NEWSLETTER

CONSELHO REGIONAL DE COIMBRA

FEVEREIRO 2023

ARTIGO

Cibercriminalidade e as dificuldades da investigação

EDITORIAL

Teresa Letras

Presidente do Conselho Regional de Coimbra

ENTREVISTA

Teresa Sobral, advogada de Viseu

LEGISLAÇÃO | JURISPRUDÊNCIA | FORMAÇÃO

EDITORIAL

Teresa Letras
Presidente do Conselho Regional de Coimbra da Ordem dos Advogados

Caras e Caros Colegas,

Volvido cerca de um mês sobre a tomada de posse, é tempo de retomar a publicação da Newsletter do Conselho Regional de Coimbra e de, através dela, levar até vós informação mais relevante para o exercício da nossa atividade, acompanhada de reflexões, entrevistas, estudos e outros textos de caráter científico.

Regozijamo-nos com o facto de, em cada edição, podermos contar com o inestimável contributo e ensinamentos de personalidades de reconhecido prestígio profissional e académico, qual prova viva do por nós professado entendimento de que a via essencial para a afirmação dos Advogados é a da qualificação, diria mesmo, da qualificação de excelência.

Queremos continuar a partilhar com os/as Colegas as preocupações, as problemáticas, as ideias e os projetos que norteiam e preenchem a atividade do Conselho, em torno dos quais desenvolvemos o nosso trabalho, nunca por nunca deixando de ter presente que a colaboração que nos possa ser dada por cada um de vós constitui não apenas a concretização da participação ativa que preconizamos como modelo de reforço e afirmação institucionais, mas também um verdadeiro estímulo ao exercício das competências estatutárias que se nos mostram atribuídas.

Queremos fazer mais e melhor! Queremos ser a voz dos Advogados e Advogadas da nossa área de circunscrição territorial e, acima de tudo, procurar as soluções para os problemas e para os obstáculos que sejam opostos ao respetivo exercício profissional. Para tanto precisamos que cada Advogado e cada Advogada seja um verdadeiro *IP* de uma vasta rede de comunicação, qual dispositivo de máxima eficiência na transmissão de informação, que nos habilite a intervir pronta e eficazmente em todos os cenários em que a mesma se imponha. Contamos com todos e cada um de vós nesta missão que nos propusemos abraçar ao longo destes três anos.

Não obstante tenhamos a consciência de que o caminho é espinhoso, não vacilaremos no propósito, nem na ação. Procuraremos ver nas vicissitudes e nos reveses com que venhamos a ser confrontados, oportunidades de melhoria na abordagem das questões.

Foi assim, agora, face ao teor do Acórdão n.º 60/2023, de 27 de Fevereiro, por via do qual o Tribunal Constitucional decidiu pronunciar-se pela constitucionalidade das normas do Decreto n.º 30/XV da Assembleia da República, o qual procede à alteração da Lei n.º 2/2013, de 10 de Janeiro, que estabelece o regime jurídico de criação, organização e funcionamento das associações públicas profissionais.

Diga-se, aliás, que o pedido de fiscalização preventiva da constitucionalidade de um conjunto de normas constantes do Decreto n.º 30/XV da Assembleia da República, submetido pelo Sr. Presidente da República à apreciação do Tribunal Constitucional não constituiu, em momento algum, elemento tranquilizador no que respeita ao que reputamos como questão fundamental suscitada pelas alterações já aprovadas. Na verdade, fora do acervo normativo apresentado para sindicância do Tribunal Constitucional ficaram as normas relativas à constituição das sociedades multidisciplinares, verdadeira e letal ameaça ao reduto matricial diferenciador da advocacia: o sigilo profissional. Por essa razão, augurava-se, já então, como agora, a

necessidade de terçar armas e de unir esforços na busca de uma solução que minore os malefícios decorrentes de uma visão cegamente liberal da *polis*, que privilegia o "Deus mercado" que tudo regula, ao ponto de se dispensar a autorregulação, apanágio das ordens profissionais. Uma solução que convoca ativamente a Ordem dos Advogados, indubitavelmente também os órgãos regionais que a integram, chamados a participar não para suprir omissões de passado, mas para construir as respostas que se exigem para o futuro.

No que a nós, Conselho Regional de Coimbra, respeita, não regatearemos esforços num exercício que é, acima de tudo, de espírito de serviço, em benefício de todos os Advogados e Advogadas, da Advocacia e da Justiça, da Cidadania e do Estado de Direito.

Um abraço da Colega,

Teresa Letras

ARTIGO

Cibercriminalidade e as dificuldades da investigação

Dr.ª Lígia Salbany
Procuradora da República

1. Introdução

A globalização que a evolução tecnológica e o aparecimento / desenvolvimento da Internet e correspondente WEB (World Wide Web), nos seus diversos patamares[1], permitiram, através da facilidade de acesso ao mundo virtual, quase instantaneamente e à escala planetária, por um número indeterminado de pessoas, com anonimato garantido[2], embora tenha facilitado o nosso quotidiano alterou radicalmente o conceito ínsito à criminalidade clássica, trazendo novos desafios para a justiça penal, mormente no âmbito da regulamentação, investigação e combate da denominada cibercriminalidade.

Tal como preconizou Faria Costa na ida década de 90, precisamente no limiar da hodierna Sociedade da Informação: *"A informação automatizada é uma realidade tão essencial que se, por hipótese - e não se está, por certo, a entrar no domínio da ficção científica -, se bloqueasse, totalmente e à escala mundial, o fluxo informacional automatizado, ainda que por breves*

[1] *1.º - académico - ARPANET (Advanced Research Projects Agency Network); 2.º luta pelos nomes de domínio ou domain names – Panfletoware; 3.º transacional – surgimento de empresas de compra e venda de serviços (eBay, Amazon e tipo .com); 4.º social ou de experiência, através das denominadas redes sociais (Facebook, Twitter, Instagram…).*

[2] *Designadamente através de programas específicos de ocultação do browser atrás do proxy do servidor, tais como o Anonymizer, o Anonymicer, o Freedom e, mais recentemente, o Microsoft 365 Defender, para anonimização de dados da Nuvem, assim como outros destinados a ocultar a localização de endereços IP, tal como o IP Spoofing, consistente num malware destinado a mascarar endereços IP com vista a ocultar a identificação do remetente, usurpando endereços de terceiros ou forjando os originais.*

horas, todos convêm em considerar que o caos se institucionalizaria. Ora, uma realidade tão importante, tão essencial para se empregar a expressão exata, que gera e suporta interesses materiais de somas astronómicas, rapidamente se impõe, repete-se, como uma questão a que o direito penal, se bem que em ultima ratio, não pode ficar indiferente."[3].

Esta dependência universal da informação automatizada produzida, transmitida e (exponencialmente) multiplicada no Ciberespaço[4], à escala mundial e sem fronteiras, conectando-nos a uma velocidade astronómica, se bem que indispensável e essencial ao desenvolvimento pessoal, social e económico tem acoplado um lado perverso, por vezes muito negro, por força da facilitação da atividade dos agentes dos mais diversos tipos de crime, contribuindo exponencialmente para o incremento e diversificação de condutas criminosas cujo combate veio alterar radicalmente o paradigma da investigação criminal, convocando diversos outros desafios, mormente no âmbito da Cibersegurança e da Proteção de Dados, de molde a assegurar os direitos fundamentais dos cidadãos cuja fruição, por definição, cabe primordialmente ao Estado garantir e proteger.

