
CYBERLAW
by CIJIC

CYBERLAW

by CIJIC

EDIÇÃO N.º VII – MAIO DE 2019

REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

NOTAS DO EDITOR:

Nesta nova edição da revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa, antes de mais, aproveito para anunciar uma nova edição do Curso de Direito do Ciberespaço, em formato novel, a ter lugar em Novembro de 2019. À semelhança do curso anterior, na oportunidade de publicação de alguns artigos, a Revista assumir-se-á como esse veículo de partilha de conhecimento.

No que concerne propriamente às notas desta edição, permitam-me partilhar algumas novidades e preocupações.

No passado dia 23 de maio do corrente, o Conselho de Ministros aprovou a Estratégia Nacional de Segurança do Ciberespaço (ENSC) 2019-2023, que ainda carece de publicação em jornal oficial. Não obstante é já do domínio público que o propósito desta nova ENSC visará *garantir a proteção e a defesa das infraestruturas críticas e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas, procedendo desta forma à revisão da ENSC de 2015*[1], tendo em atenção a evolução digital ocorrida desde então.

1 https://www.portugal.gov.pt/pt/gc21/governo/comunicado-de-conselho-de-ministros?i=278
A propósito, neste conspecto, para quem não tenha estado presente, na Conferência – Cibersegurança, na Universidade de Évora, a 14 de novembro de 2018, será interessante dar uma vista de olhos na apresentação "A Estratégia Nacional de Segurança do Ciberespaço 2.0 – Governação e execução", feita e disponibilizada por parte do CALM Gameiro Marques, da Autoridade Nacional de Segurança, cujo conteúdo pode ser encontrado @ https://www.uevora.pt/media_informacoes/agenda/(item)/25903.

Em efeméride de aniversário do Regulamento Geral de protecção de dados, e estando este em vigor desde *o vigésimo dia seguinte ao da sua publicação no Jornal Oficial da União Europeia*, naturalmente a «Cyberlaw by CIJIC» não poderia passar ao lado do tema, recorrente dos últimos anos.

De facto, nestes 3 anos volvidos, é inconcebível que Portugal ainda não tenha uma lei de execução do mesmo. De igual forma, é inconcebível que as organizações, públicas ou privadas, só conheçam o "consentimento" como fundamento de licitude para o tratamento de dados pessoais, considerando-o um verdadeiro *canivete-suíço*. Ainda havemos de pugnar por um "*direito ao esquecimento*" sobre o consentimento, pois que a livre revogabilidade do mesmo por parte da pessoa titular dos dados pessoais parece sucumbir ante tanto abuso na sua utilização por parte das mais variadas organizações.

Se a estupefação quanto ao uso abusivo da figura do consentimento não cercear a nossa incredulidade, é igualmente inconcebível que o Estado, hoje, 3 anos após a entrada em vigor do RGPD, tenha dado conta de que, por exemplo, pelo menos, 1977 freguesias estarão obrigadas a nomear um encarregado de protecção de dados. Subam ou desçam na hierarquia do Estado e imaginem a confusão em que se vive. Três anos volvidos e o Mercado Único Digital Europeu à espreita…

Não pensem, contudo que a confusão é exclusivo do sector público. Quando o foco deriva para dados pessoais sensíveis, nomeadamente, dados de saúde, notícias como por exemplo, «*Proteção de Dados condena clínicas que recusam tratar doentes por falta de assinaturas*[2]», revelam parte do preocupante e actual estado de coisas.

Com efeito, se a protecção de dados pessoais era até há pouco tempo tema desconhecido do grande público, num ápice passou a ser o *olho do furacão*, gerando leque preenchido de atropelos e violações de dados dos seus titulares. E a autoridade nacional de controlo continua amarrada a constrangimentos de índole múltipla, desde orçamentais à falta de recursos, humanos e tecnológicos. Imaginem o que escapa ao *mainstream* mediático.

Enquanto isso, a evolução do digital continua em passo acelerado. O nível de ameaça ao estado de direito democrático acompanha esta desenfreada marcha.

2 Disponível em https://www.dn.pt/lusa/interior/protecao-de-dados-condena-clinicas-que-recusam-tratar-doentes-por-falta-de-assinaturas-10901005.html,

Infelizmente, o tempo do direito e da justiça teimam em não se adaptar. Está assíncrono. O que, se por um lado até poderá induzir-nos a alguma prudência, por outro pode indiciar um factor de preocupação acrescido. Até pelo nível de risco em que coloca a sociedade, no seu todo.

Pensemos na utilização do uso de UAV's; na condução autónoma de veículos; na constante violação das propriedades essenciais da informação gerando supremacias informacionais ilegais a certos Estados; na massificação das redes sociais; na disseminação em *live streaming* de ataques a pessoas; na dispersão de conteúdo mentiroso e propagandístico *online* para desvirtuar o resultado de eleições livres e democráticas; na disseminação de ódio e violência *online*; nas novas ameaças a toda a actividade policial e de segurança do Estado; no controlo e rastreio individual *online* e no registo de crédito social em função disto; entre outras. A profusão destas notícias é de conhecimento geral. A *digitalização* humana está em curso. O ciberespaço, aparentemente, evolui para uma antiutopia.

Neste ensamble, vertiginoso e fulminante, é pois inconcebível que dois anos volvidos após um pedido de fiscalização sucessiva intentado junto do Tribunal constitucional português, por parte de um conjunto de partidos políticos, este Tribunal ainda não se tenha pronunciado quanto à constitucionalidade do acesso aos metadados, dados de tráfego e duração de comunicações por parte dos serviços secretos portugueses. É inconcebível e preocupante pois que, por um lado o serviço de informações da república esteja parado ou a trabalhar à margem da lei ante esta omissão do Tribunal; por outro lado, é inconcebível que este Tribunal, por excelência, de garantia dos direitos e liberdades fundamentais das pessoas, esteja dois anos para aferir da constitucionalidade de uma dada lei.

O que tanto demora a tomada de decisão? Falta de preparação temática dos juízes do Constitucional? Má técnica legislativa? Teimosia política? Falta de ameaças concretas, conhecidas do público, à segurança do Estado? Neste particular dos metadados, sublinho, o delírio é a nota dominante. Até porque, se *o Sistema de Acesso ao Pedido de Dados aos Prestadores dos Serviços de Comunicações Electrónicas (Sapdoc), foi declarado operacional pelo CFSIRP desde Março e está a funcionar,* no outro plano da acção, consta que poderá estar na iminência *um novo chumbo dos juízes,*

uma vez que a questão de fundo - violação do artigo 34º da CRP- manter-se-á [3]. Ora, parece-nos que este delírio, portanto, promete e vai continuar. Novo procedimento, novas discussões, nova lei, mais discussões, novo pedido de fiscalização, novo entorpecimento, novo regresso ao ponto de partida, que recordo, é a nota dominante desde que o poder político criou o *novo regime do Sistema de Informação da República Portuguesa*, em 2015.

Óbice daqui, ameaça dali, risco dacolá, não haverá uma luz de esperança que contrarie o delinear desta *antiutopia*?

A bem de todos nós, mesmo que tenha passado despercebido o *Christchurch Call*[4], julgamos decisivo o apelo à acção. Até porque o momento, o tempo e o espaço a tal nos obrigam. Aqui chegados, impõe-se-nos o sublinhar de parte das notas dos proponentes iniciais. Por um lado, o *envisage* do Presidente francês, o sr. Macron: «"*We need to build this new cyberspace, a free, open and secure Internet, which allows everyone to share, learn, innovate, but which also allows us to uphold our values, protect our citizen and empower them*"»; por outro, o apelo à adesão pluriparticipada, mundial, a cargo da Primeiro-Ministra Neozelandesa, a sra. Ardern: «"*From here, I will work alongside others signed up to the Christchurch Call to bring more partners on board, and develop a range of practical initiatives to ensure the pledge we have made today is delivered*"». Por um *mundo*, terreno e digital, melhor, de todos e para todos.

Por fim, num plano nacional, com especial saudação para a ousadia da proposta, arbitramos da pertinência do Projeto de Lei 1217/XIII[5], apresentado pelo partido Socialista, já apelidado de Carta de Direitos Fundamentais na Era Digital.

A Carta deverá corresponder a *lei de protecção de direitos, liberdades e garantias centrada nas pessoas, consagradora de valores democráticos essenciais contra ameaças que não devem ser ignoradas* procurando ir além de mera *lei compilatória das normas que na ordem jurídica portuguesa consagram (alguns) direitos*, que enuncie *um elenco diversificado e abrangente, que inove, clarifique e valha também*

3 https://www.dn.pt/poder/interior/-necessidade-inquestionavel-fiscais-das-secretas-validam-acesso-a-dados-das-comunicacoes--10935824.html

4 https://www.beehive.govt.nz/release/christchurch-call-eliminate-terrorist-and-violent-extremist-online-content-adopted

5 Disponível em: https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=43768

como programa de ação vinculativo dos órgãos de poder, pode ler-se no enunciado programático do Projeto de lei. Deixo aqui um apelo a uma participação contributiva entusiasta por forma a melhorar este esboço inicial de consagração de uma Carta de Direitos Fundamentais na Era Digital.

Resta-me, a final, agradecer a todos quantos contribuíram para mais uma edição da Revista, pelo esforço e pelo trabalho, endereçando, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, um reconhecido: Muito Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

Boas leituras.

Lisboa, FDUL, 24 de Maio de 2019

Nuno Teixeira Castro

CYBERLAW

by CIJIC

DOUTRINA

GESTÃO DE RISCO APLICADA À SEGURANÇA DA INFORMAÇÃO

LUÍSA ALEXANDRA INÁCIO VARANDAS DOS SANTOS [1]

e

MÁRIO RUI MONTEIRO MARQUES [2]

1 Luísa Alexandra Inácio Varandas dos Santos. Correio eletrónico: luisa.santos@tecnico.ulisboa.ptm
2 Capitão-tenente Mário Rui Monteiro Marques. Correio eletrónico: mario.monteiro.marques@marinha.pt

RESUMO

As sociedades modernas veêm-se, nos dias de hoje, alimentadas por uma quantidade enorme de informação, acrescendo o facto de que numa era digital, essa quantidade de informação é extraordinariamente dinâmica na forma como se produz, como se transforma e como é divulgada.

A informação assume nos dias de hoje, um papel de enorme relevância. O que anteriormente era visto como um ativo valioso apenas pelas forças Militares, passa assim a ter a mesma atenção em contexto Civil na procura da privacidade da informação pessoal dos Cidadãos.

Com o reconhecimento da informação, como um ativo de extremo valor, seja qual for o contexto da sua utilização, passa a existir uma necessidade de a proteger contra ameaças, surgindo assim o conceito de Segurança da Informação com o objetivo de assegurar os princípios e características fundamentais: a confidencialidade, a integridade, a disponibilidade, a autenticidade e não repúdio, e a legitimidade da Informação.

A melhor forma de proteger a informação é conhecer o meio envolvente desta, os fatores internos e externos que a podem influenciar positivamente ou negativamente, que riscos e oportunidades de melhoria existem no seu ciclo de vida e de que forma efetuamos a gestão desses riscos e dessas oportunidades de melhoria, de modo a obter a Segurança da Informação, dentro do contexto em que a mesma se insere.

O presente artigo aborda a "Gestão de Risco aplicada à Segurança da Informação", com uma metodologia baseada na implementação de um processo de gestão de risco segundo a norma *standard* ISO/IEC 31000:2009 - *Risk Management - Principles and guidelines*, integrada com as normas standard em matéria de Gestão Segurança da Informação e Gestão de Serviços de Tecnologias de Informação.

Palavras-Chave: Segurança da informação, Risco, Confidencialidade, Integridade, Disponibilidade, Autenticidade, Legitimidade.

1. INTRODUÇÃO

É em contexto Organizacional que o presente trabalho se pretende focar, onde a simples necessidade de gestão de dados de processos de negócio, passou a uma imprescindível necessidade de transformar a informação dos processos de negócio em conhecimento valioso para a tomada de decisões estratégicas das Organizações.

Esta crescente necessidade Organizacional, de gerir a informação de processos de negócio de modo a produzir conhecimento estratégico, recorre às Tecnologias e Sistemas de Informação, assumindo estas o seu lugar de relevância nas Organizações. Por este motivo, as Tecnologias e Sistemas de Informação têm sido particularmente beneficiadas em investimentos das Organizações respetivas, procurando uma evolução Tecnológica continua e apta a responder com eficiência aos desafios de negócio em que determinada Organização se insere. Tendo sido este o fator de sucesso em mercados de enorme concorrência. Conhecer a Organização, conhecer os produtos e serviços que a mesma produz, conhecer os seus Clientes, Fornecedores e partes interessadas, conhecer a informação Organizacional e protege-la de ameaças, é um fator de sucesso e até mesmo de sobrevivência em mercados de muita concorrência, ou mercados extremamente regulados e legislados particularmente em matéria de informação sensível e secreta, como é o caso por exemplo do setor da Saúde e do setor Judicial!

Temos assistido, não só ao crescimento dos Sistemas de Informação Organizacionais, mas também, a um aumento de interações entre vários Sistemas de Informação, que facilmente comunicam entre si, permitindo obter, tratar, armazenar e divulgar informação de uma forma integrada e potencialmente útil à estratégia das Organizações, onde estão inseridos.

A legislação que tem surgido nas últimas décadas, quer a nível nacional quer a nível europeu, tem-se esforçado por acompanhar a preocupação da Segurança da Informação, com o foco na Segurança das Redes e da Informação, Interoperabilidade Digital e Privacidade de Dados Pessoais, respetivamente: RNID - Regulamento Nacional de Interoperabilidade Digital, Diretiva UE 2016/1148 e Regulamento (UE) 2016/679 [6], [7] e [8].

Ainda assim, pese embora tenha crescido a preocupação da União Europeia e dos seus Estados Membros em legislar sobre Segurança da Informação em matéria de redes, sistemas de informação e dados pessoais, apelando a uma gestão do risco e a potenciais ameaças, o facto é, que a lei tem sido omissa na metodologia que as Organizações devem adotar para implementação de processos de gestão de risco, deixando a cargo das mesmas a adoção de processos de cerificação voluntários que possam contribuir para o cumprimento da legislação em vigor na prevenção contra ameaças. Neste sentido, a maior parte das Organizações tem recorrido às normas *standard* ISO "Internacional Organization for Standardization", Organização internacional não-governamental independente, com sede em Genebra, que desenvolve padrões de normalização para o âmbito Organizacional, tais como: Gestão de Segurança da Informação, Gestão de Serviços de Tecnologias de Informação, Gestão de Risco, entre outros. O presente trabalho tendo como foco a "Gestão de Risco aplicado á Segurança da Informação", pretende assim demonstrar a aplicabilidade prática da adoção de um processo de Gestão de Risco segundo a norma *standard* ISO/IEC 31000:2009 – "*Risk Management - Principles and guidelines*" (**Figura 1**), acompanhada das normas standard em matéria de Gestão de Segurança da informação e Gestão de Serviços de Tecnologias de Informação.

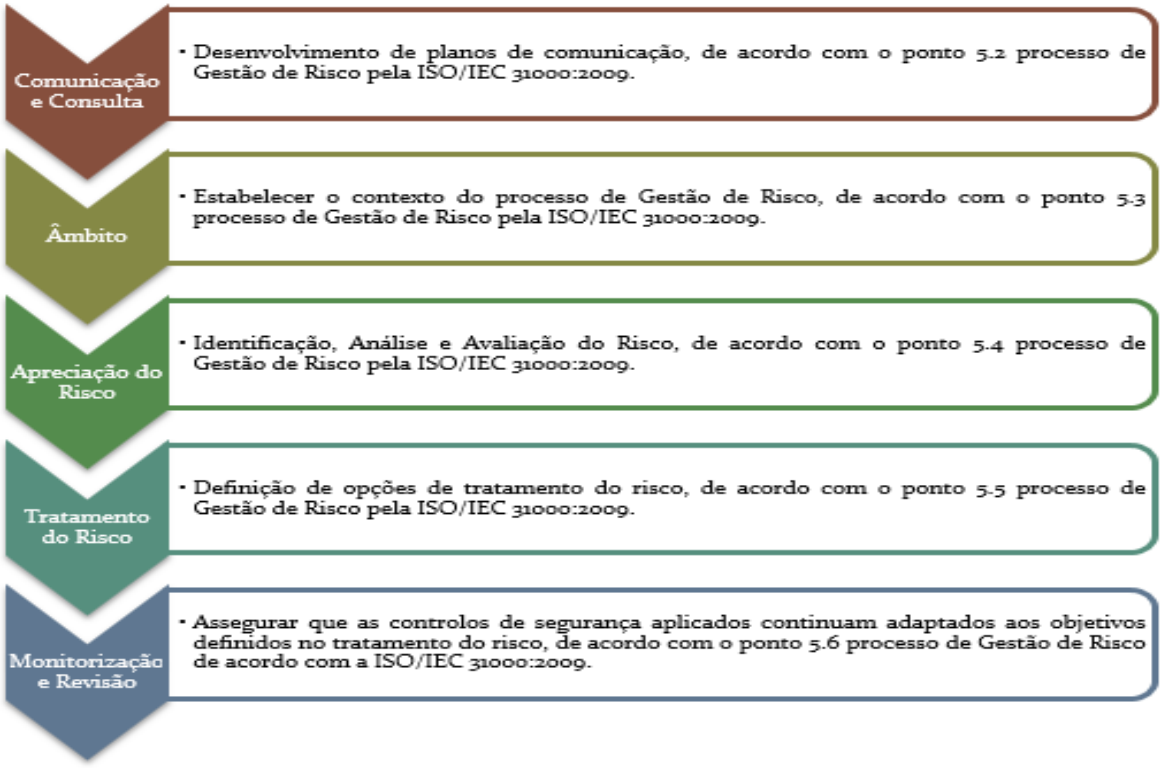

Figura 1 – Fases de processo de Gestão de Risco pela ISO/IEC 31000:2009 - Risk Management - Principles and guidelines [5]

2. PROCESSO DE GESTÃO DE RISCO APLICADO À SEGURANÇA DA INFORMAÇÃO

As Organizações têm várias componentes que não apenas a tecnológica e o negócio, que carecem de análise na implementação de um Processo de Gestão de Risco aplicado à Segurança da informação adiante designado por **PGRSI**, entre elas, temos a considerar, a componente humana, ou seja, os Colaboradores de determinada Organização, os seus Fornecedores e Partes Interessadas.

