim não será se se provar que o cliente não cumpriu, deliberadamente, ou por negligência grave, uma ou mais das suas obrigações, recaindo sobre o prestador do serviço de pagamento, o ónus da prova de tais circunstâncias.

Acórdão do Tribunal da Relação de Évora de 12 de abril de 2018

A responsabilidade por pagamentos fraudulentos não autorizados, realizados com recurso ao serviço de *homebanking*, pertence, em princípio, ao banco. Cabe porém ao utilizador em caso de negligência grave.

Se este acedeu a uma página eletrónica fraudulenta, convencido de que se tratava da autêntica página da entidade bancária, e aí introduziu, além dos habituais número de identificação e do código *PIN*, a totalidade das coordenadas inscritas no cartão matriz, agiu com negligência grave, uma vez que tinha sido advertido de que a solicitação de mais de duas posições deste cartão indicia a presença de página fraudulenta. Impunha-se pois cautela ao titular da conta.

Acórdão do Tribunal da Relação de Lisboa de 21 de dezembro de 2017

Quanto alguém, desconhecido, acede *online* a uma conta bancária de um cliente de *homebanking* e efetua pagamentos de forma fraudulenta, não é adequado concluir, sem mais, que esta quebra de segurança é imputável ao utilizador desse serviço. Por isso, se não se demonstrar que o utilizador teve qualquer comportamento suscetível de pôr em causa a segurança do sistema (por se desconhecer como o terceiro desconhecido logrou obter as chaves de acesso à conta), o banco é responsável pelos movimentos fraudulentos, que tem que reembolsar.

São nulas e devem ser excluídas das Condições Gerais do contrato de utilização do serviço, cláusulas que estabelecem a presunção de que as operações bancárias realizadas fraudulentamente por terceiro foram consentidas e autorizadas pelo cliente.

Acórdão do Tribunal da Relação de Lisboa de 12 de outubro de 2017

Se ocorrer uma utilização fraudulenta do sistema de *homebanking* e não for demonstrado que houve, da parte do cliente, qualquer incumprimento das regras de segurança que este se obrigou a observar para utilizar o serviço, não pode ser formulado qualquer juízo de censura sobre o mesmo e, por isso, será o banco quem deverá suportar os prejuízos resultantes da intromissão de terceiros no sistema, por o seu sistema de *homebanking* não ser seguro e permitir a intromissão de terceiros.

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 possam 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 do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal da Relação do Porto de 29 de outubro de 2013

Quando ocorre um caso de *phishing*, inverte-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.

5 – CRIMES CONTRA CRIANÇAS

Quanto aos crimes de que crianças possam ser particularmente vítimas, na Internet, a jurisprudência tem tratado quase exclusivamente a pornografia de menores e os abusos sexuais, nestes se incluindo mais recentemente o crime de aliciamento de menores.

PORNOGRAFIA DE MENORES

Têm vindo a aumentar as decisões das Relações sobre pornografia de menores, o que espelhará com certeza o número de inquéritos a este propósito instaurados pelo Ministério Público. 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.

Uma das discussões jurisprudenciais mais antigas reporta-se à qualificação como crime do mero download *de ficheiros de pornografia infantil. A tendência claramente maioritária vai no sentido afirmativo.*

Acórdão do Tribunal da Relação de Lisboa de 31 de outubro de 2019

Integram o conceito de fotografias pornográficas (para os efeitos do crime previsto no Artigo 176º/1, alíneas b) e c) do CP) as fotografias que o agente tirou do "rabo e dos seios" da uma menor quando esta fazia o pino, uma vez que, sendo zonas erógenas, são capazes de produzir excitação sexual no observador.

Acórdão do Tribunal da Relação do Porto de 6 de fevereiro de 2019

Comete o crime de devassa da vida privada quem, sem autorização da pessoa visada, e estando ciente do respetivo conteúdo, intencionalmente divulga fotografias onde aquela se encontra retratada despida, em roupa interior e em poses de natureza sexual.

Acórdão do Tribunal da Relação do Porto de 7 de dezembro de 2018

O crime de *pornografia de menores* pune quem utiliza menor para a produção de material pornográfico, mas também quem distribuir este material. Pune ainda quem adquira ou detenha esse material com o propósito de o distribuir, importar, exportar, divulgar, exibir ou ceder.

Fazer *download* de imagens de pornografia de menores, de um servidor para o dispositivo informático pessoal, integra o conceito de *importar* previsto na alínea c) do nº 1 do artigo 176º do Código Penal.