2. Definição de Cibercrime

Conceptualmente não existe uma definição unívoca das expressões "cibercrime" e "cibercriminalidade", nascidas com a Convenção sobre o Cibercrime de 2001[5] e introduzidas na nossa nomenclatura jurídica desde a entrada em vigor da Lei n.º 109/2009, sendo inúmeros os seus sinónimos: crime tecnológico, crime informático, crime virtual, High-Tech crime,

[3] *Costa, José Francisco de Faria, algumas reflexões sobre o estatuto dogmático do chamado "Direito Penal Informático", in Direito Penal da Comunicação, alguns escritos, Coimbra Editora, 1998, página 116.*

[4] *Também conhecido como o 5.º Golbal Common (espaço comum), conceito que Barry Posen define como "espaços que não estão sob o controlo direto de qualquer Estado, mas que são vitais para o acesso e ligação a quaisquer pontos do mundo" (citado por Viana, Vítor Rodrigues, in "Cibersegurança", idn Nação e Defesa, Instituto da Defesa Nacional, Revista Quadrimestral, n.º 113, página 5.).*

[5] *Na antiga lei 109/91 eram utilizadas as expressões "crime informático" e "criminalidade informática".*

computer-related crime, entre outras denominações atualmente em uso.

Segundo a Comissão Europeia: *"O crime cibernético consiste em atos criminosos cometidos online por meio de redes de comunicações eletrónicas e sistemas de informação.*

A UE implementou leis e apoia a cooperação operacional através de ações não legislativas e financiamento.

O cibercrime é uma questão sem fronteiras que pode ser classificada em três grandes definições:

- *crimes específicos da Internet, como ataques contra sistemas de informação ou phishing (por exemplo, sites bancários falsos para solicitar senhas que permitam o acesso às contas bancárias das vítimas);*
- *fraude e falsificação online: fraudes em larga escala podem ser cometidas online por meio de instrumentos como roubo de identidade, phishing, spam e código malicioso;*
- *conteúdo online ilegal, incluindo material de abuso sexual infantil, incitação ao ódio racial, incitação a atos terroristas e glorificação da violência, terrorismo, racismo e xenofobia.*

Muitos tipos de crimes, incluindo terrorismo, tráfico de seres humanos, abuso sexual de crianças e tráfico de drogas, passaram para a Internet ou são facilitados pela Internet. Como consequência, a maioria das investigações criminais tem uma componente digital.

As leis e ações da UE visam:

- *melhorar a prevenção, investigação e repressão de crimes cibernéticos e exploração sexual infantil;*
- *desenvolver capacidades na aplicação da lei e no judiciário;*
- *trabalhar com a indústria para capacitar e proteger os cidadãos."*[6].

[6] *"Cybercrime consists of criminal acts committed online by using electronic communications networks and information systems. The EU has implemented laws and supports operational cooperation through non-legislative actions and funding.*
Cybercrime is a borderless issue that can be classified in three broad definitions:

Ilustrando a amplitude e dinâmica do conceito, no Relatório Europol do ano 2021, com objeto no «Internet Organised Crime Threat Assessment (IOCTA)», aponta-se o seguinte: *"No relatório deste ano, o impacto da pandemia de COVID-19 permanece visível. Os cibercriminosos continuaram explorando as oportunidades criadas por bloqueios e teletrabalho contínuo. Os programas de afiliados de ransomware ganharam destaque e estão vinculados a uma infinidade de ataques de alto perfil contra instituições de saúde e provedores de serviços. Operadores de malware móvel e fraudadores alavancaram a crescente dependência de serviços de compras online e estão cada vez mais usando-os como parte de seu modus operandi para acessar as contas bancárias de suas vítimas. As crianças que passam mais tempo online tornam-se mais suscetíveis ao aliciamento, levando a um aumento de material de exploração autoproduzido. Muitas das ameaças no cenário do crime cibernético são exacerbadas pelo crescimento do serviço crime-as-a-service na Dark Web. As ofertas do serviço malware-as-a-service e o leilão de dados furtados/usurpados possibilitam o planeamento de ataques futuros. Os criminosos também continuam melhorando sua segurança operacional ao abusar de serviços de comunicação criptografados de ponta a ponta e criptomoedas."*[7]. O que destaca o facto

· crimes specific to the internet, such as attacks against information systems or phishing (e.g. fake bank websites to solicit passwords enabling access to victims' bank accounts);
· online fraud and forgery: large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code;
· illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenofobia.

Many types of crime, including terrorism, trafficking in human beings, child sexual abuse and drugs trafficking, have moved online or are facilitated online. As a consequence, most criminal investigations have a digital componente.

EU laws and actions aim to:
· improve the prevention, investigation and prosecution of cybercrime and child sexual exploitation;
· build capacity in law enforcement and the judiciary;
· work with industry to empower and protect citizens." (tradução Google).

[7] Tradução Google do original - internet_organised_crime_threat_assessment_iocta_2021.pdf *"(…) In this year's report, the impact of the COVID-19 pandemic remains visible. Cybercriminals have continued exploiting opportunities created by lockdowns and continued teleworking. Ransomware affiliate programs have increased in prominence and are tied to a multitude of high-profile attacks against healthcare institutions and services providers. Mobile malware operators and fraudsters have leveraged the increased reliance on online shopping services and are*

de se tratar de uma definição ainda em construção.

Acompanhando o conceito (formal) fornecido pelo artigo 11.º, n. º1, alíneas a), b) e c) da Lei 109/2009, de 15 de setembro, doravante Lei do Cibercrime, temos os crimes especificamente aí previstos (alínea a); os crimes cometidos por meio de um sistema informático (alínea b); ou os crimes cuja investigação exija a recolha de prova em suporte eletrónico, ou seja, de prova digital (alínea c).

Contudo, a definição que nos parece mais feliz, em correspondência com as inerentes dificuldades conceptuais, amplitude e latitudes possíveis de densificação do respetivo conceito, será a que nos é proposta por Pedro Verdelho[8], através da distinção de três principais grupos de crimes:

· crimes que embora sejam cometidos on-line, por via de computadores ou sistemas de computadores, apenas se distinguindo dos crimes tradicionais pelo meio utlizado para a sua prática (e.g burla praticada pela internet; injúria /difamação por mensagem de correio eletrónico ou através de mensagem difundida através de uma rede social; crimes de ódio, branqueamento com recurso a uma conta bancária titulada num banco virtual; aliciamento de menores).

· Crimes gerados em ambiente informático que se distinguem dos crimes tradicionais pela circunstância de só poderem ser cometidos por meio informático (e.g: crimes de burla informática e devassa informática).