Todas as componentes envolvidas na implementação de um Processo de Gestão de Risco aplicado á Segurança da informação em determinada Organização, requerem especial preocupação relativamente a vulnerabilidades que as mesmas possam ter, face a potenciais ameaças, ou seja, de que modo essas componentes Organizacionais estão realmente protegidas no âmbito da Segurança da Informação, reduzindo e minimizando o impacto de uma ameaça a determinada Organização.

Existe assim a necessidade da Organização analisar todas as condicionantes internas e externas que possam representar riscos significativos para a Segurança da Informação da Organização, mais especificamente que coloquem em causa os princípios da Segurança da Informação de determinada Organização [1]:

- **Confidencialidade** - assegurar que apenas quem está autorizado é que pode aceder à informação. Esta característica depende de um procedimento interno de classificação de informação, definido pela Organização, identificando que informação é confidencial, secreta, publica, interna, ou, outro tipo de informação, definindo por cada tipo de classificação de informação, quem pode aceder e, de que modo pode aceder ou divulgar informação [1], [2], [3] e [4].

- **Integridade** - assegurar que a informação e os seus métodos são completos. Isto significa que independentemente dos canais e formas onde a informação possa ser tratada e divulgada, a mesma, nunca perde o seu valor conceptual nem é adulterada. Esta situação depende de um procedimento interno de definição e controlo de versões de informação que possa ser produzida sobre a mesma origem, definido pela Organização, identificando todas as versões que foram produzidas sobre a mesma informação, datas e autores de versões

produzidas, bem como, identificação de que informação adicional acrescida, ou, que informação foi retirada da inicial [1], [2], [3] e [4].

- **Disponibilidade** - assegurar que os utilizadores autorizados têm acesso à informação e aos seus ativos associados sempre que necessitem. Obviamente que este tipo de característica tem de levar em conta o tipo de informação e a quem deve ser disponibilizada, dependendo da sua classificação [1], [2], [3] e [4].

- **Autenticidade e não repúdio/desconhecimento** - assegurar a fiabilidade das transações e o intercâmbio de informação entre organizações e colaboradores. Esta característica pode ser garantida através de utilização de mecanismos de backup de logs (registos) de dados de acesso e alteração da informação [1], [2], [3] e [4].

- **Legitimidade** - garantir que o tratamento da informação cumpre com as leis e regulamento do sector (área de negócio) a que se aplica [1], [2], [3] e [4].

É também importante destacar outros princípios que a Segurança da Informação tem implícitos, pese embora não sejam aqueles que definem as suas características fundamentais, ainda assim também estes carecem de preocupação face a possíveis riscos a que possam estar sujeitos, nomeadamente:

- A proteção dos dados de carácter pessoal e a privacidade das pessoas;

- A proteção dos direitos de propriedade intelectual e industrial;

- O estabelecimento de um sistema de classificação da informação com o objetivo de proteger melhor os ativos críticos da organização;

- A salvaguarda dos registos da organização.

É através da implementação de um **PGRSI**, que a Organização consegue avaliar o impacto dos riscos que podem pôr em causa os princípios e características fundamentais da Segurança da Informação, antecipando ações corretivas aos riscos detetados.

3. PGRSI - COMUNICAÇÃO E CONSULTA

Esta fase engloba todas as outras do **PGRSI** (**Figura 1**), a Organização deve comunicar com todas as partes interessadas, Colaboradores, Clientes, Fornecedores, etc…, desenvolvendo planos de comunicação e consulta, abordando as questões relacionadas com o risco, causas e consequências do mesmo e formas de tratar o risco, na Organização.

Na prática esta fase é alimentada pelas fases seguintes que serão demonstradas, sendo que nesta fase, abrangendo todo o **PGRSI**, podem ser consultadas as partes interessadas da Organização de modo a definir critérios de risco e avaliação de risco, para os riscos identificados e comunicados. Assim, devemos olhar para esta fase, como um comportamento da Organização reagindo a eventos decorrentes da implementação do **PGRSI** que devem ser prontamente comunicados e consultados pelas partes interessadas de modo a contribuir para a melhoria contínua do **PGRSI**.

4. PGRSI - ÂMBITO

O âmbito de aplicação do **PGRSI**, resulta da identificação correta de todas as componentes Organizacionais que produzem, acedem, tratam e disponibilizam informação, no sentido de identificar onde, como e com que probabilidade se podem concretizar riscos numa Organização. Deste modo, pode ser definido o âmbito do **PGRSI** da seguinte forma:

- **RECURSOS INTERNOS** – Recursos humanos internos á Organização tais como: Auditores Internos, Juristas internos, Utilizadores Internos, Colaboradores Internos em geral, etc.
- **RECURSOS EXTERNOS** – Recursos humanos externos á Organização Auditores Externos, Consultores, Prestadores de Serviço, Utilizadores Externos, Colaboradores Externos em geral, etc
- **SERVIÇOS DE TECNOLOGIAS DE INFORMAÇÃO** – Conjunto de Sistemas de Informação que dão suporte ao negócio numa Organização, por exemplo soluções de *Business Intelligence* (processos de tratamento de dados de larga escala), soluções de Sistemas de Informação Integrados de Processos de Negócio da Organização, etc.
- **PARTES INTERESSADAS À ORGANIZAÇÃO** – Fornecedores internos e externos, Clientes, Negócio.
- **DOCUMENTOS CONTROLADOS E ACORDOS DOCUMENTADOS** – Acordos de Níveis de Qualidade e Disponibilidade de Serviço, Políticas e Regulamentos Organizacionais, Legislação, Códigos de Conduta, e Planos (Contingência, Continuidade de Negócio, Plano de Tratamento do Risco, entre outros).
- **SOFTWARE** – Sistemas Operativos, Aplicações e Bases de Dados.
- **DISPOSITIVOS** – Computadores, Monitores, Discos, Smartphones, Tablets, etc.
- **COMUNICAÇÕES** – Circuitos Internet, Circuitos de Voz, etc.
- **SERVIDORES** – Centralização de fornecimento de serviços e protocolos de rede.
- **ARMAZENAMENTO DE DADOS** – Arquiteturas de Armazenamento de dados.
- **INFRAESTRUTURA DE REDE** – Redes de dados Locais e Virtuais.

Estamos assim perante o âmbito de aplicação do **PGRSI**, que comporta toda a informação, nas suas formas, suportes e canais de circulação, assumidos no seu ciclo de vida, dentro de uma Organização e de todas as suas partes interessadas. Reconhecendo que o âmbito de aplicação do **PGRSI** nomeadamente: a Organização em si, Fornecedores, Clientes, Mercado, Legislação e Regulação, evoluem ao longo do tempo, o **PGRSI**, deve permitir avaliar aquilo que hoje constitui uma ameaça, mas que amanhã pode não constituir, passando a representar uma oportunidade.

5. PGRSI - APRECIAÇÃO DO RISCO

A fase de Apreciação do Risco resulta de um processo global de identificação, análise e avaliação do mesmo, passamos assim a demonstrar de uma forma integrada estas fases, tendo em conta o âmbito do **PGRSI**. Importa antes de tudo distinguir o que são ameaças e o que são vulnerabilidades:

- **AMEAÇA**, representa um possível ataque interno ou externo a determinado alvo, com intenção de provocar danos totais ou parciais nesse alvo.
- **VULNERABILIDADE**, representa alguma fragilidade de determinado alvo, que possa ser explorada por uma ameaça de modo a provocar maior impacto num determinado ataque, ou seja, conteúdos não protegidos, ou, com reduzida proteção, ou, com proteção desatualizada e que não acompanham as ameaças atuais.

5.1. Identificação do risco

5.1.1. Inventário de ativos

Procede-se á identificação dos ativos a proteger e dependências entre si dentro do âmbito do **PGRSI**, através da realização de um inventário de Ativos, em que um Ativo é um item que suporta informação, dentro do âmbito do **PGRSI**, com valor para a Organização e dos quais dependem a realização de atividades de Serviços de Tecnologias de Informação como, por exemplo: Servidores, Computadores, *Smartphones*, Impressoras, Discos e Unidades de Armazenamento, Circuitos de Comunicação, etc.

O inventário de Ativos deve permitir valorizá-los em função do seu impacto para a Organização, tendo em conta, incidentes relacionados com os princípios da Segurança da informação, de confidencialidade, de integridade, de disponibilidade, de autenticidade e não repúdio, e de legitimidade da informação. Desta forma deve-se inventariar os Ativos da seguinte forma:

- ✓ Designação do Ativo;
- ✓ Dependentes diretos do Ativo;
- ✓ Localização do Ativo;
- ✓ O dono ou responsável pela sua utilização do Ativo;
- ✓ Os serviços ou processos nos quais o Ativo está envolvido.

5.1.2. Matriz de impacto

Define-se uma Matriz de Níveis de Impacto e de Linhas Orientadoras para a análise de impacto, de modo a quantificá-lo face á concretização de uma ameaça, através da definição de níveis de impacto por determinados valores definidos para linhas orientadoras.

Estas linhas orientadoras podem levar em conta os contributos das partes interessadas, conforme previsto na fase de Comunicação e Consulta do **PGRSI**. Propõe-se a título de exemplo as seguintes dimensões para a elaboração da Matriz:

a. **Níveis de Impacto -** Estabelecemos os níveis de impacto de 1 a 5, para os diferentes valores de cada linha orientadora (b.) de análise de impacto de concretização da ameaça, com o seguinte critério:

- ✓ **Nível 1** Sem Impacto nos serviços prestados;
- ✓ **Nível 2** Impacto reduzido nos serviços prestados;
- ✓ **Nível 3** Impacto significativo nos serviços prestados;
- ✓ **Nível 4** Impacto grave nos serviços prestados;
- ✓ **Nível 5** Ameaça à sobrevivência do Negócio.

b. **Linhas Orientadoras -** Estabelecemos as linhas orientadoras de análise de impacto de concretização da ameaça, do seguinte modo:

- ✓ **Perdas Financeiras** - Perda direta de clientes ou quota de mercado, custos de oportunidade, perda de vantagens competitivas e/ou custos de recuperação.
- ✓ **Esforço de Operações** - Incremento dos esforços de produção, esforços operacionais, esforços associados à contratação de RH adicionais e/ou de recuperação de imagem.
- ✓ **Reputação e Imagem** - Perda de confiança dos clientes, público em geral, partes interessadas, entidades reguladoras, entidades de supervisão e/ou colaboradores.
- ✓ **Legais/Regulamentares** - Sujeição a potenciais investigações, multas ou penalidades por parte de entidades reguladoras/governamentais, sanções contratuais e/ ou processos em tribunal.
- ✓ **Envolvimento da Gestão de Topo da Organização** - Envolve diretamente a Gestão de Topo influenciando o processo de tomada de decisão,

seja a nível estratégico, de investimentos e/ou conceção e desenvolvimento de novos serviços.

c. **Matriz de Limites de Impacto por Valores de Linhas Orientadoras para a avaliação de impacto -** Com base nos níveis de impacto definidos em (a.) relacionados com as linhas orientadoras de análise de impacto definidas em (b.), estabelece-se a seguinte Matriz de limites orientadores de avaliação de impacto (**Figura 2**):

a. Níveis de Impacto	b. Linhas Orientadoras				
IMPACTO	**PERDAS FINANCEIRAS**	**ESFORÇO DE OPERAÇÕES**	**REPUTAÇÃO E IMAGEM**	**LEGAIS E REGULAMENTARES**	**EMVOLVIMENTO DA GESTÃO DE TOPO DA ORGANIZAÇÃO**
1 Sem **Impacto nos serviços prestados**	Perdas até X.000,00€	Sem impacto significativo no esforço operacional	Afeta negativamente as relações com outras partes da Organização. Sem impacto nos meios de comunicação.	Sem impacto significativo no cumprimento de contratos, acordos, regulamentações e leis em vigor.	Resolução de incidentes ao nível das equipas técnicas, o serviço afetado não é estratégico para a Organização.
2 **Impacto reduzido nos serviços prestados**	Perdas até XX.000,00€	Impacto reduzido no esforço operacional	Afeta negativamente as relações com o publico e com outras organizações no meio. Atenção pontual nos meios de comunicação, mas sem por em causa a imagem da Organização.	Impacto reduzido no cumprimento de contratos, acordos, regulamentações e leis em vigor.	Resolução de incidentes ao nível das equipas técnicas, com necessidade de esclarecimentos dos diretores de primeira linha, o serviço afetado não é estratégico para a Organização.
3 **Impacto significativo nos serviços prestados**	Perdas até XXX.000,00€	Impacto significativo no esforço operacional (sobrecarga de recursos).	Afeta negativamente as relações com o publico e com outras Organizações. Atenção adversa nos meios de comunicação, mas sem por em causa a imagem da Organização.	Impacto significativo no cumprimento de contratos, acordos, regulamentações e leis em vigor.	Envolvimento direto dos diretores de primeira linha na resolução de incidentes, a Gestão de Topo da Organização é notificada, o serviço afetado não é estratégico para a Organização.
4 **Impacto grave nos serviços prestados**	Perdas até X.000.000,00€	Grande impacto no esforço operacional, alocação de horas extra aos recursos.	Publicidade Negativa passa nos meios de comunicação, suscetível de colocar em causa a imagem da Organização.	Grande impacto no cumprimento de contratos, acordos, regulamentações e leis em vigor.	Requer decisão e gestão pontuais por parte da Gestão de Topo da Organização, o serviço afetado é

					estratégico para a Organização.
5 **Ameaça à sobrevivência do Negócio / Prestação de Serviço**	Perdas superiores a X.000.000,00€ ou perdas suficientes para impedir a continuidade do negócio	Impacto Catastrófico no esforço operacional (para além de alocação de horas extra aos recursos, existe a necessidade de suspender atividades diárias).	Publicidade Negativa passa nos meios de comunicação com grande repercussão, colocando em causa a imagem da Organização.	Impacto catastrófico no cumprimento de contratos, acordos, regulamentações e leis em vigor.	Requer envolvimento ativo da Gestão de Topo da Organização, o serviço afetado é estratégico para a Organização.

Figura 2 – Matriz de Limites de Impacto por Valores de Linhas Orientadoras para a avaliação de impacto (a Matriz é puramente exemplificativa podendo ser gerada outra qualquer Matriz ao critério do Responsável pela implementação de um PGRSI em determinada Organização e Contexto Organizacional)

5.1.3. Avaliação do impacto sobre os ativos

É necessário avaliar para cada ativo, de acordo com a Matriz de limites orientadores de avaliação de impacto (**Figura 2**), na fase em que não existem medidas aplicadas, ou seja, sem controlos de segurança da informação aplicados, o impacto que terão caso se verifiquem incidentes de segurança da informação relacionados com a confidencialidade, a integridade, a disponibilidade, a autenticidade e não repúdio, e a legitimidade da informação. O valor máximo da matriz associada a cada ativo dar-nos-á o valor do mesmo; no entanto, se outros ativos dependem dele, o valor do ativo que estamos a analisar passará a ser o valor máximo dos ativos dependentes deste.

A título de exemplo, podemos olhar para os seguintes ativos um Servidor de Comunicações de Voz de uma Organização e um Servidor Web de suporte a um Site Institucional dessa mesma Organização, se avaliarmos o seu impacto de acordo com a Matriz de impacto por ativo (**Figura 3**), tendo em conta a existência de incidentes se segurança da

informação, que coloquem em causa a confidencialidade, a integridade, a disponibilidade, a autenticidade e não repúdio, e a legitimidade da informação, teríamos a seguinte escala de ponderação:

Incidente	Escala	Nível Impacto apurado de acordo com linhas orientadoras (Figura 2) Ativo Servidor Comunicações	Nível Impacto apurado de acordo com linhas orientadoras (Figura 2) Ativo Servidor Web
Disponibilidade	Falha na disponibilidade até 15 minutos	1	1
	Falha na disponibilidade até 3 horas	2	1
	Falha na disponibilidade até 1 dia	3	2
	Destruição Parcial de Informação	4	3
	Destruição Total de Informação	5	4
Integridade	Modificação não publicada	1	1
	Modificação sem controlo de versões	2	1
	Modificação não autorizada	3	2
	Perda parcial de histórico de versões	4	3
	Perda total de histórico de versões	5	4
Confidencialidade	Informação não classificada	1	1
	Informação confidencial acedida por pessoa interna não autorizada	2	1
	Informação confidencial acedida por pessoa externa não autorizada	3	2

	Divulgação interna de informação confidencial	4	3
	Divulgação externa de informação confidencial	5	4
Autenticidade e Não Repúdio	Informação sem fonte de autenticidade	1	1
	Alteração por negligência de autenticidade da Informação	2	1
	Alteração propositada de autenticidade da Informação	3	2
	Divulgação interna de informação sem autenticidade	4	3
	Divulgação externa de informação sem autenticidade	5	4
Legitimidade	Evidencia de não conformidade com regulamentos internos	1	1
	Evidencia de não conformidade normativa ou regulamentar	2	1
	Evidencia de não conformidade legal de acordo com legislação aplicada à área de negocio da Organização	3	2
	Dados pessoais acedidos, ou, sobre alvo de tratamento sem autorização dos titulares	4	3
	Dados Sensíveis acedidos, ou, sobre alvo de tratamento sem autorização dos titulares	5	4

Figura 3 – Matriz de impacto por Ativo (a Matriz é puramente exemplificativa podendo ser gerada outra qualquer Matriz ao critério do Responsável pela implementação de um PGRSI em determinada Organização e Contexto Organizacional)

Podemos assim verificar que o valor máximo da matriz associada a cada ativo dar-nos-á o valor de cada um dos ativos em análise, assim poderemos dizer, ainda na fase em que não existem medidas aplicadas, ou seja, sem controlos de segurança da informação, que o valor de impacto sobre o ativo Servidor de Comunicações de Voz de uma Organização é 5 (Ameaça à sobrevivência do Negócio de acordo com Figura 2) e o valor de impacto sobre o ativo Servidor Web de suporte a Site Institucional é 4 (Impacto grave nos serviços prestados de acordo com **Figura 2**), máximos valores assumidos por cada um dos ativos na Matriz de impacto por ativo (**Figura 3**).

5.2. Análise do risco

5.2.1. Identificação das ameaças a que estão expostos os ativos

Identificam-se, as ameaças às quais, se considera, que possam estar expostos os ativos por exemplo: desastres naturais (sismos, terramotos, etc), inundações, incêndio, falta de recursos humanos ou equipa insuficiente, acidentes de trabalho, manipulação de informação e cópias de informação, corrupção ou má configuração de *software*, abuso de direitos de perfil de administração de rede informática, acesso físico ou logico não autorizado a instalações e áreas condicionadas, etc…

Para cada uma das ameaças será necessário valorizar, tanto o antes como o depois da aplicação de medidas de segurança, o valor de frequência da mesma.