Acórdão do Tribunal da Relação de Coimbra de 24 de abril de 2018

Fotografias do corpo humano só serão pornográficas se representarem a prática de ato sexual, de um qualquer enredo dessa natureza ou se traduzirem uma exposição lasciva dos órgãos sexuais. Portanto, o tipo de crime de *pornografia de menores* (artigo 176º do CP), pressupõe que se leve o menor a participar nas atividades ali descritas. Este crime não ocorre quando o agente obtém, de modo sub-reptício, dissimulado, sem conhecimento dos visados, imagens de menores desnudados.

Neste caso, pode ocorrer o crime de devassa da vida privada (artigo 192º do CP).

Acórdão do Supremo Tribunal de Justiça de 22 de fevereiro de 2018

A pornografia supõe uma representação grosseira da sexualidade, que faz das pessoas mero objeto despersonalizado para fins predominantemente sexuais, ou um desempenho de atividades sexuais explícitas, reais e simuladas, ou ainda a representação dos órgãos sexuais para fins predominantemente sexuais. A obtenção de fotografias ou imagens filmadas, em que se traduziu a troca de imagens do corpo desnudado de menor através

da aplicação *Facebook* ou da videochamada em *smartphone*, porque se trata de mera exposição corporal, de cunho não pornográfico, atentatório do livre desenvolvimento da vida sexual do menor, não consubstancia a prática do crime de pornografia de menores.

Acórdão do Tribunal da Relação de Lisboa de 20 de dezembro de 2017

A concretização de um *download* dos ficheiros de pornografia de menores, existentes num servidor num outro e a consequente transferência para um computador em Portugal, constitui uma importação, para efeito de preenchimento do elemento objetivo do tipo de crime de pornografia de menores (alínea c) do nº 1 do Artigo 176º do CP).

Acórdão do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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.

ABUSO SEXUAL DE CRIANÇAS

A generalidade das decisões incluídas nesta secção tratam as figuras do crime continuado e do chamado crime de trato sucessivo, *a propósito dos crimes de abuso sexual de crianças.*
Inclui-se ainda uma decisão inovadora, sobre o crime de aliciamento de menores para fins sexuais *(ou* grooming*), o qual chegou finalmente aos tribunais superiores, depois de ter sido introduzido na alteração legislativa ao Código Penal de 2015.*

Acórdão do Tribunal da Relação de Coimbra de 11 de dezembro de 2019

O crime de aliciamento de menores para fins sexuais (Artigo 176º-A do CP) supõe uma abordagem da criança, por qualquer meio tecnológico de informação e comunicação, como a Internet e o telemóvel. Na forma agravada (do Artigo 176-ºA, nº 2), configura já a realização de atos materiais conducentes a num encontro do agente com o menor – deslocação ao local do encontro, prestação de auxílio ao transporte da vítima, ou marcação de um espaço físico para o efeito, por exemplo.
Comete este ilícito o agente que, através de diversas mensagens enviadas a menor insinuando atos sexuais a praticar com a mesma, tenta encontrar-se com ela, dispondo-se a pagar-lhe a viagem e sugerindo-lhe boleia para um sítio onde se poderiam encontrar.

Acórdão do Supremo Tribunal de Justiça de 13 de março de 2019

A imputação de um único crime de abuso sexual ou de pornografia de menores, relativamente a cada um dos menores envolvidos, lançando mão da figura do crime de trato sucessivo, não se afigura correta. A indeterminação relativamente ao número de crimes cometidos em determinado período não deve ser colmatada com o recurso à figura do trato sucessivo.
A fase investigatória deve procurar determinar o número, ainda que elevado, de crimes cometidos.

Acórdão do Supremo Tribunal de Justiça de 20 de fevereiro de 2019

O chamado crime de trato sucessivo, figura não contemplada na lei, mais não é do que uma tentativa de ampliar a construção jurídica do crime continuado, despojando-o da marca essencial que é a realização plúrima da ação típica no quadro da solicitação de uma mesma situação exterior que diminua consideravelmente a culpa do agente.

Acórdão do Tribunal da Relação de Évora de 12 de julho de 2018

O crime de abuso sexual de criança ou adolescente, ainda que cometido várias vezes sobre a mesma vítima, está excluído da figura do crime continuado, por estarem em causa bens eminentemente pessoais.

Acórdão do Supremo Tribunal de Justiça de 22 de março de 2018

A jurisprudência do STJ, já antes maioritária, é presentemente praticamente unânime, ao afastar a figura de «trato sucessivo» dos casos de crimes contra a autodeterminação sexual do Artigo 171º e 172º do CP. O crime de "trato sucessivo" é uma criação da doutrina e também da jurisprudência para abarcar as situações de reiteração de crimes iguais ou próximos, em que se não pode falar de uma situação exterior que diminua consideravelmente a culpa do agente e, portanto, insuscetíveis de serem tratados como crime continuado.