· Crimes informáticos em sentido estrito, praticados contra o meio informático (e.g: dano informático, acesso ilegítimo, interceção ilegítima, sabotagem informática, entre os

increasingly using it as a part of their modi operandi to access their victims' bank accounts. Children spending more time online has made them more susceptible to grooming, leading to an increase of self-produced exploitation material. Many of the threats in the cybercrime landscape are exacerbated by the growing crime-as-a-service market on the Dark Web. Malware-as-a-service offerings and the auctioning of people's stolen data enable the planning of future attacks. Criminals also continue improving their operational security by abusing end-to-end encrypted communication services and cryptocurrencies. (…)".

[8] *Verdelho, Pedro, Cibercrime, in Direito da Sociedade da Informação, Vol. IV, Associação Portuguesa do Direito Intelectual, Coimbra Editora, 2003, pág.348.*

demais especificamente tipificados na Lei do Cibercrime).

Pese embora a diversidade de ações suscetíveis de integrarem o conceito sob análise, dúvidas não restam, para esse efeito, da indispensabilidade do recurso a um computador ou outro qualquer equipamento, dispositivo ou rede /sistema informático com conectividade em ambiente digital, ou seja, no âmbito do Ciberespaço, tantas vezes apontado como o quinto domínio operacional, à semelhança da terra, do mar e do espaço[9].

3. O Combate ao Cibercrime

A comunidade internacional há muito que vem cooperando na luta contra o cibercrime, numa estratégia a nível global, em conformidade com a extensão do fenómeno e os danos que vem provocando na sociedade, não sendo Portugal exceção.

Neste contexto, em 23 de novembro de 2001, o Conselho da Europa adotou a **Convenção sobre o Cibercrime**, assinada em Budapeste, de onde constam três objetivos fundamentais:

"(1) a harmonização dos elementos relativos a infrações no contexto do direito penal substantivo de âmbito nacional e das disposições conexas na área da cibercriminalidade, (2) a definição, ao abrigo do Código do Processo Penal interno, dos poderes necessários para investigar e intentar ações penais relativamente a tais infracções, assim como a outras infracções cometidas por meio de um sistema informático ou às provas com elas relacionadas e existentes sob a forma eletrónica,

(3) a implantação de um regime rápido e eficaz de cooperação internacional."[10].

Nessa sequência, através da Resolução da AR n.º 88/2009, publicada no Diário da República, 1.ª Série, n.º 179, de 15 de

[9] *Craig, Anthony e Valeriano, Brandon, Realism and Cyber Conflict: Security in the Digital Age, 2018, pág. 1 (Cyberspace is now considered the fifth domain of warfare after land, sea, air, and space - Economist 2010). Steiger, S., et al., Conceptualising conflicts in cyberspace. Journal of Cyber Policy, Vol. 3, Issue 1, pág. 85.*

[10] *Cfr. Minuta Portuguesa do Relatório Explicativo da Convenção Cibercrime (STE N.º 185), ponto III – 16 - https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese-ExpRep.pdf*

setembro, foi aprovada a Lei n.º 109/2009 – Lei do Cibercrime, que transpôs para a ordem jurídica interna a decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

Este diploma constitui uma ferramenta de relevo para a investigação da cibercriminalidade, designadamente através da **preservação expedita** de dados, incluindo dados de tráfego (artigo 12.º); **revelação expedita** de dados de tráfego (artigo 13.º); **injunção** para apresentação ou concessão do acesso a dados armazenados num sistema informático (artigo 14.º); **pesquisa** de dados informáticos num sistema informático (artigo 15.º); **apreensão** de dados informáticos em tempo real, mormente no decurso de pesquisa informática (artigo 16.º); **apreensão** de mensagens de correio eletrónico e registos de comunicações semelhantes (artigo 17.º); **interceção e registo** de dados informáticos de conteúdo e de tráfego (artigo 18.º); recurso a **ações encobertas** previstas na Lei 101/2001, de 25 de agosto (artigo 19.º); cooperação internacional (artigos 20.º a 26.º e 29.º).

4. Constrangimentos da Investigação da Cibercriminalidade

4.1. O cariz transfronteiriço, a deslocalização e a diversidade de regulamentação

Devido à globalização deste fenómeno, consabidamente enquadrado como um **delito à distância**, visto que o ciberespaço constitui um mundo sem fronteiras, é natural que se coloquem problemas de aplicação da lei no espaço, tanto a nível internacional, como nacional, o que convoca a necessidade de adequação do princípio da territorialidade e da afinação da cooperação policial e judiciária internacionais.

Com efeito, aproveitando a brandura da legislação penal de outros sistemas jurídicos, designadamente no que se reporta à panóplia de condutas que, para o efeito, tipificam, procedimentos e metodologias de investigação, regimes

de extradição e grau de cooperação internacional que estipulam, muitos agentes deste tipo de criminalidade estabelecem estratégias de atuação cirurgicamente destinadas a dificultar ou mesmo impedir a ação penal, com vista à continuação da atividade criminosa e manutenção do *status quo* de impunidade que ardilosamente lograram atingir.

Neste conspecto, deixou o local da prática do crime de estar referenciado a determinado espaço físico, podendo a conduta delituosa ser facilmente perpetrada em qualquer latitude do (para muitos) paradisíaco mundo virtual, mediante a deslocalização de conteúdos entre servidores, naturalmente para servidores alojados em Estados com legislações mais favoráveis, preferencialmente onde as pretendidas condutas não sejam penalmente tipificadas e punidas, tal como acontece nos servidores *off-shore*, "zonas francas" ou "paraísos cibernéticos", com o objectivo dos Ciber delinquentes se furtarem à *longa manus* da justiça.

O artigo 27.º da Lei do Cibercrime, com fundamento nos princípios da nacionalidade, territorialidade, defesa dos interesses nacionais e aplicação universal (independentemente da nacionalidade do agente, do local dos factos ou do objeto da ação), prevê, no seu n.º 1 (alíneas a. a d.), que salvo tratado ou convenção internacional em contrário é aplicada a lei penal Portuguesa: (i) aos factos praticados por Portugueses, se não lhes for aplicada a lei penal de outro Estado; (ii) aos crimes fisicamente praticados em território Português ainda que visem sistemas informáticos localizados fora território Português; (iii) aos crimes que visem sistemas informáticos localizados em território português, independentemente do local onde esses factos forem fisicamente praticados; (iv) aos crimes cometidos em benefício de pessoas coletivas com sede em território Português.

No n.º 2, recorrendo ao princípio da aplicação convencional da lei penal entre Estados Membros da União Europeia, estabelece que em caso de

competência simultânea de tribunais portugueses e de tribunais de outro Estado membro da União Europeia, pode, em qualquer um deles, ser validamente instaurado ou prosseguido o procedimento penal com base nos mesmos factos.

Em caso de dúvida, estabelece a competência do tribunal onde primeiramente tiver havido notícia do crime, nos termos do n.º 4 do mesmo preceito.