O valor da ameaça de cada ativo pode ser medido pela implementação de um processo de gestão de incidentes de segurança da informação [3] e [4], obtendo o número total de incidentes com a causa em determinada ameaça sobre um ativo, em determinado período. Para este trabalho, vamos hipoteticamente referenciar os seguintes valores:

- ✓ **Baixa (B):** Verificado pelo menos um Incidente de determinada ameaça sobre determinado ativo num período > 12 meses;
- ✓ **Média (M):** 6 meses < Verificado pelo menos um Incidente de determinada ameaça sobre determinado ativo num período < 12 meses;
- ✓ **Alta (A):** Verificado pelo menos um Incidente de determinada ameaça sobre determinado ativo num período < 6 meses ou menos.

Uma vez valorizadas as ameaças para cada um dos ativos, caso um deles seja alvo de várias ameaças, o valor de ameaça do ativo será o maior valor de todas as suas ameaças.

5.2.2. Identificação das vulnerabilidades a que estão expostos os ativos e a sua relação com as ameaças

Para cada ativo devem-se identificar, sobretudo em função de cada ameaça, as vulnerabilidades que possam favorecer a sua ação, indicando a probabilidade de que possa ocorrer o pior cenário possível, por exemplo: armazenamento de informação não protegido, baixas de pessoal, controlo de recrutamento inadequado, falha de fornecimento de energia, ausência de plano de incêndio, controlo de acessos de rede inadequado, ausência de controlo de licenciamento de software, ausência de formação profissional dos recursos, ausência de politicas/procedimentos/normas etc…

O valor da vulnerabilidade de cada ativo pode ser medido pela implementação de um processo de gestão de incidentes de segurança da informação [3] e [4], obtendo a percentagem da vulnerabilidade através do número de incidentes com a causa em determinada vulnerabilidade de um ativo, em determinado período, sobre o número total de incidentes de segurança que esse ativo teve com a mesma vulnerabilidade em determinado período. Para este trabalho, vamos hipoteticamente referenciar os seguintes valores:

- ✓ **Baixa (B):** Probabilidade de ocorrência de determinada vulnerabilidade sobre determinado ativo no espaço de um ano < 33%;

- ✓ **Média (M):** 33% < Probabilidade de ocorrência no espaço de um ano < 66%;

- ✓ **Alta (A):** Probabilidade de ocorrência no espaço de um ano > 66%.

Uma vez valorizadas as vulnerabilidades para cada um dos ativos, caso um deles tenha várias vulnerabilidades, o valor da vulnerabilidade do ativo será o maior valor de todas as suas vulnerabilidades.

5.3. Avaliação do risco

5.3.1. Cálculo do risco intrínseco

O Risco Intrínseco, é o risco sem a aplicação de qualquer tipo de medidas de segurança, ou seja, é o risco que os ativos têm por si, em função das ameaças e vulnerabilidades que lhes são aplicáveis.

Caso se analisem os valores de cada ativo, o seu valor de ameaça e o seu valor de vulnerabilidade (**Figura 4**), obteremos o Risco Intrínseco de cada ativo.

	Ameaça	Baixa			Média			Alta		
	Vulnerabilidade	B	M	A	B	M	A	B	M	A
Valor do Impacto sobre o Ativo segundo matriz **Figura 3**	0	0	1	2	0	1	2	0	1	2
	1	1	2	3	1	2	3	1	2	3
	2	2	3	4	2	3	4	2	3	4
	3	3	4	5	3	4	5	3	4	5
	4 (valor Ativo SW)	4	5	6	4	5	6	4	5	**6**
	5 (valor Ativo SCV)	5	6	7	5	6	**7**	5	6	7

Figura 4 – Exemplo de Matriz de Risco Intrínseco (a Matriz é puramente exemplificativa podendo ser gerada outra qualquer Matriz ao critério do Responsável pela implementação de um PGRSI em determinada Organização e Contexto Organizacional)

Nos exemplos dos ativos dados no ponto 5.1.3. - Avaliação do Impacto sobre os Ativos, o valor do Ativo Servidor de Comunicações de Voz é 5 e o valor do Ativo Servidor Web de suporte a Site Institucional é 4 (**Figura 3**), estamos tipicamente nas duas últimas linhas da Matriz de Risco Intrínseco (**Figura 4**), agora imaginemos o seguinte:

Os Ativos, Servidores, foram alvo de uma auditoria de segurança no ano de 2018 e verificou-se que:

- Tanto o Servidor de Comunicação de Voz (SCV) como o Servidor Web (SW) não tinham protocolos de segurança adequados, tendo sido alvos de vários ataques. No caso do SCV foi atacado em espaços temporais de 7 em 7

meses (Ameaça Média ponto 5.2.1.), já o SW foi atacado em espaços temporais de 1 em 1 meses (Ameaça Alta ponto 5.2.1.).

- Enquanto não forem aplicados protocolos de segurança nestes Servidores existe uma probabilidade de 100 % de ocorrência no período de um ano de novos ataques para ambos (Vulnerabilidade Alta de ambos os Servidores ponto 5.2.2.).

Assim, segundo a Matriz de Cálculo do Risco Intrínseco (**Figura 4**), temos o valor Risco Intrínseco = **6** para o Ativo SW e Risco Intrínseco = **7** para o Ativo SCV.

Deve ser elaborado um relatório do Risco Intrínseco, para todos os ativos do **PGRSI**, em que o Risco Total Intrínseco será o resultado de uma média aritmética simples dos valores de risco intrínseco dos ativos (dividir a soma dos riscos intrínsecos pelo número de ativos). O relatório deve ser divulgado á Gestão de Topo da Organização.

5.3.2. Definição do risco aceitável

A Gestão de Topo da Organização define o nível de riscos que está disposta a assumir, denominado "limite de risco", sendo necessária a gestão do risco dos ativos cujo valor de risco intrínseco seja superior a esse valor.

Imaginemos por exemplo que a Gestão de Topo defina o Risco Aceitável = 3, observamos que os ativos analisados no ponto 5.3.1. (**Figura 4**) com um Risco Intrínseco superior ao Risco Aceitável pela Gestão de Topo, assim, ambos os Ativos têm de ser alvo de medidas de segurança que permitam reduzir o Risco Intrínseco apurado até ao nível aceitável definido pela Gestão de Topo.

O limite de risco, ou Risco Aceitável, resulta do equilíbrio entre as medidas de segurança da informação a implementar e o impacto dessas. Se não se poderem cumprir essas medidas de segurança, deve-se, ou modificar de novo o limite de Risco Aceitável pela Gestão de Topo, ou, aplicar novas medidas de segurança da informação. Será uma decisão da Gestão de Topo da Organização!

O limite de risco do serviço é definido e revisto num determinado período temporal e aprovado diretamente pela Gestão de Topo, mesmo que se mantenha o nível do período anterior.

Para aqueles riscos que ultrapassam o limite de risco aceitável, realiza-se um procedimento de Tratamento de Riscos, de acordo com a fase descrita no ponto seguinte.

6. PGRSI - TRATAMENTO DO RISCO

A fase de tratamento de risco é levada a cabo aquando de uma primeira avaliação, assim que conhecido o Risco Aceitável pela Gestão de Topo e finalizada a análise do Risco Intrínseco (ponto 5.3.) ao qual estão sujeitos os ativos incluídos no respetivo âmbito do **PGRSI**, ou, sempre que se realize uma análise de riscos na organização.

Nesta fase são definidas as opções de tratamento do Risco Intrínseco (sem aplicação de medidas de segurança) face ao Risco Aceitável (limite de risco aceitável pela Gestão de Topo), e posteriormente apurado o Risco Residual, ou seja, o Risco apurado após aplicação de medidas de segurança sobre os Ativos.

Caso o Risco Residual não seja ainda aceitável, deve ser efetuado novo tratamento de risco, com aplicação de novas medidas de segurança que permitam uma das seguintes ações: evitar, assumir explorando oportunidades, remover, alterar, partilhar, ou, reter o risco [5].

A seleção de opções de tratamento do risco, ou seja, de aplicação de medidas de segurança, implica sempre a que a Organização faça uma relação de custo face ao benefício, relativamente aos esforços financeiros e operacionais levados em conta para a implementação de medidas de segurança para tratamento de determinado risco.

Deve ser definido um Plano de Tratamento de Risco de modo a documentar todas as opções identificadas para o tratamento dos riscos, dando a conhecer esse plano e o Risco Residual apurado á Gestão de Topo e às partes interessadas.

O Risco Residual assumido pela Organização, especificamente pela Gestão de Topo, deve ser alvo de monitorização, revisão e tratamento posterior, de acordo com a procura da melhoria contínua do próprio **PGRSI**.

6.1. Medidas de segurança da informação

As medidas de segurança a aplicar sobre os Ativos, de modo a obter o Risco Residual, devem referenciar os seguintes parâmetros:

- ✓ O custo de implementação de cada medida de segurança;
- ✓ O tipo de medida de segurança (Jurídica, Tecnológica, Gestão, etc);

- ✓ O tipo de proteção (evitar, detetar, reduzir o impacto, recuperar, redução da ameaça, transferir o risco, explorar e redução de vulnerabilidade);
- ✓ O seu estado (em estudo, em implementação, aplicada, revista);
- ✓ O controlo legal e normativo, à qual faz referência.

No caso de existirem condicionamentos de aplicação das medidas de segurança, devem ser indicados quais os fatores que condicionaram a sua ausência de aplicação.

6.2. Cálculo risco residual

Implementadas as medidas de segurança por ativo com o Risco Intrínseco superior ao Risco Aceitável, calculamos o Risco Residual, ou seja, o nível de risco resultante após implementação das medidas aplicáveis de segurança da informação, documentando esta operação no documento de aplicabilidade SoA (*Statement of Applicability*) [5].

No SoA relacionam-se todos os controlos de segurança, tanto os que serão implementados como os que não serão implementados, para os não implementados dever-se-á justificar a não implementação, de modo a reduzir a frequência de ocorrência das ameaças avaliadas na análise de riscos, e as ações previstas no Plano de Tratamento de Riscos atual. Por tudo isto, o Risco Residual é o risco a ser assumido pela Gestão de Topo.

Serão assim, calculados de novo os valores de risco dos ativos, após nova revisão dos valores das ameaças e das vulnerabilidades de cada ativo, ou seja, após aplicação de controlos de segurança.

O Risco Residual apurado deve ser detalhado, tanto por ativo como por serviço, com a finalidade de conhecer as áreas em que será necessário dar prioridade na implementação de novos controlos de segurança no Plano de Tratamento de Riscos.

6.3. Aceitação pela gestão de topo

A Gestão de Topo, considera que, tanto o custo das medidas a implementar como o Risco Residual resultante, são aceitáveis, em função dos objetivos estratégicos e de segurança da Organização, considerados em cada período definido, desta forma a Gestão de Topo deve aprovar a conformidade do documento de aplicabilidade SoA e ao relatório de Risco Residual para proceder à sua implementação.

Em caso de rejeição, a Gestão de Topo deverá expor os seus motivos, procedendo-se assim a uma nova seleção de controlos e contramedidas de segurança, para posteriormente realizar um novo cálculo do Risco Residual e elaborar um novo relatório de Risco Residual que seguirá o mesmo processo até aqui exemplificado, até à sua aceitação por parte da Gestão de Topo.

6.4. Plano tratamento de riscos

Estabelece-se no Plano de Tratamento de Riscos, as ações que a Organização vai realizar para implementar os controlos de segurança selecionados no documento de aplicabilidade (SoA - *Statement of Applicability*, documento de seleção de controlos), levando em conta:

- ✓ Calendário de implementação, definindo metas e datas para a sua realização;
- ✓ Priorizar ações com base nos resultados da análise de risco;
- ✓ Atribuir responsabilidades, antes da implementação dos controlos, identificar os responsáveis por assegurar a correta implementação de cada um dos controlos de segurança;
- ✓ Planear a aquisição ou disponibilidade dos recursos necessários.

O Plano de Tratamento de Riscos deve também ser aprovado pela Gestão de Topo.

7. PGRSI - MONITORIZAÇÃO E REVISÃO

O **PGRSI** deve permitir identificar novas ameaças ao longo do tempo, podemos assim assegurar que o **PGRSI** desempenha um papel preponderante na atualização, revisão e seguimento das ameaças, vulnerabilidades, riscos e controlos de segurança da informação aplicados sobre os Ativos do âmbito do **PGRSI**.

Esta fase do **PGRSI** é também ela, á semelhança da fase Comunicação e Consulta, transversal a todas as fases do **PGRSI**, e consiste em verificar de modo regular o próprio **PGRSI**, sendo que para isso deve a Gestão de Topo definir o período temporal em que a monitorização e a revisão do **PGRSI** são efetuadas.

A monitorização e revisão do **PGRSI** asseguram que os controlos de segurança aplicados continuam adaptados aos objetivos definidos no tratamento do risco, face a possíveis alterações internas e externas á Organização, perseguindo assim a melhoria contínua do **PGRSI**.

8.CONCLUSÕES

Numa perspetiva Organizacional os processos de gestão de risco sempre foram, de certa forma de modo voluntário e nunca como um pressuposto de obrigação legal, aplicados ao sucesso de uma Organização, avaliando os contextos sociais, políticos e económicos, em que essa se insere e as potenciais ameaças ao sucesso do seu negócio. O conceito Gestão de Risco tem sido assim, aplicado nos mais variadíssimos contextos Organizacionais, Gestão de Risco em Projetos, Gestão de Risco Empresarial e Gestão de Risco Financeiro, entre outos.

O que é curioso é que as doutrinas de Gestão de Risco, no momento em que surgiram num contexto Organizacional, não acentuavam o seu foco em preocupações tais como: a Informação como um ativo vital numa Organização, a era das Tecnologias e Sistemas de Informação, a era da procura da confidencialidade, da integridade, da disponibilidade, da autenticidade e não repúdio, e da legitimidade da informação, como fator de relevância numa avaliação de impacto de risco Organizacional.

É a partir do momento em que se reconhecem todas estas preocupações, numa era totalmente digital, que a informação passa a ser um ativo demasiado valioso e protegido pelas Organizações. Esta preocupação é acompanhada por legislação e normas *standard*, promovendo a implementação de processos Organizacionais num contexto de Segurança da Informação.

Com o contexto Segurança da Informação, surge assim a definição da metodologia de Gestão de Risco aplicada à Segurança da Informação, pese embora o facto da sua implementação continuar a ser visto sob com uma perspetiva voluntária das Organizações e não obrigatória.

Não existe nenhum sistema 100% seguro, mesmo com a adoção de processos de cerificação voluntários que possam contribuir para o cumprimento da legislação em vigor na prevenção contra ameaças, no entanto cada vez mais se torna evidente que os processos de gestão de risco nas Organizações, sejam quais forem os objetivos dos seus negócios, devem ser orientados à Segurança da Informação, pois a simples exposição de Informação confidencial, ou a perda de Informação, ou a ausência de credibilidade da Informação, de determinada Organização, pode ter consequências judiciais relevantes, contraordenações consideráveis, perda de credibilidade, e até mesmo á extinção da Organização!

"*Hence the saying: If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."* **Sun Tzu on the Art of War, III Atack by Stratagem sec. V a.C. [9]**

REFERÊNCIAS BIBLIOGRÁFICAS

[1] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (2013). NP ISO 27001:2013 - Tecnologia de informação Técnicas de segurança Sistemas de gestão de segurança da informação – Requisitos.

[2] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (2013). NP ISO 27002:2013 - Tecnologia de informação Técnicas de segurança – Código de boas praticas para Controlos de Segurança da informação.

[3] ISO/IEC 20000-1: 2011 - Information technology - Service management - Part 1: Service management systems requirements

[4] ISO/IEC 20000-2: 2012 - Information technology - Service management - Part 2: Guidance on application of service management systems.

[5] ISO/IEC 31000:2009 - Risk Management - Principles and guidelines

[6] Diretiva UE 2016/1148 do Parlamento Europeu e do Conselho. Jornal Oficial Da União Europeia.

[7] (a) Republica, D. da. (2012). Resolução do Conselho de Ministros N. 91 de 2012 (RNID). Diário Da Repúbilica, 1.a Série - N. 216 - 8 de Novembro de 2012. (b) Republica, D. da. (2018). Resolução do Conselho de Ministros N. 2 de 2018 (RNID). Diário Da Repúbilica, 1.a Série - N. 4 - 5 de Janeiro de 2018.

[8] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Jornal Oficial Da União Europeia.

[9] Giles, L. (2000). Sun Tzu on the Art of War. (C. E. Series, Ed.). England: Allandale Online.

A EMERGÊNCIA DE PERIGOS RESULTANTES DA DISPERSÃO TECNOLÓGICA DE AERONAVES NÃO TRIPULADAS NA SOCIEDADE CIVIL

AFONSO DE FREITAS DANTAS [1]

1 Investigador do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa. Contacto: afonso.freitas.dantas@gmail.com

RESUMO

A realidade social face à compra e utilização de aeronaves não tripuladas sofreu profundas alterações nos últimos anos. Preços substancialmente reduzidos, veículos mais facilmente manobráveis e a integração de inteligência artificial mais avançada têm sido alguns dos substanciais avanços de que a tecnologia dos UAV's tem vindo a usufruir, permitindo uma maior acessibilidade à população civil de algo que em tempos se encontrava restringido ao campo militar.

É uma missão inglória tentar impedir um atentado. Os mesmos são erráticos e imprevisíveis. No entanto, até que ponto a antecipação e a prevenção são já possíveis numa realidade tecnológica em velocidade acelerada e *desregulada*?

Palavras-Chave: UAV's, Drones; Revolução tecnológica e desafios emergentes; ANAC; Lei; Responsabilidade.

1. INTRODUÇÃO

A realidade social face à compra e utilização de aeronaves não tripuladas sofreu profundas alterações nos últimos anos. Preços substancialmente reduzidos, veículos mais facilmente manobráveis e a integração de inteligência artificial mais avançada têm sido alguns dos substanciais avanços de que a tecnologia dos UAV's[1] tem vindo a usufruir, permitindo uma maior acessibilidade à população civil de algo que em tempos se encontrava restringido ao campo militar.