6 – PRIVACIDADE E DIREITO À IMAGEM

A expansão das redes de comunicação e informação e o cruzamento das mesmas com os suportes audiovisuais aumentaram exponencialmente as possibilidades de violação da privacidade e de violação do direito à imagem.

No conjunto dos acórdãos referenciados avultam dois grupos referentes, respetivamente, ao crime de devassa da vida privada e ao crime de fotografias ilícitas.

Acórdão do Tribunal da Relação de Lisboa de 26 de setembro de 2019

Pode consentir-se que seja usada a respetiva imagem num programa de televisão, desde que tal resulte de uma manifestação de vontade livre, específica e informada. Não obstante, esta manifestação pode presumir-se a partir da conduta do titular desse direito à imagem (e voz), desde que esta se revele como inequívoca no sentido da aceitação da divulgação. Será o que ocorre com quem assiste à gravação de um programa de televisão, no qual é normal a captação e difusão de imagens dos espetadores.

Acórdão do Tribunal da Relação do Porto de 11 de abril de 2019

Para o direito civil, a captação não autorizada de imagens da uma residência de outra pessoa, através de um *drone* que a sobrevoou, passando essas imagens a fazer parte de um vídeo divulgado em redes sociais (sendo aí alvo de várias visualizações e partilhas), constituiu um facto ilícito (na primeira variante de ilicitude prevista no nº 1 do Artigo 483º do Código Civil).

O direito à reserva sobre a intimidade da vida privada, enquanto direito fundamental de personalidade, caracteriza-se juridicamente como inato, inalienável, irrenunciável e absoluto, no sentido de que se impõe, por definição, ao respeito de todas as pessoas. A esta luz, a reserva juscivilística envolverá, designadamente, a proibição de introdução não autorizada em casa alheia, a proibição de observação às ocultas do domicílio de outrem e das pessoas que nele se encontrem, bem como a proibição de captação fotográfica ou por qualquer outro meio de imagens da residência de cada qual, e na área, privada, que a circunda (logradouro, jardim, parque, etc.).

DEVASSA DA VIDA PRIVADA

O crime de devassa da vida privada tem sido utilizado como alternativa de incriminação de atuações paralelas à pornografia (infantil) e às fotografias ilícitas, quando as imagens em causa, não tendo cariz sexual expresso direto, retratam corpos nus.

Acórdão do Tribunal da Relação do Porto de 6 de fevereiro de 2019

Comete o crime de devassa da vida privada quem, sem autorização da pessoa visada, e estando ciente do respetivo conteúdo, intencionalmente divulga fotografias onde aquela se encontra retratada despida, em roupa interior e em poses de natureza sexual.

Acórdão do Tribunal da Relação de Coimbra de 24 de abril de 2018

Fotografias do corpo humano só serão pornográficas se representarem a prática de ato sexual, de um qualquer enredo dessa natureza ou se traduzirem uma exposição lasciva dos órgãos sexuais. Portanto, o tipo de crime de *pornografia de menores* (artigo 176º do CP), pressupõe que se leve o menor a participar nas atividades ali descritas. Este crime não ocorre quando o agente obtém, de modo sub-reptício, dissimulado, sem conhecimento dos visados, imagens de menores desnudados. Neste caso, pode ocorrer o crime de devassa da vida privada (artigo 192º do CP).

Acórdão do Tribunal da Relação de Coimbra de 13 de dezembro de 2017

Se uma vítima é filmada de forma não autorizada, não para devassar a sua intimidade, mas para vir a extorquir-lhe dinheiro, e só porque esta não fez o pagamento pretendido, frustrando a extorsão, é que o filme é, posteriormente, publicitado numa rede social, devassando a sua intimidade, deve entender-se, a existência de um concurso real entre o crime de gravações e fotografias ilícitas e o crime de devassa da vida privada.

FOTOGRAFIAS ILÍCITAS

O surgimento, nos últimos cinco anos, 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 máquinas fotográficas digitais e, sobretudo, à popularização de telefones que incorporam câmaras fotográficas. 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 é fluída, já que as duas discussões estão intrinsecamente relacionadas, afigurando-se evidentemente como as duas diferentes faces de uma mesma problemática. Quanto às questões de direito penal substantivo, 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 do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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 do Tribunal 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).

7 – 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.
À margem, destaca-se uma decisão que aborda a divulgação de dados de crianças em redes sociais.

Acórdão do Tribunal da Relação de Lisboa de 11 de julho de 2019

A mensagem que uma trabalhadora de limpeza envia, via *Facebook*, por *chat*, para uma aluna que frequenta um estabelecimento de ensino, onde a primeira trabalha, fora do tempo e do local de trabalho, a respeito de assuntos pessoais, é um ato da vida privada da trabalhadora.