4.2. A permanência, automatismo e disseminação da conduta criminosa vs. o incremento exponencial dos danos.

O avanço tecnológico verificado no mundo digital, aliado à dinâmica própria dos computadores e da World Wide Web conduziu à permanência da conduta criminosa, através da sua repetição automática e célere disseminação no ciberespaço, tornando possível ao agente deste tipo de crimes, através do *« "efeito cascata" ou do "efeito dominó", consequência da interligação de todos os sectores da sociedade à rede»*[11], a eternização do facto criminoso com recurso a um simples *click*, multiplicando-o pelo universo dos seus utilizadores e incrementando exponencialmente os seus efeitos danosos, com lesão de número quase ilimitado de vítimas e/ou lesão da mesma vítima, repetidamente, a cada novo acesso. Tal cenário, consequentemente, conduz a que o mero acesso à rede de Internet configure, potencialmente e em si mesmo, de forma automática, um elevado risco, minando a segurança e a confiança dos utilizadores da rede e assim constituindo mais uma dificuldade para a investigação, sobretudo por via do elevado número de vítimas e do grau de danosidade para o tecido socioeconómico.

De facto, a potenciação dos danos (materiais e morais) assim causados são fonte de grande preocupação,

[11] *Marques, Vera Elisa – A problemática da investigação do Cibercrime, pág. 73, citando Rodrigues, Benjamim Silva, - Direito Penal Especial, Direito Penal Informático-Digital, Coimbra, 2009, pág. 237 (disponível in http://www.datavenia.pt/ficheiros/edicao01/datavenia01_p063-088.pdf).*

considerando, segundo as palavras de Vera Marques (op. citada), que a *"(…) extensa e alta lesividade provocada pelos crimes informáticos ultrapassa em muito a dos crimes tradicionais",* a par da *"(…) sua rentabilidade, pois o investimento é mínimo em relação ao lucro ou benefício que daí poderá advir, à economia de esforço permitida pelo automatismo e ao potencial elevado número de vítimas que a transnacionalidade faculta."*.

4.3. O sentimento de segurança e de impunidade dos cibercriminosos

Uma vez que a Sociedade de Informação não tem fronteiras gera-se um clima de "terra sem lei", de quase garantida impunidade e grandemente incentivador dos agentes da cibercriminalidade, para o que igualmente muito contribui o anonimato que a Internet permite, circunstancialismo que se erige como mais uma dificuldade da investigação.

4.4. A especial preparação dos agentes da Cibercriminalidade vs. fragilidades dos investigadores

O avanço estrondoso das tecnologias da informação (TI) e das tecnologias da informação e da comunicação (TIC), cujo acesso exige conhecimentos, preparação, recursos e disponibilidade financeira, encontrando-se os meliantes do cibercrime quase sempre um passo à frente dos investigadores, sobretudo em função da escassez de peritos especificamente capacitados, máxime na área pericial, a par da falta ou insuficiência dos adequados meios materiais e tecnológicos, numa clara desproporção de conhecimentos e recursos geradora de um quadro de manifesto desequilíbrio, incrementado pela possibilidade de acesso através de computadores localizados em espaços públicos - como no caso dos cibercafés, navegação na Deep Web e, dentro desta, na Dark Web, através de aplicativos de rede TOR, acrónimo para "The Orion Router"[12], onde não é possível a

[12] *Originalmente, este aplicativo teve como objectivo permitir ao utilizador navegar com a máxima privacidade, através do* ***bloqueio de rastreadores****, impedindo a coleta de informação necessária à identificação dos sites*

indexação dos sites e redes por mecanismos de busca, garantindo o anonimato dos seus agentes e impedindo o respetivo seguimento no ciberespaço - figuram como constrangimentos que decisivamente muito dificultam a investigação criminal, com elevada taxa de sucesso.

4.5. A impreparação dos utilizadores-vítimas da cibercriminalidade e respetiva desproteção jurídica

A falta de conhecimentos e impreparação de uma larga fatia de utilizadores da Internet, qualificando-os como "presas fáceis" dos agentes da Cibercriminalidade, muitos dos quais infiltrados na rede como utilizadores de boa-fé, muito tem contribuído para o aumento estatístico deste tipo de criminalidade dificultando a tarefa dos investigadores. Efetivamente, as características de grande parte das vítimas torna indispensável equacionar uma abordagem mais cuidada, mais preparada e mais profissional, tendo em conta a espectável incipiência da sua colaboração com a investigação, por força da iliteracia de que padecem – a nível geral e informático - mormente considerando a incapacidade para a preservação de elementos probatórios relevantes para a investigação, já sem falar da elevada probabilidade deste perfil de vítima representar um destinatário fácil dos meliantes que operam no espaço digital, normalmente dotados de competências informáticas muito acima da média.

A par do acima referido circunstancialismo, a desproteção legal das vítimas do cibercrime, principalmente das mais frágeis, também redunda numa imensa dificuldade investigatória, atenta a conexão existente entre este *handicap* e a proteção de (alguns) agentes do crime travestidos de utilizadores cumpridores, paradoxo que inexplicavelmente os beneficia, em detrimento das suas vítimas.

visitados pelo utilizador durante a navegação na rede; ***inibição de impressão digital*** *(fingerprinting), impedindo o acesso e consulta de informações reais e a identificação de um perfil, com recurso ao fornecimento de dados padrão que igualizam todos os restantes utilizadores da rede, obstando a tal identificação;* ***criptografia****, impedindo a interceção e identificação da origem dos dados.*

4.6. A problemática da Cooperação Judiciária

Embora a cooperação judiciária se mostre fulcral na luta contra o Cibercrime, sobretudo face ao seu enquadramento como **delito à distância**, conforme já anotado, não raras vezes acontece que os constrangimentos verificados neste âmbito acabam por constituir um entrave de relevo para a investigação, à semelhança do que sucede relativamente a outros tipos de criminalidade.

Com efeito, nem sempre é fácil a articulação entre Estados com diferentes ordens e sistemas jurídicos, designadamente no âmbito da dicotomia *civil law / common law*, a par das competentes soberanias e opções de política criminal, gerando divergências que por vezes não é possível compatibilizar.

Pese embora isso, impõe-se salientar o labor da comunidade internacional e as várias vitórias alcançadas no âmbito da uniformização legislativa e procedimental na luta contra a cibercriminalidade organizada transnacional, esforço conjunto que a Convenção sobre o Cibercrime (2009) cristalinamente espelha, afigurando-se este instrumento como um passo importante para atingir uma mais eficaz cooperação internacional, sopesando a harmonização conseguida no direito interno dos Estados que a ratificaram, como foi o caso de Portugal.

Em conformidade com o disposto no artigo 8.º da Constituição Portuguesa e nos termos da doutrina dominante e da interpretação perfilhada, recorrentemente, pela jurisprudência do TC[13], a Convenção sobre o Cibercrime assume *"eficácia infraconstitucional, muito embora supralegal"*[14], em cujos termos *"o direito infraconstitucional anterior contrário é substituído pelas normas internacionais recebidas na*

[13] *Ac. n.ºs 32/88, 168/88, 494/99, 522/2000, 384/2005, 117/2008 e 444/2008, citados no Estudo "A ratificação de tratados internacionais, uma perspetiva de direito comparado", EPRS - Direção-Geral dos Serviços de Estudos do Parlamento Europeu, Unidade Biblioteca de Direito Comparado PE 630.294 – Novembro 2018, pág. 10 - disponível em https://www.europarl.europa.eu/RegData/etudes/STUD/2018/630294/EPRS_STU(2018)630294_PT.pdf*

[14] *Idem.*

ordem jurídica e que estas, enquanto vigorarem, impedem a formação eficaz de ato ordinário posterior que se lhes oponha.