Associadas a estas inovações, surgem novos problemas jurídicos, legais e, até mesmo, sociais. A facilidade com que um civil usufrui de forma recreativa do uso de um *drone*, poder-se-á facilmente transpor para o uso malicioso perpetrado por um potencial criminoso, *hacker* ou até mesmo terrorista. Trata-se da abertura de uma fronteira repleta de benefícios e de perigos, podendo estes últimos vir a suplantar os primeiros se as devidas precauções não forem tempestivamente tomadas.

Não pretendemos ceder a alarmismos com este estudo, muito menos aspiramos a ser os profetas da desgraça. Intentamos, isso sim, que se explorem e contenham potenciais ameaças à segurança da sociedade e do Estado, num plano em que Portugal apenas agora começa a explorar a superfície[2], quando outras Nações já experienciaram efetivos ataques à segurança e bem-estar do seu povo[3].

---

1 "Um UAV (Unmanned Aerial Vehicle) é um veículo aéreo concebido para voar sem tripulação a bordo. Poderá ser autónomo ou semi-autónomo e ter capacidade para transportar equipamentos que lhe permitam o cumprimento de uma tarefa específica em voo, com uma duração limitada, dependendo das especificidades de cada aparelho. Em alguns países também é usada a designação de "Drone", com significado semelhante aos UAV ou unicamente para os alvos aéreos, de modo a distinguir uns dos outros", citado de ELEUTÉRIO JOÃO LARANJINHO FALEIRO, *O Uso do Espaço Aéreo Por Aeronaves Não Tripuladas – Unmaned Aerial Vehicles (UAV)*, in *"Estudos de Direito Aéreo"*, pp. 263-306 (p. 263)

2 No dia 20 de Agosto de 2018, um *drone* caiu no interior do perímetro do Aeroporto Humberto Delgado, em Lisboa, levando à interrupção do tráfego aeroportuário durante um período de 8 minutos. Cfr. LUSA (2018, 21 de Agosto). *Drone* cai na pista do aeroporto de Lisboa, dono constituído arguido, *Público*. Extraído de: https://www.publico.pt/2018/08/21/local/noticia/drone-cai-na-pista-do-aeroporto-de-lisboa-1841663

3 A 22 de Abril de 2015, um drone de 50 cm de diâmetro, contendo pequenas quantidades de césio radioativo, foi encontrado no telhado da residência do Primeiro-Ministro Japonês, Shinzo Abe. Tratou-se de um protesto contra a reabertura das centrais nucleares após o incidente de Fukushima. De acordo com o suposto protestante, o mesmo fora lá colocado no dia 9 de Abril do mesmo ano. Cfr. DOUG BOLTON (2015, 25 de Abril). Man arrested for landing 'radioactive' drone on Japanese Prime Minister's roof, *The Independent*. Extraído de: https://www.independent.co.uk/news/world/asia/man-arrested-for-landing-radioactive-drone-on-japanese-prime-ministers-roof-10203517.html

Com isto, propomo-nos a analisar a evolução do papel do *drone*, dando especial destaque ao caso Português, investigando sobre as potenciais lacunas existentes na lei, os perigos a elas associadas, bem como hipotéticas soluções.

2. UMA NOVA ERA

Se almejamos analisar o presente paradigma em que nos situamos, devemos primeiramente compreender como é que a tecnologia e os componentes que constituem estas aeronaves se tornaram tão economicamente acessíveis.

As aeronaves não tripuladas, ou *"drones"*, provêm de uma extensão de tecnologia militar à sociedade civil, à semelhança do que sucedera com o *Personal Computer* (PC) ou o *Global Positioning System* (GPS). Do prisma da economia de escala, é possível depreender que a produção em série de quaisquer peças faz reduzir substancialmente o preço do custo de produção. Aliás, a simplicidade com que os múltiplos componentes se interligam comprovam o quão desnecessário é a existência de mão-de-obra qualificada na aglomeração destes mesmos, bastando observar alguns modelos destas aeronaves para comprovar o quão baixo o valor final poderá ficar.

Mantendo-se a questão de como é que a tecnologia chegou aos baixos valores que previamente anunciámos. CHRIS ANDERSON, CEO e cofundador da empresa 3D Robotics explicou, numa entrevista em 2015, como se processou tamanha queda vertiginosa dos custos de produção[4]:

"So, this is a drone. It's one of many different kinds of drones. This one's a quadcopter. What makes it a drone is that it has a brain, it can fly by itself, it's autonomous. Five years ago this is military technology, a million dollars. Two years ago, it was very high-end commercial stuff, thirty thousand dollars. This one [the quadcopter] is $750 dollars. What happened is that basically smartphone technology, the sensors, the GPS, the processors, turned out to be the enabling technology for low-cost drones. It uses the same sensors, the same kind of processors. It's just laid out in a different form."

Esta aglomeração de fatores possibilitou o produto final como hoje o conhecemos, com variedades de potências, rotores, habilidades e dimensões. A questão, porém, já não se prende

4 Cfr. LEIF KALDOR, Documentário *"The Age of the Drone"*, 2015 (minuto 3:20–3:55). Disponível em: https://www.youtube.com/watch?v=ikoZ9aFUu8A&t=1308s

com a mera existência do que para muitos era uma actividade recreacional, mas os perigos que possam vir a resultar da sua utilização maliciosa.

2.1 Revolução bélica

A filosofia de CARL VON CLAUSEWITZ introduziu-nos o conceito clássico de guerra simétrica, definida a nível internacional, como o confronto armado entre Estados com capacidades beligerantes igualáveis ou comparáveis[5], sendo que os constantes avanços tecnológicos apenas vieram a "enriquecer" este mesmo conceito, introduzindo a realidade do ciberespaço[6], bem como a sua desumanização, por força do uso de inteligência artificial.

Ora, se o recurso ao ciberespaço já hoje se enquadra igualmente no espectro da guerra assimétrica, o mesmo era inevitável que se viesse a suceder com a inteligência artificial. Contrariamente àquilo que a generalidade da comunicação social tem vindo a transmitir, o recurso a *drones* por entidades não-estatais já é uma realidade assente em teatros de guerra, tendo apenas muito recentemente sido iniciado o debate na sociedade civil relativamente ao seu uso como potencial arma de terror, isto no seguimento do presumido "atentado"[7] à vida do Presidente da República Bolivariana da Venezuela, Nicolas Maduro.

A 23 de Agosto de 2014, um vídeo a demonstrar a base aérea de Tabqa, na Síria, foi divulgado no Youtube pelo *Daesh* com recurso ao *DJI Phantom FC40*[8], um *drone* comercial com quatro rotores.[9] Ainda que as imagens de propaganda não fossem invulgares, o facto de uma organização terrorista recorrer ao que até então era considerado com um mero brinquedo recreativo apanhou de surpresa alguns analistas, começando a surgir hipóteses de virem a adquirir UAV's militares à medida que fossem conquistando território, à semelhança daquilo que o Hamas já proclamava possuir. Contudo, não foi o sucedido.

---

5 ROBIN GEIß, "Asymmetric conflict structures" in *International Review of the Red Cross*, Vol. 88, Number 864, 2006, pp. 757-777 (p. 760)

6 Cfr. AGÊNCIA LUSA, (2018, 30 de Agosto). Ministro garante segurança da rede de comunicações dos Negócios Estrangeiros, *Observador*. Extraído de https://observador.pt/2018/08/30/ministro-garante-seguranca-da-rede-de-comunicacoes-dos-negocios-estrangeiros/

7 À semelhança de alguns observadores internacionais, consideramos que o suposto atentado à vida de Nicolas Maduro poderá mais não ter sido que uma manobra política com o intuito de cimentar o seu poder. Não é nossa missão aferir a veracidade do sucedido, porém, temos que expressar as nossas dúvidas face aos factos contraditórios transmitidos pelas autoridades Venezuelanas, razão para a nossa hipótese alternativa à de um atentado. Cfr. SHEENA GOODYEAR, (2018, 07 de Agosto). Alleged drone attack like the one in Venezuela was just a matter of time: expert, CBC *Radio*. Extraído de https://www.cbc.ca/radio/asithappens/as-it-happens-monday-edition-1.4775407/alleged-drone-attack-like-the-one-in-venezuela-was-just-a-matter-of-time-expert-1.4775410

8 Relativamente às especificidades tecnológicas do mesmo aparelho, visitar o endereço https://www.dji.com/phantom-4/info

9 Cfr. YASMIN TADJDEH (2014, 28 de Agosto). ISIS Used A Miniature Surveillance Drone In Its Biggest Syria Victory Yet, *Business Insider*. Extraído de https://www.businessinsider.com/isis-has-demonstrated-drone-capabilities-2014-8?IR=T

Nos finais de 2016, começaram a surgir vários relatos referentes a ataques perpetrados pelo *Daesh* contra as várias facções da Guerra Civil Síria com recurso a *Drones Kamikazes* (veículos remotamente controlados acoplados com cargas explosivas de RPG-7[10] foram abatidos pelo Exército Sírio)[11], *Engenhos Explosivos Improvisados disfarçados de drones de reconhecimento* (acredita-se que dois soldados Curdos que abateram e intentaram desmontar o engenho explosivo disfarçado foram as primeiras baixas relatadas com recurso a este método)[12], bem como a *Drones Bombardeiros* (usados predominantemente na zona de Mossul, Deir Ezzor e Raqqa, estes drones ficaram conhecidos pelo lançamento de granadas de 40 mm, projéteis semelhantes à granada Norte-Americana Mk 2, bem como outros tipos de explosivos improvisados)[13]. Nenhuma destas aeronaves apresentava elevados níveis de sofisticação, sendo na sua grande maioria *quadcopters* rudimentares.[14]

Esta introdução de um novo elemento bélico no campo de batalha, bem como a intensificação do trauma psicológico adjacente à sua imprevisibilidade, abriu as portas a uma nova era de terror global, apenas limitado pela imaginação e capacidade tecnológica de quem a utiliza. O *Daesh* comprovou que o terror, uma vez mais, se transformou. A sua passagem do campo de batalha para o campo do terrorismo global seria apenas uma questão de tempo.

2.2 Terror evoluído

Antes de abordarmos o prisma dos perigos à sociedade civil relacionados com este novo tipo de "armamento", convém, compreendermos o fundamento para a prática de actos terroristas, bem como o seu enquadramento legal no contexto Português.

Citando JOHN STEINBRUNER, parte-se do pressuposto que as ações perpetradas por entidades não-estatais intentam ter consequências sociais mais vastas do que a mera criminalidade comum, razão pelo qual podem ser divididas em quatro categorias distintas[15]:

---

10 Cfr. Especificações referentes à mesma carga explosiva poderão ser encontradas em https://www.globalsecurity.org/military/world/russia/rpg-7-specs.htm

11 Cfr. IVAN YAKOVLEV (2016, 10 de Dezembro)

12 Cfr. MICHAEL S. SCHMIDT & ERIC SCHMITT (2016, 11 de Outubro). Pentagon Confronts a New Threat From ISIS: Exploding Drones, *The New York Times*. Extraído de https://www.nytimes.com/2016/10/12/world/middleeast/iraq-drones-isis.html?referer

13 Cfr. NICK WATERS, (2017, 24 de Maio). Types of Islamic State Drone Bombs and Where to Find Them, *Bellingcat*. Extraído de https://www.bellingcat.com/news/mena/2017/05/24/types-islamic-state-drone-bombs-find/

14 Cfr. BEM WATSON, (2017, 12 de Janeiro). The Drones of Isis, *Defense One*. Extraído de https://www.defenseone.com/technology/2017/01/drones-isis/134542/

15 ANDREW BLUM, VICTOR ASAL, JONATHAN WILKENFELD, JOHN STEINBRUNER, GARY ACKERMAN, TED ROBERT GURR, MICHAEL STOHL, JERROLD M. POST, JOSHUA SINAI, GARY LAFREE, LAURA DUGAN, DERRICK FRANKE, BARTOSZ H. STANISLAWSKI, GABRIEL SHEFFER, MARK IRVING LICHBACH, TODD SANDLER, and WALTER ENDERS. "Nonstate Actors, Terrorism, and

- ***Violence perpetrated for its own sake.*** *Actions falling into this category are basically the work of serial killers. It may be questionable whether there are any exclusive manifestations of this phenomenon distinguishable from ordinary crime, but such behaviour is probably a significant feature of most sustained terrorist episodes. The assessment of this type of violence, it would seem, might best be done by specialists on psychopathology, social pathology, and criminal justice.*

- ***Violence done for specific, readily imputable bargaining reasons.*** *Most episodes of terrorism encountered to date fall into this category; the more consequential of them are embedded in the general problem of civil conflict. Valid assessment of this type of terrorism presumably should be considered part of the appraisal of civil conflict with all its many subspecialties.*

- ***Violence done for strategic reasons.*** *Conceptually drawing a distinction between this and previous category may be difficult, but there clearly is a widespread, and at least plausibly valid, impression that the events of September 11 and al-Qaeda activities in general reflect an underlying purpose that could not be resolved by any imaginable political bargain. The apparent intention of strategic terrorism is to provoke self-destructive reactions in a society that are too strong to be directly defeated. This type of violence depends essentially on inducing a decisive societal autoimmune effect.*

- ***Violence done to achieve catastrophic social destruction.*** *As far as imputed intention is concerned, this category would be a combination of the first and the third, but its distinguishing feature is the use of means that can achieve massive social destruction directly without depending on autoimmune effects that in principle could be controlled by the target societies. To date there are no instances on record of this kind of violence, or even any serious attempts if long-standing nuclear deterrence practices are exempted from inclusion. It is nonetheless a legitimate concern given that, in principle, a clandestine organization capable only of small-scale operations might achieve massive social destruction by using nuclear explosives or a virulent biological pathogen.*

Weapons of Mass Destruction." in *International Studies Review 7, no. 1*, 2005, pp. 133-170 (p. 138) http://www.jstor.org/stable/3699642

As ações terroristas, como hoje as conhecemos, enquadram-se maioritariamente na terceira categoria que expusemos previamente. Sendo a constante pressão psicológica o grande objetivo do terrorismo moderno, o Major BRYAN A. CARD expõe um conceito-chave para compreender o quão adequado os *drones*, devido à sua agilidade e pequenas dimensões, se tornam à perpetuação desta missão[16]:

"(…) the message is not the violence or destruction itself, but rather the message is either embedded within the violence or follows from it in subsequent messaging. (…) By striking a particularly high-value target, such as a high-ranking political figure, celebrity, or athlete, a terrorist organization can demonstrate its ability to overcome the defensive capabilities of the state, displaying the terrorists' strength and the state's weakness"

Felizmente, a Europa nunca se deparou com ataques com recurso a este método, contrariamente àquilo que se sucede no seio do Médio Oriente, mas a sua memória não se encontra esquecida dos movimentos que surgiram após a Segunda Grande Guerra. A República Portuguesa, ao contrário do que é maioritariamente entendido entre a sociedade civil, sofreu bastante às mãos de organizações clandestinas no período pós-25 de Abril, tanto internas como externas. Tais exemplos são as Forças Populares 25 de Abril (FP 25)[17], a Frente de Libertação dos Açores (FLA)[18], bem como a tentativa de assassinato ao Embaixador de Israel, em 1979[19], e o atentado à embaixada da Turquia, em 1983[20].

16 BRYAN A. CARD. "Terror from Above: How the Commercial Unmanned Aerial Vehicle Revolution Threatens the US Threshold", in *Air & Space Journal, Spring 2018*, 2018, pp. 80-95 (p. 83)

17 "O grupo Forças Populares 25 de Abril, também conhecido pela sigla "FP 25", foi uma organização de extrema-esquerda, surgida no princípio dos anos 80 e apontada como responsável pela morte de 18 pessoas em diversos assaltos e atentados.". Citado de: http://ensina.rtp.pt/artigo/os-atentados-das-fp-25/

18 "Destruídas as sedes do PCP em Ponta Delgada e as sedes do PCP MDP/CDE e do MES em Angra do Heroísmo. Foi o início da destruição dos centros de trabalho do PCP que se sucederam nos dias seguintes, noutras localidades. Muitos dos dirigentes locais do PCP foram expulsos para Lisboa. A planificação das operações anti-comunistas foi obra da FLA. (JSC)". Citado de: http://www1.ci.uc.pt/cd25a/wikka.php?wakka=PulsarAgosto75

19 "O embaixador de Israel em Portugal já tinha também sido alvo de um atentado, reivindicado por extremistas palestinianos, em Novembro de 1979. Saiu ileso, mas morreu um polícia e ficaram feridas várias pessoas. O autor do atentado esperava sozinho Ephraim Eldar junto ao edifício da embaixada, com uma arma automática na mão. Eram 9h30 quando o Volvo azul do embaixador se aproximou do prédio da Rua António Enes. A rajada de tiros fez apenas alguns ferimentos ligeiros ao israelita porque o motorista ainda conseguiu pôr em marcha o carro quando se apercebeu do ataque.". Citado de: https://www.publico.pt/2001/09/22/jornal/portugal-foi-palco-de-atentados-terroristas-nos-anos-80-162057

20 "Em Junho de 1983 a Embaixada da Turquia em Lisboa foi alvo de um atentado terrorista. O único que até hoje ocorreu em Portugal. Cinco homens, que diziam pertencer ao autodenominado Exército Revolucionário Arménio, exigiam que Turquia reconhecesse a responsabilidade no genocídio do seu povo em 1915.". Citado de: https://sicnoticias.sapo.pt/programas/perdidoseachados/2011-06-08-ataque-a-embaixada

Contudo, apenas após os ataques do 11 de Setembro de 2001, é que se começou a notar significativas alterações no nosso paradigma legal, evidenciado por JORGE BACELAR GOUVEIA[21]:

"O Direito Legal Português tem feito um esforço assinalável no aperfeiçoamento do combate ao fenómeno do terrorismo, o que pode ser comprovado sob três perspectivas:

–*restringindo direitos fundamentais, em particular a liberdade individual e a inviolabilidade do domicílio;*

–*impondo novos crimes, segundo uma descrição típica;*

–*estabelecendo regras processuais, que oferecem particularidades.*"

Exemplos desta mesma alteração surgiram-nos com a *Lei de Combate ao Terrorismo*[22], a *Lei do acesso a dados de comunicações eletrónicas para a repressão de crimes graves*[23], a *Lei de Segurança Interna*[24], a *Lei do Cibercrime*[25], a *Orientação Política para a Ciberdefesa*[26], a *Estratégia Nacional de Combate ao Terrorismo*[27], a *Estratégia Nacional de Segurança do Ciberespaço*[28], o *Regime Jurídico das Ações Encobertas para Fins de Prevenção e Investigação Criminal*[29], a *Lei Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo*[30] e o *Regime Jurídico da Segurança do Ciberespaço*[31]. São apenas algumas das medidas legais e orientações que têm vindo a ser inseridas no nosso ordenamento jurídico, com vista a dar resposta às várias ameaças latentes contra o Estado de Direito Democrático.