Acórdão do Tribunal da Relação de Guimarães de 5 de março de 2018

A publicação no *Facebook* de uma fotografia tirada de estabelecimento comercial, em que é visível o seu nome, acompanhada dos dizeres "*Não aconselho muito*", pelo teor abstrato, ambíguo e indefinido desta afirmação, não é objetivamente ofensiva da honra e da consideração devidas ao proprietário do referido estabelecimento.
Aquela expressão não vai além do que a liberdade de expressão permite, enquanto exercício do direito de exprimir opiniões, ideias ou pensamentos, não possuindo uma carga desvaliosa suscetível de afetar o bom nome e a reputação.

Acórdão do Tribunal da Relação do Porto de 13 de setembro de 2017

A prova da titularidade da conta do *Facebook* e o conteúdo na mesma divulgado não obedece a qualquer princípio de prova legal de natureza digital, a obter através da pesquisa de dados informáticos e sua apreensão, mas está apenas submetido ao princípio da livre apreciação da prova. Quer a titularidade da conta, quer o conteúdo, podem ser demonstrados por prova testemunhal, ou por registo fotográfico ou impressão em papel do mesmo.

Acórdão do Tribunal 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 do Tribunal 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 do Tribunal 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.

8 - *STALKING*

Até à introdução, em 2015, do crime de perseguição (ou stalking*, previsto no Artigo 154-Aº do Código Penal), este tipo de comportamento apenas relevava se enquadrado nos clássicos crimes contra a integridade física ou a liberdade pessoal.*
Chegou, entretanto, a tribunal superior o stalking*. As decisões que se referenciam têm forte conexão com o ambiente digital, uma vez que, nos casos concretos, uma parte substancial das respetivas factualidades traduzia o uso de sistemas informáticos (a perseguição incluía a remessa de mensagens telemáticas).*

Acórdão do Tribunal da Relação de Lisboa de 30 de novembro de 2019

Os crimes de ameaça, falsidade informática, perseguição, uso indevido de imagem, cometidos através das redes sociais e internet são censuráveis e demonstram uma energia criminosa que nos dias de hoje é facilitada. Assim, tendo em conta as exigências de prevenção especial e geral justifica-se a pena efetiva de prisão a condutas de *cyberstalking*.

Acórdão do Tribunal da Relação de Lisboa de 16 de outubro de 2018

O crime de perseguição, ou *stalking* (Artigo 154º-A, nº 1 do Código Penal) supõe a que a vítima não deseje a conduta do agressor – este é um elemento integrante e basilar do tipo de crime, que exige que os atos persecutórios não sejam queridos, nem muito menos consentidos pela vítima, que repudia o contacto com o seu perseguidor.
Assim, se a vítima permite e consente nas investidas do *stalker*, este consentimento será um verdadeiro acordo que exclui o tipo.

9 – PROTEÇÃO DE DADOS PESSOAIS

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 – naturalmente, não existem ainda decisões sobre o novo quadro legal, da Lei nº 58/2019, de 8 de agosto).

Assinala-se, em particular, a mais recente decisão nesta temática, que incide sobre o tipo de crime de acesso indevido a dados e o enquadra com enorme abrangência.

Acórdão do Tribunal da Relação de Lisboa de 7 de março de 2018

Tanto comete o crime de acesso indevido a dados pessoais (da Lei de Proteção de Dados Pessoais) aquele que, por si, cria um ficheiro de dados automatizados como aquele que mantém um ficheiro automatizado daquele tipo, mesmo que não seja por ele criado, ou ainda o que utiliza um qualquer ficheiro informático, tendo acedido a ele por qualquer forma.

Acórdão do Tribunal 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 do Tribunal 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 - 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 gerais: 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 lado, 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 do Tribunal da Relação de Lisboa de 26 de março de 2019

Um crime de acesso ilegítimo (Artigo 6º da Lei do Cibercrime) à caixa de correio eletrónico de uma pessoa coletiva deve ter-se como consumado na sua sede, apesar do agente ter executado o crime noutro local, através da internet.

Apesar da desmaterialização característica da sociedade moderna, as pessoas (singulares ou coletivas), continuam a ter um local onde concentram e armazenam o seu património e direitos, mesmo aqueles direitos que só se manifestam de forma desmaterializada, o que coincide, sociologicamente, com o local da residência ou da sede.

E se é verdade que se pode aceder ilegitimamente à caixa de correio eletrónico de outra pessoa a partir de qualquer sítio, dispondo de equipamento informático, ligação à internet e coordenadas de acesso, a pessoa que criou e usa uma caixa de correio eletrónico não é uma entidade virtual: é ela em concreto quem vê atingida a segurança e confidencialidade da sua correspondência.

Acórdão do Tribunal 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 do Tribunal 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)