Já quando em confronto com norma constitucional, a conclusão é distinta visto não poder o acordo aplicar-se quando contenda com a Lei Fundamental, qualquer que seja o preceito de que se esteja em presença."[15].

Sendo a Cibercriminalidade um fenómeno global impõe-se que o seu combate opere com recurso à denominada Ciber Cooperação, sendo que em Portugal muitos esforços têm sido envidados nesse sentido, sobretudo a partir da entrada em vigor da Lei do Cibercrime (Lei n.º 109/2009, de 15 de Setembro) que na atual redação, conferida pela Lei n.º 79/2021, de 24-11, dedica todo o Capítulo IV à Cooperação internacional (artigos 21.º a 26.º), investindo, desde a primeira versão, a Polícia Judiciária como Ponto de Contacto Permanente para a Cooperação internacional, **vinte e quatro horas por dia, sete dias por semana** (cfr. artigos 21.º e 29.º), destacando-se, neste diploma, a competência, em caso de urgência ou perigo na demora, com vista à preservação expedita de dados, recolha de prova e localização de suspeitos.

Atenta a relevância para a investigação da Cibercriminalidade, mais destacamos, no mesmo contexto, a regulamentação da preservação e revelação expedita de dados informáticos (artigo 22.º); o acesso a dados informáticos (artigo 24.º); o acesso transfronteiriço a dados informáticos armazenados quanto publicamente disponíveis ou com consentimento (artigo 25.º); e a interceção de comunicações (artigo 26.º).

4.7. A prova digital

A prova digital e a forma pela qual é recolhida para efeitos probatórios no âmbito do processo penal assume–se como outra importante dificuldade da

[15] *Idem.*

investigação, por força do regime da prova proibida contido nos artigos 125.º e 126.º do Código de Processo Penal e do mecanismo de efeito-à-distância[16] (artigo 122.º do Código de Processo Penal), em obediência a princípios constitucionais fundamentais conducentes à proteção e tutela dos correspondentes direitos dos cidadãos, cuja violação não é admissível nem suposto suceder num Estado de Direito Democrático, como é o nosso.

Exige, pois, cuidada análise e ponderação, tendo sobretudo em conta, em especial na área da cibercriminalidade, o elevado grau de intrusão acoplado à obtenção da prova em ambiente digital.

O regime de proibição de prova constante dos artigos 125.º e 126.º do Código de Processo Penal, constitui um verdadeiro limite à descoberta da verdade material, o que à partida parece poder configurar (para alguns) um constrangimento de relevo no âmbito do sistema processual penal português, que é um sistema misto, assentando numa estrutura acusatória não absoluta, mitigada pelo princípio da investigação, com o objectivo último de alcançar a verdade material e, consequentemente, a realização da justiça.

Contudo, estamos certos que o regime de proibição de prova deve ser entendido, desde logo em obediência ao artigo 32/n.º 8 da nossa Lei Fundamental, acompanhando João Conde Correia quando defende que *" (…) num Estado de Direito a descoberta da verdade não é um valor absoluto (…)"*, apresentando-se as proibições de prova como *"(…) compreensíveis (…) ao total esclarecimento daquela (…)"*, e concluindo estar *" (…) em causa apenas o regular funcionamento do processo de forma a que ele decorra segundo as formalidades previstas na lei"*.[17]

[16] *O qual, com base no princípio Americano do" fruto da árvore envenenada" (fruit of poisonous tree), em abstrato, estende à prova secundária indiretamente obtida, através da prova inicial ou da primeira prova, a proibição que recai sobre esta última, inquinando-a com o mesmo vício – a nulidade, mediante o efeito.*

[17] *Correia, João Conde, a distinção entre prova proibida por violação dos direitos fundamentais e prova nula numa perspetiva essencialmente jurisprudencial. Revista do CEJ, 1.º Semestre/2006, n.º 4, n.º especial, páginas 178-184.*

Pese embora a nossa posição sobre a imprescindibilidade da proibição de prova, em conformidade com a norma do n.º 8 do artigo 32.º da CRP, o **efeito-à-distância** decorrente da teoria Americana, também defendida na Alemanha, da "**árvore envenenada**" (**Fruit of Poisonous tree /Fernwirkung des Beweisverbots)**, preconizando o **efeito dominó** da nulidade da prova inicial relativamente à prova secundária obtida por via da primeira prova, pode, em concreto, dificultar a investigação da cibercriminalidade, designadamente, s.m.o, por precipitação de raciocínio do interveniente processual a quem interessar tal desfecho.

Entendemos, assim, acolhendo a lição de Helena Morão, que para a valoração da prova secundária "*(…) é necessário que exista um clean path, um caminho lícito (…)*. Nada obstando *"(…) a que as provas mediatas possam ser valoradas quando provenham de um processo de conhecimento independente e efectivo, uma vez que não há nestas situações qualquer relação de causalidade entre o comportamento ilícito e a prova mediatamente obtida"*.[18]

Quanto ao efeito dominó, o TC[19], no seguimento de uma profícua e muito interessante análise do desenvolvimento da teoria doutrinal em apreço no direito Americano e da evolução da Jurisprudência do Supremo Tribunal norte-americano, concluiu estarem em causa *"(…) soluções próprias de uma ordem jurídica que é substancialmente diferente da nossa, o que não impediu tal doutrina de nos influenciar. Muitas destas soluções não têm nem poderiam ter correspondência no nosso direito. Porém, o que importa reter – e que nos permitirá avançar na subsequente indagação – é que a doutrina, amplamente citada neste processo pelo recorrente e pelos diversos tribunais recorridos, dos «frutos da árvore*

[18] *Morão, Helena, in "Efeito –à –distância das Proibições de Prova no Direito Processual Português", Revista Portuguesa de Ciência Criminal, Ano 16, n.º 4, pág. 614.*
[19] *Acórdão n.º 198/2004 do Tribunal Constitucional de 9 de Março de 2004, disponível in https://www.tribunalconstitucional.pt/tc/acordaos/20040198.html (Processo n.º 39(04, 1.ª Secção, Relator: Conselheiro Rui Moura Ramos).*

venenosa», nunca teve, na sua origem e desenvolvimento no direito norte-americano, o sentido que o recorrente parece querer atribuir-lhe de um «efeito dominó» que arrasta todas as provas que, em quaisquer circunstâncias, apareçam em momento posterior à prova proibida e com ela possam, de alguma forma, ser relacionadas.

Pelo contrário, aquilo que está em causa – e os exemplos acima referidos demonstram-no amplamente – é uma doutrina que abre um amplo espaço à ponderação das situações concretas, ou seja, à interpretação, e que está longe de justificar, através da sua invocação, o caminho único de invalidar todas as provas posteriores à prova ilegal. Diversamente, trata-se com esta doutrina da procura de modelos de decisão assentes em critérios coerentes com a ponderação de interesses que justifica que, em determinadas circunstâncias, se projecte a invalidade de uma prova proibida, para além de nela própria, noutras provas e, em circunstâncias distintas, se recuse tal projecção."[20].