Damos especial destaque à Lei de Combate ao Terrorismo, onde da qual se extrai a definição legal de "organização terrorista" e as classificações de actos terroristas, previstos

21 JORGE BACELAR GOUVEIA. "Direito da Segurança: Cidadania, Soberania e Cosmopolitismo", 2018, Almedina, (p. 671-672)

22 Lei n.º 52/2003, de 22 de Agosto, em cumprimento da Decisão Quadro n.º 2002/475/JAI do Conselho de 13 de Junho, com as seguintes alterações: Rect. n.º 16/2003, de 29 de Outubro; Lei n.º 59/2007, de 04 de Setembro; Lei n.º 25/2008, de 05 de Junho; Lei n.º 17/2011, de 03 de Maio; Lei n.º 60/2015, de 24 de Junho

23 Lei n.º 32/2008, de 17 de Julho, transpondo para a ordem interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março

24 Lei n.º 53/2008, de 29 de Agosto, com as seguintes alterações: Rect. n.º 66-A/2008, de 28 de Outubro; Lei n.º 59/2015, de 24 de Junho; Decreto-Lei n.º 49/2017, de 24 de Maio

25 Lei n.º 109/2009, de 15 de Setembro, transpondo para a ordem interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro

26 Despacho do Ministro da Defesa, n.º 13692/2013, de 28 de Outubro

27 Resolução do Conselho de Ministros n.º 7-A/2015, de 20 de Fevereiro

28 Resolução do Conselho de Ministros n.º 36/2015, de 12 de Junho

29 Lei n.º 101/2001, de 25 de Agosto, com as seguintes alterações: Lei n.º 60/2013, de 23 de Agosto; Lei n.º 61/2015, de 24 de Junho. Apenas esta última alteração veio a incluir "todos os ilícitos criminais relacionados com o terrorismo"

30 Lei n.º 83/2017, de 18 de Agosto, que transpõe parcialmente as Diretivas 2015/849/EU, do Parlamento Europeu e do Conselho, de 20 de Maio de 2015, e 2016/2258/EU, do Conselho, de 6 de Dezembro de 2016

31 Lei n.º 46/2018, de 13 de Agosto, que transpõe a Diretiva 2016/1148/EU, do Parlamento Europeu e do Conselho, de 6 de Julho de 2016

no n.º 1 do art. 2.º, 3.º e 4.º. Devido à amplitude de atos potencialmente terroristas, a lei especial visa expor que apenas poderão ser entendidos enquanto tais, quando a sua intenção for a generalizada desestabilização do funcionamento da Nação. Trata-se de um inverso ao que normalmente se sucede, pois a pormenorização dos potenciais crimes encontra-se elencada no Código Penal, que é a lei geral.

A nível Europeu, com o intuito de reforçar a cooperação interestadual entre Estados pertencentes ao respectivo continente contra o terrorismo internacional[32], foi criada a *Convenção do Conselho da Europa para a Prevenção do Terrorismo*[33], a 16 de Maio de 2005.

O Conselho da Europa adoptou a Convenção tendo em vista um aumento na "eficácia de textos internacionais existentes, na luta contra o terrorismo." O seu propósito foi um reforço nos "esforços dos Estados-membros em prevenir o terrorismo através de duas maneiras distintas:

- ao decretar, enquanto ofensas criminais, certos atos que possam levar à comissão de ofensas terroristas, nomeadamente: provocação pública, recrutamento e treino.
- ao reforçar a cooperação relativa à prevenção, tanto a nível interno (políticas nacionais de prevenção), como a nível internacional (alteração dos presentes acordos de extradição e assistência mútua e meios complementares)."[34]

A Convenção nada mais se tratou se não de um reconhecimento por parte da comunidade do continente Europeu de que o terrorismo se trata de uma realidade transfronteiriça, a qual requere a constante cooperação e troca de informações por parte dos seus Estados.

---

32 Cfr. Council of Europe, Explanatory Report to the Council of Europe Convention on the Prevention of Terrorism, in *Council of Europe Treaty Series – No. 196*, 16 of May 2005. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800d3811

33 *Conselho da Europa*, *Convenção do Conselho da Europa para a Prevenção do Terrorismo*, adoptada em Varsóvia, 16 de Maio de 2005 (ratificada no ordenamento jurídico Português através do Decreto do Presidente da República, n.º 74/2015, de 23 de Julho). Disponível em: http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c3246795a5868774d546f334e7a67774c336470626d6c7561574e7059585270646d467a4c31684a4c33526c654852766379397763484931 4e533159535638794c6d527659773d3d&fich=ppr55-XI_2.doc&Inline=true

34 Council of Europe, *Details of Treaty Nº. 196: Council of Europe Convention on the Prevention of Terrorism* (traduzido). Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/196

3. NOVAS AMEAÇAS

Retornando à atualidade, propomo-nos agora a expor as ameaças já conhecidas no seio do nosso território, bem como as medidas legais já existentes para a sua prevenção. Note-se que, apesar de terem mero carácter acidental ou apenas criminoso, estas ameaças facilmente poderão transpor-se para o campo do terrorismo. Como observámos previamente, a distinção entre um acidente e um ato terrorista poderá, muitas vezes, resumir-se à existência ou inexistência de uma mensagem associada à respetiva tragédia. Estando assim delimitados, observemos se as medidas legais atuais são adequadas à proteção da Nação.

3.1 Drones VS Aviões comerciais

Iniciemos a nossa análise com um problema que tem sido excessivamente recorrente na República Portuguesa, nomeadamente, a obstrução do espaço aéreo pertencente à aviação comercial.

Um dos primeiros relatos a ter destaque nos meios de comunicação social data do dia 13 de Dezembro de 2016, no qual um *drone* terá entrado no perímetro do aeroporto de Lisboa, sobrevoando as pistas e a placa, causando perturbações nas operações do mesmo.[35] Não se tratava do primeiro incidente relacionado com o uso indevido destas aeronaves não tripuladas, tendo o telejornal da RTP realizado uma reportagem[36] a 22 de Maio de 2015 sobre o aumento exponencial na oferta e na compra de *drones* e sobre os potenciais perigos para a aviação civil, vindo esta mesma especulação a ser comprovada pelo total de 9 incidentes que ocorreram no mesmo ano. [37]

À data dos factos constatados, o *Regime Aplicável Às Contra-Ordenações Aeronáuticas Civis*[38] e o *Decreto-Lei n.º 163/2015, de 17 de Agosto*[39], eram os únicos diplomas legais a prever os regimes sancionatórios e as respetivas coimas em caso de perturbações ao regular

35 Cfr. JORNAL I, (2016, 13 de Dezembro). Drone invade aeroporto de Lisboa, *Jornal I*. Extraído de: https://ionline.sapo.pt/538119

36 Cfr. JOSÉ MANUEL LEVY, PEDRO PESSOA, (2015, 22 de Maio). Ninguém pára os drones sobre o aeroporto de Lisboa, *RTP*. Extraído de: https://www.rtp.pt/noticias/pais/ninguem-para-os-drones-sobre-o-aeroporto-de-lisboa_v830972

37 Cfr. REDAÇÃO / STS, (2016, 13 de Dezembro). Drone sobrevoa aeroporto de Lisboa e põe em risco a segurança, *TVI 24*. Extraído de: http://www.tvi24.iol.pt/sociedade/13-12-2016/drone-sobrevoa-aeroporto-de-lisboa-e-poe-em-risco-a-seguranca

38 Decreto-Lei n.º 10/2004, de 09 de Janeiro

39 "Cria os regimes sancionatórios aplicáveis aos regimes jurídicos do céu único europeu, constante dos Regulamentos (CE) n.os 549/2004, 550/2004, 551/2004 e 552/2004, de 10 de março de 2004, e ao Regulamento (UE) n.º 805/2011, da Comissão, de 10 de agosto, que estabelece regras detalhadas para as licenças de controlador de tráfego aéreo e certos certificados em conformidade com o Regulamento (CE) n.º 216/2008, de 20 de fevereiro de 2008". Citado de: https://dre.pt/home/-/dre/70025054/details/maximized?p_auth=zIE9N0kF

funcionamento das aeronaves civis. Contudo, como já se tornava excessivamente notório, a inexistência de uma delimitação legal e clara sobre a utilização de aeronaves civis pilotadas remotamente, perpetuava o impedimento de uma atuação fiscalizadora e preventiva por parte das autoridades.

Tendo entrado em vigor a 13 de Janeiro de 2017, o *Regulamento Relativo às Condições de Operação Aplicáveis à Utilização do Espaço Aéreo pelos Sistemas de Aeronaves Civis Pilotadas Remotamente ("Drones")*[40], veio a definir de forma extensiva, os conceitos e as mais recentes limitações aos espaços e altitudes acessíveis às Aeronaves pilotadas remotamente (*RPA, Remotely Piloted Aircraft*)[41], a nova terminologia legal para *drone*. Para os efeitos do nosso estudo, interessa-nos referir que "as RPA apenas podem efetuar voos diurnos, em operações VLOS, até 120 metros acima da superfície"[42], não podendo circular dentro das áreas definidas nos termos do art. 11.º do mesmo documento. Contudo, poderão ser requeridas autorizações à ANAC, devidamente justificadas, para situações que excedam as limitações que apresentámos anteriormente[43], tendo igualmente que ser forçosamente requeridas caso a sua "massa máxima operacional" exceda os 25 kg[44]. Tristemente, mesmo após estas atualizações legais e a distribuição gratuita do *Guia de Utilização do Espaço Aéreo*[45], a mesma continuou sem surtir os devidos efeitos dissuasores.

Desde relatos da aproximação de drones a 900[46] e a 1200[47] metros de altitude durante o mês de Junho de 2017, nenhuma ocorrência foi tão grave como a que se sucedeu no dia 1. Às 16h40, um "Boeing 737-800, com capacidade para cerca de 160 passageiros, da companhia TVF, France Soleil, grupo Air France/KLM, estava na aproximação final para aterrar, a 3,5 quilómetros da pista 35" do Aeroporto Francisco Sá Carneiro, no Porto, quando um drone teria colidido contra si, a 450 metros de altitude, não fosse pelas manobras evasivas realizadas pelos pilotos.[48]

---

40 Regulamento n.º 1093/2016, de 14 de Dezembro, com a seguinte alteração: Rect. n.º 272/2017, de 04 de Maio
41 Idem. Artigo 2.º, alínea *h)*
42 Idem. Artigo 3.º, n.º 1
43 Idem. Artigo 10.º, n.º 1
44 Idem. Artigo 10.º, n.º 3
45 Disponível em: https://www.voanaboa.pt/Files/downloads/Guia-Utilizacao-Espaco-Aereo.pdf
46 LUSA, (2017, 26 de Junho). Novo Incidente com drone em Lisboa, *TSF Rádio Notícias*. Extraído de: https://www.tsf.pt/sociedade/interior/novo-incidente-com-drone-em-lisboa-8593066.html
47 JORNAL DE NOTÍCIAS, (2017, 19 de Junho). Drone voou ao lado de avião a 1200 metros de altitude em Lisboa, *Jornal de Notícias*. Extraído de: https://www.jn.pt/nacional/interior/dronevoou-ao-lado-de-aviao-a-1200-metros-de-altitude-em-lisboa-8575441.html
48 Cfr. RÁDIO RENASCENÇA, (2017, 01 de Junho). Avião evita colisão com "drone" na aproximação ao Aeroporto do Porto, *Rádio Renascença*. Extraído de: http://rr.sapo.pt/noticia/85251/aviao-evita-colisao-com-drone-na-aproximacao-ao-aeroporto-do-porto#comentar

Este relato apenas avivou a nossa memória para o incidente com o Voo US Airways 1549, no Rio Hudson, em 2009. O relatório final, realizado pela *National Transportation Safety Board*[49], determinou que cada uma das duas turbinas da aeronave (Airbus A320-214)[50] havia sugado, pelo menos, dois Gansos do Canadá[51], tendo sido observado que se encontrava um ganso com cerca de quatro quilos em cada motor. Cada motor de uma aeronave daquelas dimensões está capacitado para apenas poder ingerir um quilo de massa sem impossibilitar a produção de propulsão suficiente para sustentar a aeronave no ar.[52]

Ora, atendendo aos dados apresentados, será que um *drone* pessoal poderá causar estragos equiparáveis? Sendo a marca mais vendida em Portugal, utilizemos a *DJI* a título exemplificativo. Em acordo com as especificações providenciadas pelo *site* oficial da empresa, os veículos dividem-se em três categorias[53]: Consumidor, Profissional e Enterprise. A primeira abrange a criação de fotografias e vídeos a título recreativo; a segunda é focada em captações de imagem e vídeos a nível profissional; a terceira, a mais sofisticada, compreende aplicabilidades a nível empresarial como a agricultura, energia, segurança pública, manutenção de edifícios e auxílio à construção civil. Analisemos as especificações de fábrica daqueles que estão comercialmente disponíveis ao público:

Categoria	**Modelo**	**Peso da aeronave** (pode incluir câmara)	**Peso máximo**	**Velocidade máxima**	**Altitude máxima**	**Duração da bateria**
Consumidor	Phantom 4 Pro V2.0[54]	1375 g	1375 g	72 kph	6000 m	Aprox. 30 minutos

49 Entidade responsável pela investigação de acidentes na aviação civil nos Estados Unidos da América. Disponível em: https://www.ntsb.gov/about/history/Pages/default.aspx
50 Aeronave com 37,47 m de comprimento, 11,76 m de altura e capacidade para 165 passageiros. Extraído de: https://www.sata.pt/pt-pt/frota/a320
51 Mais informações relativas a características do mesmo animal encontram-se disponíveis em: https://www.canadiangeographic.ca/article/animal-facts-canada-goose
52 Cfr. NATIONAL TRANSPORTATION SAFETY BOARD. *Aircraft Accident Report: Loss of Thrust in Both Engines After Encountering a Flock of Birds and Subsequent Ditching on the Hudson River; US Airways Flight 1549; Airbus A320-214, N106US; Weehawken, New Jersey; January 15, 2009*, (2010), p. 80-85. Disponível em: https://www.ntsb.gov/investigations/AccidentReports/Reports/AAR1003.pdf
53 Cfr. https://www.dji.com/
54 Cfr. https://www.dji.com/phantom-4-pro-v2/info#specs

Profissional	Inspire 2[55]	3440 g	4250 g	94 kph	5000 m (com hélices adaptadas)	Aprox. 27 minutos
Enterprise	Matrice 100[56]	2355 g	3600 g	79 kph (sem carga)	Não especificado	40 minutos (com duas baterias TB48D e sem carga) – 16 minutos (1 kg de carga)
	Matrice 600 Pro[57]	9.5 kg	15.5 kg (recomendado)	65 kph	4500 m	38 minutos (com seis baterias TB48S) – 18 minutos (5.5 kg de carga)
	Spreading Wings S1000+[58]	4.4 kg	11 kg	Não especificado	Não especificado	15 minutos

55 Cfr. https://www.dji.com/inspire-2/info#specs
56 Cfr. https://www.dji.com/matrice100?site=brandsite&from=landing_page
57 Cfr. https://www.dji.com/matrice600-pro?site=brandsite&from=landing_page
58 Cfr. https://www.dji.com/spreading-wings-s1000-plus?site=brandsite&from=landing_page

Além destes dados, a *DJI* específica, igualmente, como os seus equipamentos vêm com sistema de GPS integrado e com *software* devidamente adaptado às permissões legais de cada país, estando cada utilizador obrigado a registar os seus dados pessoais, ou até mesmo requerer autorizações especiais, para sobrevoar sobre certos espaços. Ou seja, em princípio, o *software* atual deverá impedir a entrada num aeroporto. Contudo, os drones continuam a não possuir um limitador de altura, pelo que o utilizador poderá ultrapassar os 120 metros de altura legalmente previstos em Portugal.[59]

Utilizámos estes dados como exemplo, pois a inexistência de certas limitações possibilita a entrada de uma aeronave destas dentro da turbina de um avião comercial e os resultantes danos catastróficos que exemplificámos anteriormente. Seja feito de forma propositada ou acidentalmente, o verdadeiro centro da questão será sempre as vidas humanas que se encontram em risco.

3.2 Entrega de contrabando

Não obstante a ameaça mais pertinente contra aeronaves civis, existem outras que são igualmente propícias a ocorrerem nos anos vindouros, nomeadamente, a entrega de contrabando dentro dos estabelecimentos prisionais.

Fenómeno já ocorrido em países como a República Federativa do Brasil[60] e os Estados Unidos da América[61], a primeira notícia a relatar algo semelhante surge, em Portugal, no dia 05 de Outubro de 2016, reportando que ao longo de várias semanas haviam sido "detetados drones a sobrevoar as prisões de Braga, Vale do Sousa e Caxias, tendo mesmo sido identificado o piloto de um destes drones, familiar de um dos reclusos" no dia 18 de Setembro. Nada de mal se sucedeu nestas três ocorrências, tendo Jorge Alves, do Sindicato Nacional do

59 Dados extraídos de dois vídeos providenciados pela secção *"FLY SAFE"* da página Web oficial da *DJI*: Cfr. https://www.dji.com/flysafe?site=brandsite&from=footer

60 "Três pessoas foram presas com um drone (veículo aéreo não tripulado) que levaria 18 celulares para a Penitenciária Desembargador Adriano Marrey II, em Guarulhos, na Grande São Paulo, na madrugada desta terça-feira (21). Segundo a polícia, nove carregadores e quatro fones de ouvidos também foram encontrados com o trio.". Citado de: G1 SÃO PAULO, (2014, 21 de Agosto). Trio é preso com drone que levaria 18 celulares para presídio em Guarulhos, *G1*. Extraído de: http://g1.globo.com/sao-paulo/noticia/2014/08/trio-e-preso-com-drone-que-levaria-18-celulares-para-presidio-em-guarulhos.html

61 "Um drone deixou cair um pacote com droga no átrio de um centro de reabilitação e correção norte-americano, quando utentes estavam no recreio, despoletando uma batalha campal. A encomenda continha tabaco, marijuana e heroína, confirmou o Departamento de Reabilitação e Correção do Ohio ao jornal ao News Journal. O incidente ocorreu no final de julho, quando os guardas foram obrigados a intervir numa luta entre os detidos. Nove deles foram castigados e colocados na solitária.". Citado de: REDAÇÃO / CF, (2015, 05 de Agosto). Drone entrega droga na prisão, *TVI24*. Extraído de: http://www.tvi24.iol.pt/internacional/eua/drone-entrega-droga-na-prisao

Corpo da Guarda Prisional, mencionado que julgavam tratar-se de recolhas de imagens por mera curiosidade.[62]

Foi apenas com a entrada em vigor do *Regulamento n.º 1093/2016*, no n.º 3 do seu art. 11.º,[63] que passou a ser proibido que aeronaves pilotadas remotamente pudessem sobrevoar estabelecimento prisionais ainda que, uma vez mais, pouco efeito prático tenha surtido. A 12 de Agosto de 2018, a Direção Geral dos Serviços Prisionais recebeu um alerta sobre a possibilidade de estarem a ser introduzidas drogas e telemóveis na prisão de alta segurança de Vale de Judeus, na Azambuja, com recurso a aeronaves remotamente controladas, tendo sido posteriormente confirmado o avistamento de um drone no perímetro através da videovigilância, ainda que nada tenha sido encontrado.[64]

3.3 Aeromodelismo enquanto potenciador do terrorismo

Existe uma vasta comunidade global que se dedica à prática de aeromodelismo, comprovado pela existência de páginas Web dedicadas exclusivamente ao mercado dos drones, como é o caso da *DIY Drones*[65], as quais estão conectadas a lojas *online* que possibilitam a compra de peças e sistemas eletrónicos para construir um de forma autónoma[66] inclusive componentes que aumentam a durabilidade e eficácia dos mesmos.[67] O problema que surge com esta prática é a capacidade do indivíduo se evadir a quaisquer registos de identidade, como a que a *DJI* requer, possibilitando a prática de atos criminosos sem nunca ser detetado.[68]

---

62 Cfr. MARIA INÊS COELHO, (2016, 05 de Outubro). Prisões portugueses estão a ser sobrevoadas por drones, *Pplware*. Citado e extraído de: https://pplware.sapo.pt/informacao/prisoes-portuguesas-estao-sobrevoadas-drones/

63 "3 — Sem prejuízo do disposto no Decreto -Lei n.º 248/91, de 16 de julho, uma RPA, não pode igualmente voar sobre instalações onde se encontrem sedeados órgãos de soberania, embaixadas e representações consulares, instalações militares, instalações das forças e serviços de segurança, locais onde decorram missões policiais, estabelecimentos prisionais e centros educativos da Direção -Geral de Reinserção e Serviços Prisionais, exceto quando devidamente autorizadas pelas entidades representativas desses órgãos e sem prejuízo do cumprimento do disposto no presente Regulamento."

64 Cfr. MIGUEL CURADO, (2018, 14 de Setembro). Guardas temem drones com droga e telemóveis, *Correio da Manhã*. Extraído de: https://www.cmjornal.pt/portugal/detalhe/guardas-temem-drones-com-droga-e-telemoveis

65 Cfr. https://diydrones.com/

66 A loja online, em questão, vende três kits para principiantes começarem a construir o seu próprio *drone*. Cfr. https://store.mrobotics.io/category-s/124.htm

67 Cfr. https://store.mrobotics.io/category-s/115.htm

68 *"On 16 May 2017, 10 Chinese-made DJI Phantom-4 Pro drones were seized at Bengaluru which could fly up to 6,000 metres altitude and carry up to half a kilogram payload. This drone is capable of acting by itself upon finding obstacles, has an intelligent battery system and an advanced satellite navigation system compatible with GPS as well as the Russian Global Navigation Satellite System (GLONASS). Thus, all that a terrorist would need to do in order to can bomb a target or place an explosive anywhere is by launching a pre-programmed drone from a secluded place at a set time and disappear. The programmed drone would thus do the job."*. Citado de:

Estes *drones*, consoante os conhecimentos individuais de cada operador, poderão ter um *software* mais ou menos desenvolvido, e ambos os cenários apresentam graves problemas de segurança. A existência de *software* mais sofisticado, à semelhança do que já foi previamente dito, possibilita um melhor controlo sobre o veículo, requerendo menos treino para o utilizar.[69] O oposto, nomeadamente a existência de *software* menos avançado, possibilita a criação daquilo que ficou conhecido como um *zombie drone*.[70]

São apenas alguns dos desafios que podemos vir a ter que debater, no futuro próximo, face à regulamentação das lojas físicas e *online* que facultam estas peças e componentes.

ATUL PANT. "Drones: An Emerging Terror Tool" in *Journal for Defence Studies, Vol. 12, No. 1, January–March 2018*, 2018, pp. 61-75 (p. 64)

69 *"Drones can be easily purchased online or from numerous hobby or electronics stores without the need for theft. (…) Multiple models are available and can be utilized by and adversary with little knowledge or training needed. The advancements in radio controlled devices, GPS, video, flight duration times, controllability and damage resistance all make current iterations of drones more reliable that previous versions over the years"*. Citado de: G4S CORPORATE RISK SERVICES. *Drones: Threat from Above*, 2017, (p. 8)

70 Samy Kamkar, programador, criou um software chamado *SkyJack*. Este, quando inserido no drone "líder", possibilita o corte do sinal Wi-fi entre outro drone e o seu controlador. Bastará aproximar-se num raio de 100 metros do mesmo, que o software obrigará o drone "vítima" a segui-lo. O mesmo software continua disponível, gratuitamente, em: https://samy.pl/skyjack/ . Cfr. PAUL MARKS, (2013, 9 de Dezembro). Drones turned into zombies using an easy Wi-fi hack, *NewScientist*. Disponível em: https://www.newscientist.com/article/dn24726-drones-turned-into-zombies-using-an-easy-wi-fi-hack/

4. UM DECRETO-LEI INEFICAZ

Exposto o paradigma do nosso território, torna-se necessária uma análise à nova legislação que entrou em vigor no dia 28 de Julho de 2018, o Decreto-Lei n.º 58/2018, de 23 de Julho[71].

A nova lei é uma tentativa de aperfeiçoamento do regulamento da ANAC, melhorando aspetos cruciais à segurança pública:

- Obriga o utilizador a registar o seu sistema de aeronave não tripulada (UAS, Unmanned Aircraft System)[72] sempre que a aeronave tiver mais de um total de 250 gramas[73];
- Toda e qualquer venda de aeronaves com peso superior a 250 gramas tem que ser declarada à ANAC, tendo os vendedores que fornecer os dados estipulados pelo art. 4, n.º 1.º[74];[75]
- Contratação obrigatória de seguro de responsabilidade civil, aplicável a danos patrimoniais, para aeronaves com peso superior a 900 gramas.

Nas palavras do Ministro do Planeamento e das Infraestruturas do XXI Governo Constitucional, à data, Pedro Marques, "«*constatou-se que não tínhamos os instrumentos suficientes, não só para detetar, mas sobretudo para penalizar as utilizações indevidas*»"[76]. Contudo, o problema persiste. Ainda que já possua eficácia legal, a execução prática do presente diploma está dependente da criação e disponibilização pela ANAC de uma plataforma eletrónica que possibilite o registo da parte do vendedor e do operador.[77] Por outras palavras, é como se o presente decreto-lei fosse ainda não existisse.

---

71 "Estabelece um sistema de registo e seguro de responsabilidade civil obrigatório aplicável aos sistemas de aeronaves civis não tripuladas («drones»)". Citado de: https://dre.pt/web/guest/pesquisa/-/search/115740753/details/maximized

72 "sistema que compreende a aeronave não tripulada e o equipamento de controlo remoto da mesma". Citado de: Artigo 2.º, alínea *h)* do Decreto-Lei n.º 58/2018, de 23 de Julho

73 Idem. Artigo 3.º, n.º 1 e 2

74 Não desejamos ser exaustivos, razão pelo quão apenas citamos o disposto na alínea *a)*, o qual estabelece os dados pessoais necessários para o devido registo: "O nome, o número de identificação civil, o número de identificação fiscal, o endereço de correio eletrónico e os números de contacto telefónico do operador requerente, bem como a respetiva morada ou sede, caso se trate de pessoa coletiva;". Citação extraída de: https://dre.pt/web/guest/pesquisa/-/search/115740753/details/maximized

75 Idem. Artigo 8.º, n.º 1 e 2

76 Citação extraída de: https://www.portugal.gov.pt/pt/gc21/comunicacao/noticia?i=drones-passam-a-ter-registo-obrigatorio

77 Cfr. DEPARTAMENTO DE COMUNICAÇÃO DA AUTORIDADE NACIONAL DA AVIAÇÃO CIVIL, (2018, 6 de Julho). Comunicado de Imprensa 03/2018 – Esclarecimentos sobre o Decreto-Lei aprovado pelo Governo relativo ao registo e seguro de drones, *ANAC*. Extraído de: https://www.anac.pt/vPT/Generico/Noticias/noticias2018/Paginas/ComunicadodeImprensa032018.aspx

Apesar dos significativos avanços legislativos ao longo dos últimos 10 anos, Portugal continua substancialmente atrasado em relação aos seus contemporâneos Europeus no que diz respeito a ameaças com recurso a *drones*. A análise que realizámos à falta de meios preventivos, até à data, denota o quão suscetível a República Portuguesa se encontra face a esta ameaça.

4.1 O exemplo francês

De acordo com a página oficial do Ministério da Transição ecológica e solidariedade (*Ministère de la Transition écologique et solidaire*)[78], o aumento exponencial de 90 utilizadores declarados no mês de Novembro de 2012, para cerca de 3200 em Dezembro de 2016, forçou o Governo a tomar medidas regulatórias com vista a possibilitar o desenvolvimento em segurança deste setor, prevenindo assim a ocorrência de acidente ou, até mesmo, ataques terroristas.[79]

Para o mesmo efeito, foram adotados o *"Arrêté du 17 décembre 2015 relatif à l'utilisation de l'espace aérien par les aéronefs qui circulent sans personne à bord"*[80] e o *"Arrêté du 17 décembre 2015 relatif à la conception des aéronefs civils qui circulent sans personne à bord, aux conditions de leur emploi et aux capacités requises des personnes qui les utilisent"*[81], tendo igualmente sido disponibilizado um mapa digital relativo às áreas restritas de todo o território Francês[82].

A legislação Francesa é bastante semelhante ao presente decreto-lei Português, ainda que englobe mais detalhes. Delimita as actividades com *drones* em três categorias, nos termos do art 3.º do *Arrêté du 17 décembre 2015 relatif à la conception des aéronefs civils qui circulent sans personne à bord, aux conditions de leur emploi et aux capacités requises des personnes qui les utilisent*: actividades de lazer e competitivas; voo com vista a realizar testes e experiências; e atividades particulares, que são aquelas que não se enquadrarão em nenhuma

78 Site oficial do Ministério disponível em: https://www.ecologique-solidaire.gouv.fr/
79 Cfr. Informação providenciada pela secção *"Quelle place pour les drones dans le ciel français?"* da página Web do respetivo Ministério, publicada a 13 de Dezembro de 2016. Extraído de: https://www.ecologique-solidaire.gouv.fr/quelle-place-drones-dans-ciel-francais
80 JORF n°0298 du 24 décembre 2015, page 23890, texte n° 20. Decreto de 17 de Dezembro de 2015 relativo à utilização do espaço aéreo para as aeronaves que circulam sem pessoas a bordo (traduzido)
81 *JORF n°0298 du 24 décembre 2015, page 23897, texte n° 22.* Decreto de 17 de Dezembro, 2015 relativo ao conceito de aeronaves civis que circulam sem pessoas a bordo, as condições para o seu emprego e as capacidades exigidas às pessoas que as utilizam (traduzido)
82 Cfr. https://www.geoportail.gouv.fr/donnees/restrictions-pour-drones-de-loisir

das anteriores. Igualmente, o legislador teve o cuidado de não delimitar de forma igual as áreas potencialmente restritas[83]:

"Drones are not allowed to fly in the immediate vicinity of an airfield, and must adhere to strict altitude limits in the surrounding zone, absent authorization from the airfield's operator. For the purposes of these regulatory provisions, the area surrounding an airfield is divided into three zones, the dimensions of which depend on the type of airfield at the center. For example, if a runway is less than 1,200 meters long and is not equipped for instrument approach procedures, the zone where drone flying is entirely prohibited (except with the airfield operator's permission) extends 5 kilometers from either end of the runway, and 0.5 kilometers from either edge of the runway. In the zone that extends from 0.5 to 3.5 kilometers from each edge of the runway, drones may not fly at an altitude of more than 50 meters without the airfield operator's permission. Finally, in the zone that extends from 3.5 to 5 kilometers from each edge of the runway, drones may not fly at an altitude of more than 100 meters without authorization. Airfields that have longer runways, are equipped for instrument approach procedures, or are used for ultralight aviation, and heliports have similar restrictions but with differences in distances and altitude limits."

Por fim, o ordenamento jurídico Francês prevê sanções muito mais severas do que aquelas previstas em Portugal, nomeadamente, a possibilidade de se ser encarcerado até seis meses e de ser aplicada uma coima de €15.000 em casos de negligência ou erro. Em caso de ser classificado como um voo intencional, a pena aumentará até um ano e uma coima de €45.000.[84]

Estas são apenas algumas das alterações legislativas que poderiam ser introduzidas no presente regulamento da ANAC, com vista a dissuadir potenciais incursões ilícitas em zonas restritas e proibidas.

83 *The Law Library of Congress*, (2016, 22 de Julho). Regulation of Drones: France, *Library of Congress*. Disponível em: https://www.loc.gov/law/help/regulation-of-drones/france.php#_ftn8
84 Artigo L6232-2 do *Code des transports*

5. CONCLUSÕES

À semelhança do que já está a ser testado no Aeroporto Humberto Delgado, a implementação obrigatória de equipamentos de deteção e inibição de drones em áreas proibidas e restritas poderá ser um meio adequado e necessário à prevenção de futuras incursões, acidentais, criminosas ou terroristas.

No espetro das empresas manufatoras de aeronaves remotamente pilotadas, poderá ser necessário a criação de legislação que obrigue tais criadores e fabricantes a implementar *software* que impossibilite drones civis de superarem os 120 metros de altura, com vista a igualmente impedir futuros incidentes.

É claro, nada disto é capaz de impedir um atentado. Os mesmos são erráticos e imprevisíveis. Contudo, é-nos já hoje possível acompanhar a evolução tecnológica acelerada, bem como antecipar a concretização de alguns abusos antes que uma verdadeira tragédia se abata sobre o nosso país.

Ademais, como temos vindo a transparecer, a utilização criminosa destes mesmos objetos encontra-se praticamente limitada, unicamente, pela imaginação daqueles que intentam subverter o Estado de direito democrático, pelo que é praticamente impossível antecipar toda e qualquer ação que venha a suceder. Contudo, atendendo aos dados apresentados, tememos pela insuficiência legislativa suficiente nesta área, quando quer a ANAC quer o poder legislativo *tout court* português já deviam ter tomado a dianteira no que respeita à criação de legislação inovadora e ousada no âmbito da prevenção e da acção.

6.BIBLIOGRAFIA

- BLUM, ANDREW. ASAL, VICTOR. WILKENFELD, JONATHAN. STEINBRUNER, JOHN. ACKERMAN, GARY. GURR, TED ROBERT. STOHL, MICHAEL. POST, JERROLD M. SINAI, JOSHUA. LAFREE, GARY. DUGAN, LAURA. FRANKE, DERRICK. STANISLAWSKI, BARTOSZ H. SHEFFER, GABRIEL. LICHBACH MARK IRVING. SANDLER, TODD. ENDERS, WALTER. "Nonstate Actors, Terrorism, and Weapons of Mass Destruction." in *International Studies Review 7, no. 1*, 2005, pp. 133-170

- BOLTON, DOUG. Man arrested for landing 'radioactive' drone on Japanese Prime Minister's roof, *The Independent*, 25 de Abril 2015

- CARD, BRYAN A. "Terror from Above: How the Commercial Unmanned Aerial Vehicle Revolution Threatens the US Threshold", in *Air & Space Journal, Spring 2018*, 2018, pp. 80-95

- COELHO, MARIA INÊS. Prisões portugueses estão a ser sobrevoadas por drones, *Pplware*, 05 de Outubro 2016

- CURADO, MIGUEL. Guardas temem drones com droga e telemóveis, *Correio da Manhã*, 14 de Setembro 2018

- DEPARTAMENTO DE COMUNICAÇÃO DA AUTORIDADE NACIONAL DA AVIAÇÃO CIVIL. Comunicado de Imprensa 03/2018 – Esclarecimentos sobre o Decreto-Lei aprovado pelo Governo relativo ao registo e seguro de drones, *ANAC*, 06 de Julho 2018

- FALEIRO, ELEUTÉRIO JOÃO LARANJINHO. *O Uso do Espaço Aéreo Por Aeronaves Não Tripuladas – Unmaned Aerial Vehicles (UAV)*, in *"Estudos de Direito Aéreo"*, 2007, pp. 263-306

- G1 SÃO PAULO. Trio é preso com drone que levaria 18 celulares para presídio em Guarulhos, *G1*, 21 de Agosto 2014

- G4S CORPORATE RISK SERVICES. *Drones: Threat from Above*, 2017

- GEIß, ROBIN. "Asymmetric conflict structures" in *International Review of the Red Cross*, Vol. 88, Number 864, 2006, pp. 757-777

- GOODYEAR, SHEENA. Alleged drone attack like the one in Venezuela was just a matter of time: expert, CBC *Radio*, 07 de Agosto 2018

- GOUVEIA, JORGE BACELAR. "Direito da Segurança: Cidadania, Soberania e Cosmopolitismo", 2018, Almedina

- JORNAL DE NOTÍCIAS. Drone voou ao lado de avião a 1200 metros de altitude em Lisboa, *Jornal de Notícias*, 19 de Junho 2017

- JORNAL I. Drone invade aeroporto de Lisboa, *Jornal I*, 13 de Dezembro 2016

- KALDOR, LEIF. Documentário *"The Age of the Drone"*, 2015

- LEVY, JOSÉ MANUEL. PESSOA, PEDRO. Ninguém pára os drones sobre o aeroporto de Lisboa, *RTP*. 22 de Maio 2015

- LUSA. Testados equipamentos para inibir *drones* em áreas restrinas e proibidas, *Público*, 18 de Janeiro 2018

- LUSA. *Drone* cai na pista do aeroporto de Lisboa, dono constituído arguido, *Público*, 21 de Agosto 2018

- LUSA, AGÊNCIA. Ministro garante segurança da rede de comunicações dos Negócios Estrangeiros, *Observador*, 30 de Agosto 2018

- MARKS, PAUL. Drones turned into zombies using an easy Wi-fi hack, *NewScientist*, 09 de Dezembro 2013

- NATIONAL TRANSPORTATION SAFETY BOARD. *Aircraft Accident Report: Loss of Thrust in Both Engines After Encountering a Flock of Birds and Subsequent Ditching on the Hudson River; US Airways Flight 1549; Airbus A320-214, N106US; Weehawken, New Jersey; January 15, 2009*, 2010

- PANT, ATUL. "Drones: Na Emerging Terror Tool" in *Journal for Defence Studies, Vol. 12, No. 1, January–March 2018*, 2018, pp. 61-75

- RÁDIO RENASCENÇA. Avião evita colisão com "drone" na aproximação ao Aeroporto do Porto, *Rádio Renascença*, 01 de Junho 2017

- REDAÇÃO / CF. Drone entrega droga na prisão, *TVI24*, 05 de Agosto 2015

- SCHMIDT, MICHAEL S. & ERIC SCHMITT. Pentagon Confronts a New Threat From ISIS: Exploding Drones, *The New York Times*, 11 de Outubro 2016

- TADJDEH, YASMIN. ISIS Used A Miniature Surveillance Drone In Its Biggest Syria Victory Yet, *Business Insider*, 28 de Agosto 2014

- THE LAW LIBRARY OF CONGRESS. Regulation of Drones: France, *Library of Congress*, 22 de Julho 2016

- WATERS, NICK. Types of Islamic State Drone Bombs and Where to Find Them, *Bellingcat*, 24 de Maio 2017

- WATSON, BEM. The Drones of Isis, *Defense One*, 12 de Janeiro 2017

- YAKOVLEV, IVAN. 10 de Dezembro 2016

CIBERAMEAÇAS E (IN)SEGURANÇA

LUÍS ELIAS [1]

1 Superintendente da PSP. Diretor do Departamento de Operações. Doutorado em Ciência Política na Faculdade de Ciências Sociais e Humanas. Licenciado em Ciências Policiais pelo Instituto Superior de Ciências Policiais e Segurança Interna. O presente estudo representa o desenvolvimento da comunicação apresentada no Curso de Pós-Graduação sobre Direito do Ciberespaço, organizado pelo Instituto de Ciências Jurídico-Políticas e pelo CIJIC da Faculdade de Direito da Universidade de Lisboa.