No mesmo o arresto e no contexto da referida teoria, igualmente interpretou o artigo 122.º/n. º 1 do Código de Processo Penal no sentido de uma norma que *"(…) abre um espaço interpretativo no qual há que procurar relações de dependência ou de produção de efeitos (o artigo 122º, nº 1 do CPP fala em actos dependentes ou afectados pelo acto inválido) que, com base em critérios racionais, exijam a projecção do mesmo valor negativo que afecta o acto anterior. Daí que os critérios atrás enunciados, fixados na jurisprudência norte-americana, acabem por constituir bons instrumentos de trabalho, que sugerem mesmo caminhos passíveis de ser seguidos entre nós, como aliás tem sucedido em outras ordens jurídicas."*[21]

Nesta conformidade, estamos com Costa Andrade quando sinaliza a necessidade de *"(…) ter em conta a singularidade do caso concreto."*[22]

[20] *Acórdão n.º 198/2004 do Tribunal Constitucional de 9 de março de 2004 (Diário da República, II Série, n.º 129, de 2 de junho de 2004, p. 8544 a 8551).*
[21] *Idem.*
[22] *Andrade, Manuel da Costa, in "Sobre as proibições de prova em Processo Penal", pág. 314 e segs. (op. citada no mesmo Acórdão).*

E como bem decidiu o Acórdão do TRC submetido, juntamente com o conforme Acórdão do STJ, à apreciação do Tribunal Constitucional, impõe-se esclarecer os princípios gerais da aquisição das provas, em prol da mitigação do efeito-à-distância, através da aplicação das seguintes regras básicas:

i. Afastamento da proibição do que resulta da mera constatação da realidade emergente.

ii. Não comunicabilidade, pelo efeito-à-distância, da invalidade aos dados conclusivos;

iii. Não contaminação, pelo efeito-à-distância, da prova "coisificada" persistente;

iv. Inaptidão do efeito-à-distância atingir a confissão livre e sem reservas do arguido.

Complementarmente, acompanhamos a afirmação do TC no sentido de poder *"afirmar-se com segurança que o sentido de uma norma prescrevendo que a invalidade do acto nulo se estende aos que deste dependerem ou que ele possa afectar (artigo 122º, nº 1 do CPP) é, desde logo, o de abrir caminho à ponderação que – como adiante se verá - subjaz à chamada doutrina dos «frutos proibidos». Isto, cotejado com a apontada amplitude das garantias de defesa contidas no artigo 32º da CRP, leva a que este Tribunal considere que, efectivamente, certas situações de «efeito-à-distância» não deixam de constituir uma das dimensões garantísticas do processo criminal, permitindo verificar se o nexo naturalístico que, caso a caso, se considere existir entre a prova inválida e a prova posterior é, também ele, um nexo de antijuridicidade que fundamente o «efeito-à-distância», ou se, pelo contrário, existe na prova subsequente um tal grau de autonomia relativamente à primeira que a destaque substancialmente daquela.*

Outro sentido não tem, aliás, a doutrina dos «frutos da árvore venenosa», desde a sua formulação no direito norte-americano, que não seja aquele que exige a ponderação do caso concreto determinando a existência, ou não, desse nexo de antijuridicidade entre a prova

proibida e a prova subsequente que exige para esta última o mesmo tratamento jurídico conferido àquela.".

5. O Acórdão do Tribunal Constitucional[23]

Na sequência do pedido da Senhora Provedora de Justiça de apreciação e declaração, com força obrigatória geral, da inconstitucionalidade das normas constantes dos artigos 4.º, 6.º, e 9.º da Lei n.º 32/2008, de 17 de julho, por violação do princípio da proporcionalidade na restrição dos direitos à reserva da intimidade da vida privada e familiar, nos termos do artigo 26.º, n.º 1 da CRP, ao sigilo das comunicações, consagrado no n.º 1 do artigo 34.º da CRP e à tutela jurisdicional efetiva prevista no n.º 1 do artigo 20.º do mesmo diploma, decidiu o Tribunal Constitucional:

"a) Declarar a inconstitucionalidade, com força obrigatória geral, da norma constante do artigo 4.º da Lei n.º 32/2008, de 17 de julho, conjugada com o artigo 6.º da mesma lei, por violação do disposto nos números 1 e 4 do artigo 35.º e do n.º 1 do artigo 26.º, em conjugação com o n.º 2 do artigo n.º 18.º, todos da Constituição;

b) Declarar a inconstitucionalidade, com força obrigatória geral, da norma do artigo 9.º da Lei n.º 32/2008, de 17 de julho, relativa à transmissão de dados armazenados às autoridades competentes para investigação, deteção e repressão de crimes graves, na parte em que não prevê uma notificação ao visado de que os dados conservados foram acedidos pelas autoridades de investigação criminal, a partir do momento em que tal comunicação não seja suscetível de comprometer as investigações nem a vida ou integridade física de terceiros, por violação do disposto no n.º 1 do artigo 35.º e do n.º 1 do artigo 20.º, em conjugação com o n.º 2 do artigo 18.º, todos da Constituição."

[23] *Acórdão n.º 268/2022, Processo n.º 828/2019, plenário do TC, relatado pelo Senhor Conselheiro Afonso Patrão, in* https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html

A lei n.º 32/2008, de 17 de julho, transpôs para o direito interno a Diretiva 2006/14/CE do Parlamento e do Conselho, de 15 de março (que alterou a Diretiva 2002/58/CE do Parlamento e do Conselho), relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações.

O Tribunal de Justiça da União Europeia (TJUE), através do Acórdão de 8 de Abril de 2014, decidindo no caso "*Digital Rights Ireland Ltd e outros v. Minister for Communications, Marine and Natural Resources*"[24], declarou a invalidade da referida Directiva, não tendo Portugal a diligência de realizar as pertinentes alterações do direito nacional, em concreto da Lei n.º 32/2008, a qual, integrando a transposição de uma Diretiva Europeia e consubstanciando um ato de aplicação do direito da União, nos termos e para os efeitos do artigo 51.º da Carta Fundamental dos Direitos da União Europeia (Carta), está a esta vinculada, tendo, como tal, que respeitar a decisão do TJUE, conduzindo necessariamente à desconformidade do diploma em apreço com a Carta.

A decisão do TJUE fundamentou-se na violação do princípio da proporcionalidade pela restrição que a Directiva operaria dos direitos ao respeito pela vida privada e familiar e à proteção de dados pessoais, consagrados nos artigos 7.º e 8.º da Carta; e embora decidindo que as normas inerentes à imposição do dever de conservação de dados de tráfego e de localização gerados no contexto de comunicações eletrónicas e do dever da sua transmissão às autoridades competentes para efeitos de investigação, deteção e repressão de crimes graves - eram, em si mesmas, medidas legítimas e adequadas ao fim visado - **acabou por concluir que as mesmas violavam o princípio da proporcionalidade, na sua dimensão de [do subprincípio da] necessidade.**

[24] *disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62012CJ0293&from=pt*

Embora tenhamos por assente que Portugal deveria ter procedido à alteração da Lei 32/2008 no devido tempo, tendo em conta a sua desconformidade com os princípios da Carta, estamos convictos de que esta decisão representa mais um revés na luta contra a criminalidade organizada, mormente aquela que opera no mundo virtual, o que para nós representa motivo de grande preocupação.