RESUMO

Este artigo reflete sobre o uso intensivo de tecnologias de informação e comunicação e impactos sociais, políticos e na segurança.

Aborda os conceitos de ciberespaço, de cibersegurança, de ciberameaças e de cibercriminalidade. Analisa a Estratégia Nacional de Segurança do Ciberespaço. Sublinha a relevância do Gabinete Nacional de Segurança, do Centro Nacional de Cibersegurança, do Centro de Ciberdefesa e da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica.

Os desafios no futuro decorrente da revolução tecnológica em curso serão certamente maiores e trarão problemas difíceis de ultrapassar para a segurança pública, das redes e dos cidadãos.

Palavras-Chave: Tecnologias de Informação, Comunicação, Ciberespaço, Ciberameaças, Cibercriminalidade.

1. INTRODUÇÃO

A sociedade da informação contemporânea é caraterizada pelo uso intensivo de tecnologias de informação e comunicação. Muitas das empresas atuais defendem a prevalência da rede, face à hierarquia formal, como o modo de organização e de obtenção de melhores oportunidades de mercado. Sustentam também o crescente uso do digital e da mediação de tecnologias que constituem a infraestrutura básica das organizações.

Na sociedade em rede, o poder e a falta dele são avaliados em função do acesso a redes e do controlo dos seus fluxos de recursos, informacionais ou financeiros (Castells, 1998). As redes são portas de acesso onde se sucedem oportunidades. Fora das redes, a sobrevivência é cada vez mais difícil. As grandes empresas de tecnologias de Informação como a *Google*, a *Facebook*, o *Baidu* e a *Tencent* poderá incluir a médio prazo na "transferência de autoridade dos seres humanos para os algoritmos" (Harari, 2018: 103-104), o que cria riscos de acumulação de informação e de conhecimento numa muito reduzida percentagem de peritos em termos globais e num reduzido número de Governos, aumentando o perigo do totalitarismo.

O mundo hoje é altamente conectado, opera em ritmo acelerado e em constante mudança. O facto de vivermos em plena revolução tecnológica e de o devir das nossas sociedades ser permanente tem provocado um enorme impacto na forma como as ameaças encaram este novo ambiente e também no modo como os Estados e as respetivas áreas de soberania (segurança interna, defesa, informações, justiça) se adaptam ao mundo cada vez mais reticular e desafiador dos paradigmas. A evolução das tecnologias de informação e comunicações conduziu ao primado de uma cultura mundial, contribuindo para a ocidentalização dos modelos políticos, económicos e sociais, tornando-os globais e universais (Ramonet, 1998). O sistema político atual torna-se assim "planetário, permanente, imediato e imaterial" (Ramonet, 1998: 67).

Nos últimos anos, as fronteiras físicas entre os Estados têm vindo a ser esboroadas pelo caráter transnacional das ameaças e riscos e os Estados, face à crescente desterritorialização da segurança acelerada ainda mais pela rede global, cooperam internacionalmente, trocam e partilham informações, planeiam e executam operações conjuntas, criam redes de peritos, por

forma a prevenirem e combaterem os fenómenos que mais afetam a segurança coletiva. Fernandes considera que "a internet é uma das grandes forças equalizadoras do mundo. Sendo uma das principais forças motrizes da globalização e do progresso das comunicações, ela fornece meios inigualáveis de intercâmbio cultural, informativo e de ideias. Ela criou um nível antes inimaginável de interligação que beneficia o mundo dos negócios, governos e cidadãos. Contudo, da mesma forma que a internet proporciona acesso à mesma informação a pessoas que vivem em circunstâncias totalmente diferentes, atua também como um equalizador entre governos e atores não-estatais" (Fernandes, 2014: 11).

A *internet* e as redes digitais em geral constituem-se como um novo ambiente para a criminalidade organizada, para o recrutamento, para a radicalização, para a subversão e ativismo politico com as mais diversas causas e conotações ideológicas. Verifica-se uma desterritorialização das ameaças e riscos, fazendo do mundo virtual, uma nova dimensão para a expansão das atividades ilícitas e para a ação das Forças e Serviços de Segurança. A internet "enquadra-se perfeitamente na conceção anárquica do sistema internacional, pois o ciberespaço tornou-se um novo campo de batalha internacional" (Fernandes, 2014: 12).

No mundo cibernético, os conceitos técnicos são desenvolvidos e utilizados por peritos num círculo relativamente fechado. Os analistas têm de dominar estes conceitos, tal como o jargão técnico e ser capazes de comunicar ideias complexas e propostas de solução às hierarquias policiais e ao poder político, com vista à tomada de decisão informada e adequada.

Neste sentido, refletiremos sobre as noções de ciberespaço, de cibersegurança, de ciberameaças e, em concreto, de cibercriminalidade, acerca dos desafios que se colocam aos Estados, instituições e sociedade civil para fazer face aos fenómenos decorrentes de um sistema económico-financeiro, sociopolítico, cultural cada vez mais interconectado e gerador de incertezas.

2. CONCEITOS DE CIBERESPAÇO, DE CIBERSEGURANÇA, DE CIBERAMEAÇAS E DE CIBERCRIMINALIDADE

As palavras ciberespaço, cibersegurança, ciberameaças e cibercriminalidade entraram de forma definitiva no léxico quotidiano, no meio académico e nos textos jurídicos, pelo que, sem intenção de apresentar definições incontestáveis e definitivas, propomo-nos contextualizar cada um destes conceitos de forma sumária.

2.1. Ciberespaço

O ciberespaço não encontra um significado ou definição objetiva e universalmente aceite. De acordo com o dicionário Priberam de língua portuguesa, trata-se do "*espaço ou conjunto das comunidades de redes de comunicação entre computadores, nomeadamente a internet*".

Gibson foi dos primeiros autores a utilizar o termo ciberespaço na década de 80 do século XX, numa perspetiva sobretudo romântica, considerando-o "uma alucinação consensual experimentada diariamente por biliões de operadores legítimos, em todas as nações, por crianças a quem são ensinados conceitos de matemática... Uma representação gráfica de dados extraídos dos bancos de dados de cada computador no sistema humano. Complexidade impensável. Linhas de luz no espaço da mente, grupos e constelações de dados" (Gibson, 1984: 22).

Kuehl sustenta que o ciberespaço "*é um domínio operacional que se carateriza pela utilização da eletrónica e do espetro eletromagnético para criar, guardar, modificar trocar e explorar informação através de sistemas baseados em tecnologia de comunicação de informação interligados e as suas infraestruturas associadas*" (Kuehl, 2009: 24-42).

Outra definição de ciberespaço poderá ser "*a rede global de infra- estruturas de tecnologias de informação interligadas entre si, especial- mente as redes de telecomunicações e os sistemas de processamento dos computadores*" (Fernandes, 2012: 55).

O ciberespaço pode ainda ser apresentado como "*um ambiente em si mesmo, onde se deve ter em linha de conta tanto a sua componente tecnológica, isto é, as vulnerabilidades inerentes ao seu emprego e ameaças que possam afetá-lo, como os fatores humanos, uma vez que são estes que caraterizam os utilizadores deste ambiente*" (IDN, 2013: 9-10). Para Natário consiste "*no mundo virtual que os utilizadores da internet visitam quando estão online, acedendo aos mais diversos conteúdos, jogando ou utilizando os variadíssimos serviços interativos que a rede mundial de computadores disponibiliza. (...) Mas é*

fundamental distinguir o ciberespaço da infraestrutura física das redes de comunicação, pois existe uma generalizada confusão concetual. As telecomunicações e a informática, a chamada telemática, limitam-se a permitir a comunicação à distância, enquanto o ciberespaço é um ambiente virtual que se serve destes meios de comunicação para o estabelecimento de relações virtuais" (Natário, 2013).

O ciberespaço é, assim, um ambiente virtual ao nível global utilizado para os mais diversos efeitos: para lazer; para a troca e partilha de conhecimento no meio académico e científico ou técnico; para a realização de negócios; para a difusão de ideias e de conceções políticas, sociais, económicas, culturais; para a comunicação entre pessoas, empresas, instituições e Governos; mas também para a prática de uma vasta panóplia de crimes; para a disseminação de ideologias radicais que questionam e combatem os sistemas políticos, económicos e sociais vigentes; para radicalização e recrutamento para o terrorismo; entre muitas outras práticas que questionam a soberania dos Estados e colocam em risco a segurança das comunidades e dos cidadãos.

Em suma, o ciberespaço está ligado às ideias de:

- globalização, na medida em que a comunicação e o acesso a conteúdos de informação à escala mundial permitiram que pessoas ou grupos de diferentes culturas, origens sociais e económicas, de áreas geográficas diversas, interagissem, se conhecessem e mantivessem contacto permanente *online*, trocando e partilhando informação, fazendo negócios, criando laços de amizade, situação que nunca tinha sido possível até hoje na história da Humanidade;

– criação de um universo virtual paralelo ao mundo físico, ou seja, o surgimento e expansão de uma nova realidade onde se operacionalizam fluxos infinitos de informação, embora a distribuição geográfica dos utilizadores da internet seja muito desigual, em função das disparidades socioeconómicas entre os diversos Estados, do desenvolvimento das infraestruturas, das taxas de penetração tecnológica ou do de nível de educação;

– libertarismo, ou seja, a conceção utópica que considera a internet um espaço que não tem fronteiras, que não está condicionado pelos limites impostos pela soberania e domínio dos governos nacionais e onde os cidadãos têm toda a liberdade de expressar as suas opiniões, contactar entre si e estabelecer relações, concretizando assim a sua emancipação do domínio e regulação dos Estados e das suas instituições. A primeira corrente teórica a tratar do "*controlo*" do ciberespaço tem como expoente Barlow, norte-americano, poeta, escritor e ativista da *internet*. As ideias de Barlow prosperaram nos primórdios da expansão comercial da internet, em 1996 e o sentimento de liberdade era a expressão maior da *web*. A visão era a

de que as leis do mundo real não teriam validade sobre o ciberespaço, pois este seria "*um mundo à parte, mundo esse alheio e indiferente ao direito tradicional*". Esta corrente teórica ganhou impulso maior quando Barlow publicou em 1996 a "*Declaration of independence of cyberspace*" (Declaração de independência do ciberespaço), em contraponto às medidas jurídicas adotadas pelo Governo dos EUA com o "*Communications Decency Act*", continuando ainda a inspirar os *hacktivistas* e as conceções mais contestárias em relação ao estatocentrismo, bem como quanto ao controlo e regulação da rede;

– desenvolvimento e de impacto da tecnologia nas sociedades hodiernas, na medida em que a rede global e a inovação exponencial na área das tecnologias tem transmutado a nossa sociedade, a economia de mercado, as relações sociais, a interação dos Estados com os cidadãos e vice-versa, sendo hoje impensável conceber o mundo sem internet, sem plataformas de comunicação e de disseminação da informação de forma instantânea e imediata.

De acordo com o preâmbulo da Resolução do Conselho de Ministros n.º 36/2015 de 12 de junho que aprovou a Estratégia Nacional de Segurança do Ciberespaço, "*as tecnologias são, no entanto, vulneráveis, criando riscos sociais e materiais*". Se, por um lado, trazem claros benefícios à sociedade, por outro lado, vêm aumentar, de forma significativa, os riscos decorrentes da sua dependência e da quantidade de informação armazenada e em circulação, expondo o Estado, as empresas e os cidadãos. O ciberespaço transpõe a vida real para um mundo virtual, com caraterísticas únicas que impõem novas formas de interação e de relacionamento.

Segundo o *site Internet World Stats* de 2017 a Ásia tem 49,7% dos utilizadores da internet no mundo, a Europa 17%, a América Latina e Caraíbas 10,4%, África 10%, América do Norte 8,2%, Médio Oriente 3,8% e a Oceânia 0,7%.

A taxa de penetração da *internet* na população é a seguinte: América do Norte 88,1%, Europa 80,2%, Oceânia 69,6%, América Latina e Caraíbas 62,4%, Médio Oriente 58,7%, Ásia 46,7% e África 31,2%.

A média da taxa de penetração da *internet* em todo o mundo é de 51,7% (cerca de 3 biliões e 885 milhões de utilizadores em todo o globo). Os seis países com mais utilizadores são: 1.º China, 2.º Índia, 3.º Estados Unidos, 4.º Brasil, 5.º Indonésia e 6.º Japão. Os dois países com mais contas da rede social Facebook são a Índia com 241 milhões e os Estados Unidos com 240 milhões.

2.2. Cibersegurança

A cibersegurança pode ser definida como o sistema e processo de vigilância do ciberespaço para identificar os incidentes, as ameaças e as vulnerabilidades da rede digital assim como para assegurar uma proteção e reação eficiente às atividades das organizações criminosas transnacionais nas suas diversas formas, à radicalização e recrutamento para o terrorismo, ao ativismo político radical e subversivo, as quais procuram destruir os fundamentos do Estado de direito e pôr em causa a segurança das comunidades e dos cidadãos. Segundo Ralo, "*na cibersegurança incluem-se as atividades de monitorização, prevenção e resposta às ameaças que ponham em risco o espaço de liberdade individual/coletiva e de prosperidade que ele constitui e cuja responsabilidade de policiamento deve caber às Forças de Segurança e aos Serviços de Informações. A diferença entre a ciberdefesa e a cibersegurança é, por vezes, muito ténue e, devido à natureza de algumas ameaças, acabam por se sobrepor numa larga percentagem*" (Ralo, 2013).

Conforme previsto na Estratégia da U.E. para a Cibersegurança de 7 de fevereiro de 2013, a cibersegurança refere-se, por norma, às precauções e ações que podem ser utilizadas para proteger o ciberespaço, tanto nos domínios civil como militar, contra as ameaças decorrentes da interdependência das suas redes e infraestruturas informáticas ou que as possam danificar, procurando-se assim manter a disponibilidade e a integridade das redes e infraestruturas e a confidencialidade das informações nelas contidas.

A cibersegurança é hoje uma área essencial para os Estados e para a sociedade civil, tendo em vista prevenir ataques às redes dos setores público e privado, os quais podem colocar em causa a estabilidade coletiva. Na Estratégia Nacional de Segurança do Ciberespaço, podemos encontrar os elementos fundamentais da cibersegurança, como sejam:

- o conhecimento das ameaças e das vulnerabilidades existentes. Este conhecimento é essencial para a realização de análise de risco, com vista a uma melhor aplicação dos meios e recursos disponíveis para o tratamento dos riscos, bem como para a identificação das lacunas a colmatar;

- desenvolver e aplicar medidas que visem a capacitação humana e tecnológica das infraestruturas públicas e das infraestruturas críticas, com vista à prevenção e à reação de e a incidentes de cibersegurança;

- criar mecanismos de reporte de incidentes de cibersegurança para entidades públicas e para os operadores de infraestruturas críticas, com vista à eficácia operacional e a uma melhor avaliação situacional. A desejada avaliação situacional resulta na criação de condições para a

identificação de um nível de alerta nacional em matéria de segurança do ciberespaço, partilhado entre todas as entidades envolvidas;

- em articulação com as autoridades competentes e a comunidade nacional de segurança do ciberespaço, criar uma base de conhecimento que reúna informação sobre ameaças e vulnerabilidades conhecidas, para servir as entidades públicas e os operadores de infraestruturas críticas, produzir e apresentar um quadro integral e atual dos incidentes, ameaças e vulnerabilidades que pendem sobre o ciberespaço nacional.

2.3. Ciberameaças

As ciberameaças são aquelas que exercem a sua atividade e se difundem na rede fruto da utilização massiva das tecnologias de informação, podendo afetar infraestruturas críticas, o equilíbrio funcional da sociedade – sistemas informáticos dos Governos, das empresas, dos cidadãos em geral -, assim como os sistemas políticos e financeiros internacionais.

Podemos salientar como ciberameaças mais relevantes na atualidade as seguintes: o ciberterrorismo, a ciberespionagem, a cibercriminalidade, o *hacking* e o *hacktivismo*.