Acolhemos, assim, a opinião de Rui Cardoso[25] no sentido da incongruência entre a decisão e a fundamentação do Acórdão em questão, quando constata que *"Apesar de, na fundamentação, admitir que a conservação dos dados de base (números de telefone, endereços de correio eletrónico, nomes e moradas dos seus utilizadores, e ainda o endereço IP quanto às comunicações eletrónicas) não é desconforme à Constituição, declarou depois inconstitucional todo o artigo da lei que os incluía e, assim, nem tais dados poderão ser conservados."*.

Outrossim nos causa bastante desconforto o facto de, como mais adiante sinaliza, *"aquilo que passou agora a ser proibido para investigação de crimes graves continuará a ser permitido, quanto aos dados de tráfego (data, hora de início e duração das chamadas efetuadas, serviços e números chamados, volume de dados transmitidos), aos fornecedores de serviço, que, para efeitos de faturação, os poderão continuar a guardar. Não, não há erro no que disse: para o Tribunal Constitucional e a Provedora de Justiça (que nunca suscitou a inconstitucionalidade dessa lei), a retenção de dados de telecomunicações pode ser feita para acautelar a faturação dessas empresas, mas não para investigar e punir crimes graves."*.

Por último, mais uma vez reproduzindo a opinião de Rui Cardoso: *"Um número elevado de tipos de crimes que ficam em absoluto sem qualquer possibilidade de poder ser identificado o seu autor (nem*

[25] *Cardoso, Rui, "O tribunal Constitucional entre o real e o surreal", artigo de opinião, exclusivos Semanário Expresso, 2 de maio de 2022, disponível em* https://expresso.pt/opiniao/2022-05-02-O-Tribunal-Constitucional-entre-o-real-e-o-surreal-e0e48418

será possível dar o primeiro passo nessa investigação) ou, ainda que teoricamente assim não seja, na prática será isso que irá acontecer. Como esses crimes passarão a ficar impunes, irão então aumentar, ainda mais do que vêm aumentando. Crime que compensa é crime que aumenta.".

6. Conclusão

Tentámos dar nota, ainda que muito sumariamente, das dificuldades sentidas na investigação da cibercriminalidade, reiterando a ideia de que enquanto fenómeno de dimensão transnacional que diariamente atinge e afeta número indeterminado de vítimas utilizadores de boa-fé da Rede de Internet, com elevados danos, a nível pessoal, social e económico, imperioso se mostra que o seu combate opere do mesmo modo, isto é, de forma global e integrada, convocando o esforço de todos, designadamente em sede da cooperação internacional, visando: a uniformização legislativa; a capacitação dos investigadores e aplicadores da lei; a formação dos utilizadores comuns, protegendo-os com a necessária e devida eficácia; a uniformização das regras processuais de obtenção e valoração da prova digital.

Entretanto, aguardemos pela decisão da Assembleia da República relativamente à proposta de Lei n.º 11/XV/1.ª, do XXIII Governo Constitucional, aprovada no Conselho de Ministros de 26 de maio de 2022[26], certos de que o acesso aos dados de telecomunicações armazenados pelos fornecedores desses serviços - desde que devidamente regulamentado e autorizado pela competente autoridade judiciária, em função das concretas finalidades da investigação e repressão criminais, respeitando os direitos fundamentais dos seus titulares - se mostra imprescindível para a proteção das vítimas e dos seus mais elementares direitos, mormente o direito à vida, integridade física, liberdade, autodeterminação sexual, património e segurança, afigurando-se-

[26] https://www.parlamento.pt/ActividadeParlamentar/Paginas/IniciativasLegislativas.aspx

nos de justiça encontrar uma solução que proteja e garanta os direitos fundamentais dos agentes e vítimas da cibercriminalidade, casuisticamente, de harmonia com a hierarquia dos valores subjacentes.

ENTREVISTA
com a colega Teresa Sobral
Natural e com domicílio profissional em Viseu

O que a levou a ingressar na profissão?

Após conclusão do curso de Direito, inscrevi-me no estágio da Ordem dos Advogados com o objectivo de descobrir o que era a prática da advocacia e ganhar experiência nessa área para, depois, ingressar no CEJ. Porém, fruto do bom estágio que tive e sobretudo do carácter independente da profissão, rapidamente descobri na advocacia uma profissão motivante.

Quais os principais obstáculos e desafios que enfrenta actualmente no desenvolvimento da actividade enquanto advogada?

Os obstáculos e desafios que encontramos nesta profissão são muitos e a situação pandémica que vivemos veio agravá-los. O maior obstáculo neste momento é a dificuldade no acesso a serviços essenciais prestados por entidades públicas (autoridade tributária, conservatórias, serviço de estrangeiros e fronteiras, entre outros), emergindo cada vez mais entraves ao exercício do mandato forense. Pré-marcações para datas longínquas, falta de espírito de colaboração e sentido prático – e, por vezes até, desvalorização do papel do advogado – demonstrado pelos actores daqueles serviços. Como desafio, saliento a necessidade de constante actualização e formação do advogado

ante o *leviathan* legi-ferante em todas as áreas do Direito.

Hoje em dia fala-se muito na conjugação da família com a profissão. Essa articulação é possível na advocacia?

Sim, é possível, mas com muito esforço e sacrifício. É importante encontrar um ponto de equilíbrio e ter algum suporte familiar. Pessoalmente, a minha maior dificuldade é usufruir do *direito ao desligamento* - conseguir estar em casa em família, mentalmente livre, sem pensar no trabalho, nos prazos e nos problemas dos constituintes. É um exercício diário, as mais das vezes votado ao fracasso: até adormecer, o advogado carrega consigo nos ombros o peso dos problemas dos outros.

Quais as dificuldades que sente no exercício da profissão na sua comarca?

Conforme referi, as dificuldades prendem-se com o livre e atempado acesso a certos serviços públicos sem pré-agendamento - o que não se coaduna com a urgência que muitas vezes os assuntos impõem e que os nossos clientes reclamam. No demais, tenho a sorte de exercer numa comarca – Viseu – em que os colegas se conhecem e em que existe solidariedade, espírito de entreajuda e respeito. No dia a dia, esta cooperação facilita o exercício da profissão.

Após a pandemia, qual é a sua perspectiva do estado da justiça no futuro?

A pandemia veio acentuar a morosidade da justiça e penso que a recuperação não será tão rápida como desejado. O grau de rapidez irá depender do nível de colaboração e cooperação entre todos os que colaboram na administração da Justiça. Mas com a pandemia também levamos algo para o futuro: diligências à distância.

Que conselhos dá a quem está a dar os primeiros passos na advocacia?

O melhor conselho que dou a quem está a dar os primeiros passos na advocacia é o seguinte: avoquem os ingredientes necessários para se vencer em qualquer

profissão: dedicação, dedicação, dedicação, postura, respeito.

"O meu primeiro julgamento foi em 2006, um processo sumário de condução de veículo em estado de embriaguez, ainda na qualidade de estagiária. Nessa altura existiam escalas presenciais no Tribunal feitas maioritariamente pelos estagiários que, à época, tinham competência para praticar actos desacompanhados do patrono. Fazíamos escala em pares e por turnos (manhã/tarde) o que fomentava o convívio e entreajuda entre colegas."

LEGISLAÇÃO

Decreto-Lei n.º 10/2023

PRESIDÊNCIA DO CONSELHO DE MINISTROS

Estabelece as normas de execução do Orçamento do Estado para 2023

Portaria n.º 42/2023

ECONOMIA E MAR, AMBIENTE E AÇÃO CLIMÁTICA, INFRAESTRUTURAS E COESÃO TERRITORIAL

Regulamenta o regime de avaliação e gestão do ruído ambiente e transpõe para a ordem jurídica interna a Diretiva (UE) n.º 2020/367, da Comissão, de 4 de março de 2020, a Diretiva Delegada (UE) n.º 2021/1226, da Comissão, de 21 de dezembro de 2020, e dá execução ao Regulamento (UE) n.º 2019/1010, do Parlamento Europeu e do Conselho, de 5 de junho de 2019

Decreto-Lei n.º 11/2023

PRESIDÊNCIA DO CONSELHO DE MINISTROS

Procede à reforma e simplificação dos licenciamentos ambientais

Lei n.º 7/2023

ASSEMBLEIA DA REPÚBLICA

Autoriza o Governo a legislar em matéria de direito de autor e direitos conexos aplicáveis a determinadas transmissões em linha, transpondo a Diretiva (UE) 2019/789, do Parlamento Europeu e do Conselho, de 17 de abril de 2019

Decreto-Lei n.º 16/2023

PRESIDÊNCIA DO CONSELHO DE MINISTROS

Concretiza o processo de descentralização de competências para os municípios e para as entidades intermunicipais no domínio da educação

Decreto-Lei n.º 17/2023

PRESIDÊNCIA DO CONSELHO DE MINISTROS

Altera o regime da organização e funcionamento do XXIII Governo Constitucional

JURISPRUDÊNCIA

Acórdão do Supremo Tribunal de Justiça n.º 1/2023

SUPREMO TRIBUNAL DE JUSTIÇA

«O prazo de interposição dos recursos de decisões proferidas no procedimento previsto no art. 3.º da Lei n.º 75/98 de 19-11, é de 15 dias, nos termos do art. 32.º/3 do RGPTC, aprovado pela Lei n.º 141/2015, de 8-9»

Acórdão do Supremo Tribunal de Justiça n.º 2/2023

SUPREMO TRIBUNAL DE JUSTIÇA

«O perdão de penas de prisão previsto no artigo 2.º da Lei n.º 9/2020, de 10 de abril, verificados que sejam os demais requisitos legais, só pode ser aplicado a condenados que sejam reclusos à data da sua entrada em vigor»

Acórdão do Tribunal Constitucional n.º 5/2023

TRIBUNAL CONSTITUCIONAL

Pronuncia-se pela inconstitucionalidade, por referência ao Decreto n.º 23/XV da Assembleia da República, «que regula as condições em que a morte medicamente assistida não é punível e altera o Código Penal», da norma constante da alínea f) do artigo 2.º, conjugada com a norma constante do n.º 1 do artigo 3.º, das normas constantes dos artigos 5.º, 6.º e 7.º, e das normas constantes do artigo 28.º, «na parte em que alteram os artigos

134.º, n.º 3, 135.º, n.º 3, e 139.º, n.º 2, do Código Penal»; não se pronuncia pela inconstitucionalidade das demais normas cuja apreciação foi requerida

Acórdão do Supremo Tribunal de Justiça n.º 3/2023

SUPREMO TRIBUNAL DE JUSTIÇA

«À contagem da pena acessória de proibição de conduzir veículos com motor prevista no artigo 69.º do Código Penal aplicam-se, por analogia, nos termos do artigo 4.º do Código de Processo Penal, as regras de contagem da pena de prisão constantes do artigo 479.º do Código de Processo Penal.»

Acórdão do Supremo Tribunal de Justiça n.º 6/20.3GARMZ.E1.S1

«I- Tendo sido a decisão absolutória da 1ª instância, alterada para decisão condenatória pela Relação, justifica-se que o legislador, aceitando esta solução, admita mais um grau de recurso para o STJ (art. 400.º, n.º 1, al. e), do CPP), com vista à reapreciação do caso concreto.

II- Os segmentos da argumentação do STJ, com os quais a recorrente discorda (e que a mesma lê, de forma isolada e conforme lhe é conveniente), não equivalem, como alega, ao conhecimento de questões de que o Tribunal não podia conhecer (art. 379.º, n.º 1, al. c), do CPP).

III- A recorrente está a inverter as situações e a pretender impor a sua perspetiva e apreciação dos factos, o que não pode ser, pois está a confundir a sua análise pessoal e subjetiva com nulidade do acórdão. Na verdade, a discordância da recorrente quanto à decisão do STJ não equivale à existência de qualquer nulidade, nem tem a virtualidade de tornar nulo o mesmo acórdão do STJ.»

Acórdão do Supremo Tribunal de Justiça n.º 214/20.7PCCSC.L1.S1

«I- Por se verificar o condicionalismo previsto nos arts. 400.º, n.º 1, al. f) e 432.º, n.º 1, al. b), do CPP, havendo "dupla conforme", o acórdão da Relação é definitivo quanto às questões processuais e de direito que apreciou e que o arguido/recorrente volta agora a colocar (sob diversas formas, algumas até apresentadas indevidamente como

questões novas) no recurso para o STJ, ressalvada a questão da pena única, por ser superior a 8 anos, que pode ser sindicada.

II- Destinando-se os recursos a suscitar a oportuna apreciação da decisão de que se recorre (neste caso do acórdão do Tribunal da Relação) nele não devem ser apresentadas questões novas que não foram colocadas ao Tribunal recorrido (ressalvado aquelas que devam ser conhecidas oficiosamente), uma vez que o STJ não pode apreciar tais novas questões sem haver decisão que sobre elas recaia.

III- Na determinação da pena única a aplicar, há que fazer uma nova reflexão sobre os factos em conjunto com a personalidade do arguido, pois só dessa forma se abandonará um caminho puramente aritmético da medida da pena para se procurar antes adequá-la à personalidade unitária que nos factos se revelou.»

FORMAÇÃO


CICLO DE FORMAÇÃO
VIAGENS
PELAS MAIS RECENTES ALTERAÇÕES AO CÓDIGO DO TRABALHO E AGENDA DO TRABALHO DIGNO
1ª PARAGEM
TELETRABALHO
Doutora Joana Nunes Vicente
Professora Universitária
2 MARÇO 2023
15:00 - 16:30
AUDITÓRIO DO CONSELHO REGIONAL DE COIMBRA
DA ORDEM DOS ADVOGADOS
INSCRIÇÃO
ORGANIZAÇÃO
ORDEM DOS ADVOGADOS
CONSELHO REGIONAL DE COIMBRA
JUTRA
ASSOCIAÇÃO LUSO-BRASILEIRA DE JURISTAS DO TRABALHO