O ciberterrorismo consiste no uso das tecnologias de informação para difundir propaganda acerca de uma ou de várias organizações terroristas e da sua atividade, para a disseminação de ideologia radical promovendo o terror e o medo e contestando o modelo de sociedade vigente, para o recrutamento de novos membros e para o financiamento de terrorismo. Pode igualmente executar ataques informáticos com grande impacto nos sistemas e redes de computadores e infraestruturas críticas, bem como outras atividades de sabotagem, de pirataria e de utilização dos sistemas informáticos para provocar prejuízos, perturbar, parar ou destruir a atividade de alvos determinados ou indiscriminados.

A ciberespionagem é caraterizada pela exploração de vulnerabilidades encontradas em redes informáticas e em *sites* para ter acesso a informação sensível e classificada. Pode ser perpetrada por Estados, empresas rivais ou indivíduos que procuram adquirir conhecimentos e recolher informações, que lhe podem conceder uma vantagem estratégica e competitiva sobre terceiros ou ainda para benefícios financeiros provenientes da venda de informação subtraída. Atualmente, existem diversos relatórios de informações que referem o recrutamento de *hackers* por parte de serviços de inteligência de potências internacionais, com vista à espionagem em países rivais, nomeadamente em setores estratégicos nas áreas da segurança e defesa, energia, banca, finanças, tecnologia de ponta, farmacêuticas, entre outros.

A cibercriminalidade pode ser definida como toda e qualquer prática criminosa que tenha associada à sua realização, ou como meio, um aspeto cibernético ou a utilização de

computadores. Chawki refere que o cibercrime pode ser entendido "*como qualquer ação ilegal associada com a interligação de sistemas de computadores e redes de telecomunicações, onde a ausência de tal interligação impede a prática ilícita desta ação*" (Chawki, 2006). Numa outra perspetiva, "*crimes informáticos, crimes relacionados com a informática, crimes relacionados com a alta tecnologia e cibercriminalidade partilham o mesmo significado, na medida em que usam redes de informação e de comunicações que não têm quaisquer limitações em termos físicos ou geográficos e decorrem da circulação de dados intangíveis e voláteis*" (Kierkegaard, 2007: 432-433). A cibercriminalidade é caraterizada pela transnacionalidade, anonimato, tecnologia, organização e impacto (Natário, 2013).

O *United Nations Office on Drugs and Crime* (UNODC) classifica os crimes informáticos como crimes dependentes do âmbito cibernético, necessitando de uma infraestrutura tecnológica, sendo caraterizados pela criação, disseminação e difusão de malware, ransomware, ataques a infraestruturas críticas nacionais e inativando um sítio na *internet*, sobrecarregando-o com dados (um ataque *DDoS*); crimes possibilitados pelo ambiente cibernético, os quais podem ocorrer quando os computadores ou outros dispositivos estão desligados da rede ou quando dependentes da infraestrutura tecnológica, incluindo fraudes *online*, tráfico de drogas e branqueamento de capitais; a exploração e o abuso sexual de crianças, fóruns na *darknet* e a extorsão.

A cibercriminalidade não necessita de uma proximidade física entre a vítima e o agressor/criminoso. As restrições territoriais são irrelevantes no ciberespaço, isto é, os cibercrimes são transnacionais, podem ultrapassar as fronteiras de mais de um Estado, não estão confinados por fronteiras nacionais, o que implica que, para um criminoso na rede, seja tão fácil atacar um alvo em territórios longínquos, como vitimar um vizinho.

O anonimato concretiza-se através da utilização da tecnologia pelos criminosos para alcançarem níveis de dissimulação sem paralelo no mundo real, assumindo uma multiplicidade de identidades falsas ou fazendo-se passar por cidadãos inocentes, dificultando assim a tarefa das autoridades.

A tecnologia – *internet*, redes de computadores ou de telecomunicações – é usada como meio ou como fim para o cometimento de crimes. Possibilita aos criminosos utilizarem a automação, usurparem identidades, praticarem fraudes com cartões de crédito e utilizarem esquemas de cifragem para dificultar o trabalho das autoridades, camuflando eficazmente muitas das comunicações criminosas.

As organizações de cibercriminalidade recrutam jovens universitários, engenheiros informáticos e outros peritos em sistemas de informação, procuram como alvo as instituições financeiras, estabelecem alianças com organizações criminosas de tráfico de droga, tráfico de armas, tráfico de seres humanos, ou transformam-se em organizações que exploram a criminalidade sexual, a pedofilia, as burlas e os tráficos de diversa ordem, visando sobretudo o lucro.

A cibercriminalidade incide sobre as pessoas, a propriedade, as organizações e sobre os Estados. Todavia, não é fácil de definir o verdadeiro impacto da cibercriminalidade. A ausência de estatísticas válidas relativas às consequências financeiras causado pela cibercriminalidade e a persistente confusão acerca da tipificação exata destes incidentes são os maiores obstáculos à existência de uma métrica rigorosa que permita avaliar a verdadeira dimensão e intensidade do cibercrime. Alguns dos fatores apontados para as cifras negras ou baixa taxa de denúncia às autoridades policiais e judiciárias dos crimes cibernéticos relacionam-se com a relutância que as organizações e empresas têm em reportar a ocorrência de intrusões nos seus sistemas, o medo do que isso possa trazer à sua imagem pública e à sua posição no mercado concorrencial e mesmo as reticências dos cidadãos em reportarem as fraudes ou outros ilícitos de que são vítimas. Tudo isto contribui para que as estimativas de ocorrências criminais sejam inferiores à realidade.

Deste modo, "*faz sentido que as Forças de Segurança sejam responsáveis por coordenar a resposta do Estado às atividades relacionadas com o cibercrime e o hacktivismo, que os Serviços de Informações da República atuem em casos de ciberespionagem e ciberterrorismo e que as Forças Armadas tenham de intervir para fazer face a ações de ciberguerra*" (Nunes, 2012: 115).

Os termos *hack* e *hacking* referem-se à reconfiguração ou reprogramação de um sistema de função de forma não autorizada pelo proprietário, administrador ou *designer*. Os vocábulos têm vários significados relacionados com a tecnologia e ciência de computação: podem-se referir a uma correção ou melhoria rápida e inteligente de um problema num programa de computador ou podem significar uma solução deficiente (embora relativamente rápida) para um problema informático como um "remendo". Os termos "*hack*" e "*hacking*" são também usados para se referirem a uma modificação de um programa ou dispositivo para dar ao utilizador o acesso a recursos não disponíveis anteriormente, como adaptações de acessibilidade.

É comum o uso da palavra *hacker* fora do contexto eletrónico/computacional, sendo utilizada para definir não somente as pessoas ligadas à informática, mas também os

especialistas que praticam o hacking em diversas áreas. Assim, segundo alguns autores, *hackers* são pessoas que utilizam os seus conhecimentos de forma legal. Criam programas como *Paint.Net, Photoshop, Microsoft Office*. Os *hackers* foram os peritos informáticos que criaram a internet, desenvolveram o sistema operacional *Unix* e o que ele é hoje, mantem a *Usenet*, fazem a *World Wide Web* funcionar e mantêm a cultura de desenvolvimento livre conhecida atualmente.

Existem diversos tipos de *hackers*: os *white hat* (chapéu branco) que utilizam os seus conhecimentos com o principal interesse em segurança, isto é, procuram a exploração e deteção de erros e de conceitos, em cumprimento da lei; os *gray hat* (chapéu cinzento) utilizam os seus conhecimentos de certa forma parecidos com os *white hat*, mas, por vezes, violam as leis; os *black hat* (chapéu preto) são considerados como o "*lado negro*" de um *hacker*, isto é, *hackers* criminosos, que quebram as leis, abusam dos seus limites; os *newbie* (novatos) são pessoas novas na área, que ainda não têm grandes competências, mas podem ter bons conhecimentos; os *lammer* são pessoas arrogantes que pensam que são peritos, no entanto, não têm grandes conhecimentos.

A diferença entre um *hacker* e um *cracker* é basicamente de ordem ideológica. O cracker é uma espécie de *hacker* com disposição para provocar um dano, subtrair informações, invadir um computador, desfigurar a página principal de uma instituição ou até mesmo prestar serviços ao crime organizado. Os grupos de *crackers* são os potenciais sujeitos ativos de inúmeras atividades delituosas que são viabilizadas através da *internet*, daí o risco de cooptação pelo crime organizado (Neto, 2009: 83). Os *crackers* são indivíduos ou grupos que utilizam os seus conhecimentos de forma ilegal, muitas vezes, sem grandes qualificações ou competências em programação e sem ética, criminosos que quebram a segurança de sistemas, agindo ilegalmente e fora da ética *hacker*. A título meramente exemplificativo, criam programas para copiar ilegalmente *software*, criam *cheats* (batota) para copiar palavras-passe, entre outras.

O *hacktivismo* é um termo controverso e de difícil definição, na medida em que engloba diversos tipos de organizações, de ideologias e formas de ação direta digital. Alguns argumentam que esta palavra é usada para descrever como a ação direta eletrónica pode trabalhar para a mudança social através da combinação de conhecimentos de programação de computadores, aliada ao pensamento crítico. Outros autores usam este vocábulo como sinónimo de um ato ou estratégia maliciosa e atos destrutivos que comprometem a segurança dos computadores na *internet*.

O *hacktivismo* é a ação conduzida por indivíduos ou grupos que utilizam meios informáticos e veem a internet como um veículo para promover e catalisar as suas causas e disseminar a sua mensagem. A ideologia defendida pode ter motivações distintas, desde políticas a religiosas, mas o objetivo final é comum: chamar a atenção da opinião pública para determinado assunto.

O desenvolvimento da tecnologia levou os grupos que formam a sociedade a adaptarem-se a uma nova maneira de divulgar, protestar e aliar-se. Segundo Mathews (1997: 51-52), a revolução das telecomunicações, com o advento da internet, trouxe uma tecnologia barata e de fácil acesso que ajudou a colocar em crise o monopólio da informação, que estava nas mãos dos Governos, além de facilitar a interação por deixar o espaço aberto para a expressão das pessoas na rede, já́ que a democracia e a descentralização são colocadas em lugar de destaque, enquanto a hierarquia e a burocracia são desvalorizadas. O que começou com o uso de *e-mails*, desenvolveu-se para a divulgação através de sites, com a simplificação do processo de postagem de mensagens e montagem de paginas na *internet*, e chegou às redes sociais e *sites* onde é possível alcançar um número quase infinito de indivíduos através da partilha de mensagens que podem ser divulgadas por conhecidos e desconhecidos, bastando apenas haver alguma ligação, seja por participar do mesmo grupo de interesses, seja por haver algum nível de amizade (Furtado, 2013: 19).

De acordo com alguns autores, o *Twitter* merece um lugar de destaque nas redes sociais, "*amplificado pela utilização de telemóveis, aumentando significativamente a influência dos 'movimentos politicamente motivados' em dois aspetos: exploração da democratização de acesso à internet, já́ que não é preciso ter um site para divulgar os seus ideais, muito menos dominar a tecnologia para fazê-lo e ainda pela velocidade de atualização dos posts ou mensagens (...). Hoje, com o Twitter, numa questão de segundos é possível postar uma mensagem que poderá́ ser lida por milhões de pessoas (...) O acesso às redes sociais, a capilaridade (alcance global e local dessa rede e a velocidade com que é possível trocar mensagens nessas plataformas digitais, tornam-nas muito eficientes e atraentes para o ciberativismo*" (Utsonomiya & Reis, 2011: 7),

O *hacktivismo* pode assumir assim diversas facetas. Uma faceta tecno-libertária assente na ideia de que a "*internet* pode contribuir para criar uma nova era de 'transparência' na política (...). Parece ter sido essa a convicção/missão de Julian Assange, o carismático fundador do *site Wikileaks*" (Fernandes, 2014: 57) e ainda uma faceta corporizada pelos "radicais anticapitalistas, a comunidade de ativistas do ambiente, dos direitos humanos e dos revolucionários políticos, designados nos anos 60, como contracultura" (Leigh & Harding,

2011: 56). Os grupos *hacktivistas Anonymous* e os *LulzSec*, por exemplo, contestam o que "percecionam como um abuso de poder dos governos e das empresas, defendendo a necessidade de promover a transparência na política e nos negócios" (Benkler, 2012).

O *hacktivismo* engloba diversos grupos e organizações que defendem os direitos humanos, a transparência política, a descentralização da informação, a cultura de partilha, o livre acesso à informação, a liberdade de expressão, o uso e desenvolvimento de programas e sistemas em código aberto e licenças livres. Por vezes, algumas organizações *hacktivistas* aproximam-se do ciberterrorismo ou da cibercriminalidade, na medida em que causam danos nos sistemas informáticos e equipamentos, espalham vírus e penetram em redes de instituições e empresas, com o objetivo de sub- trair informação classificada e dados pessoais, bem como difundem ideias contestando o nosso modelo de sociedade e fazendo, em alguns casos, a apologia de alteração do seu sistema social e político através da ação direta. As principais missões das organizações hacktivistas consistem na criação de *sites* ou sistemas com objetivos políticos, no desenvolvimento de programas em código aberto, no espelhamento de *sites*, na subtração de documentos dos Governos ou de instituições públicas e privadas, na difusão da cultura *hacker* e da ação direta digital. Desenvolvem também técnicas mais avançadas como *spoofing*, *email-bombing* e uso de *DoS*.

Por isso, a narrativa e evocação de princípios como a liberdade de expressão, o livre acesso a informação, a privacidade individual e a transparência política, confundem-se com práticas tipificadas como crimes pela lei penal, nem sempre sendo fácil distinguir quais os verdadeiros propósitos de algumas organizações ou indivíduos que se autodesignam hacktivistas, constituindo-se como ameaças transnacionais com um potencial avassalador de desestabilização da economia global e da segurança internacional.

3. ESTRATÉGIA NACIONAL DE SEGURANÇA DO CIBERESPAÇO

Portugal tem uma Estratégia Nacional de Segurança do Ciberespaço desde 2015 (Resolução do Conselho de Ministros n.º 36/2015 de 12 de junho), sendo previsível que leve alguns anos a ser concretizada em toda a sua plenitude. A Estratégia assenta sobre os princípios gerais da soberania do Estado, das linhas gerais da Estratégia da U.E. para a Cibersegurança e na estrita observância da Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa, da Carta dos Direitos Fundamentais da União Europeia, da proteção dos direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade, e alicerça-se em cinco pilares: subsidiariedade, complementaridade, cooperação, proporcionalidade e sensibilização.

A Estratégia desenvolve-se de acordo com vários objetivos: promover uma utilização consciente, livre, segura e eficiente do ciberespaço; proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos; fortalecer e garantir a segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais; afirmar o ciberespaço como um domínio de desenvolvimento económico e de inovação. Define ainda seis eixos de intervenção, enformados em medidas concretas e respetivas linhas de ação, destinadas a reforçar o potencial estratégico nacional no ciberespaço.

O Eixo 1 (Estrutura de segurança do ciberespaço) é consubstanciado através do estabelecimento da coordenação político-estratégica para a segurança e defesa do ciberespaço; da consolidação do papel de coordenação operacional e de autoridade nacional em matéria de cibersegurança, relativamente às entidades públicas e às infraestruturas críticas, do CNCSeg; do desenvolvimento da capacidade de ciberdefesa; do desenvolvimento da capacidade nacional de resposta a incidentes; do estabelecimento de um gabinete para gestão de crises no ciberespaço; da definição e implementação de processos de governação da segurança do ciberespaço.

O Eixo 2 (Combate ao Cibercrime) é concretizado através da revisão e atualização da legislação; da agilização das capacidades da Polícia Judiciária.

O Eixo 3 (Proteção do ciberespaço e das infraestruturas) é efetuado através da avaliação da maturidade e a capacidade das entidades públicas e privadas que administrem infraestruturas críticas ou serviços vitais de informação; da adaptação e melhoria contínua da segurança dos sistemas de informação das entidades públicas, dos operadores das infraestruturas críticas e dos serviços vitais de informação, para assegurar uma maior

resiliência (capacidade de sobrevivência) nacional, adaptando-os aos novos riscos e ameaças do ciberespaço; da análise ao ambiente de informação, para tentar antecipar eventuais ataques e tomar as decisões apropriadas, acompanhando os últimos desenvolvimentos tecnológicos e analisando e antecipando ameaças; da aplicação, por parte das entidades públicas, das medidas necessárias à continuidade das operações, de modo a responder às principais crises que afetem ou ameacem a segurança dos sistemas de informação ou os operadores de infraestruturas críticas; do desenvolvimento da capacidade de deteção de ataques aos sistemas de informação; da promoção da aplicação, por parte das entidades públicas, das medidas necessárias à continuidade das operações, de modo a responder às principais crises que afetem ou ameacem a segurança dos sistemas de informação ou os operadores de infraestruturas críticas; da inclusão de medidas de segurança do ciberespaço nos planos de proteção de infraestruturas críticas nacionais.

O Eixo 4 (Educação, sensibilização e prevenção) concretiza-se através da consciencialização não só das entidades públicas e das infraestruturas críticas, mas também das empresas e da sociedade civil. Por sua vez, é fundamental que o país se dote de recursos humanos qualificados para lidar com os complexos desafios da segurança do ciberespaço.

O Eixo 5 (Investigação e desenvolvimento) tem em vista apoiar, fomentar e potenciar as capacidades tecnológicas, para que sejam desenvolvidas soluções nacionais, seguras e confiáveis, que possam ser certificadas, permitindo assim potenciar a proteção dos sistemas perante as diversidades das ameaças.

O Eixo 6 (Cooperação) concretiza-se através da segurança e defesa do ciberespaço requer uma forte cooperação e colaboração entre aliados e parceiros, nacionais ou internacionais. Requer uma abordagem em rede, pelo que a cooperação nacional e internacional nos diversos domínios de atuação é da maior importância.

De salientar o Conselho Superior de Segurança do Ciberespaço criado através da RCM n.º 115/2017 de 24 de agosto que tem por missão assegurar a coordenação político-estratégica para a segurança do ciberespaço e o controlo da execução da Estratégia Nacional de Segurança do Ciberespaço (ENSC) e da respetiva revisão. É presidido pelo Primeiro-ministro ou pelo Ministério em quem ele delegar, sendo composta pela Autoridade Nacional de Segurança, SG/SSI, SG/SIRP, Coordenador do Centro Nacional de Cibersegurança, DG. da Autoridade Tributária e Aduaneira, Ministério Público, Diretor da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica da Polícia Judiciária, Diretor Geral da Educação, entre outros.

4. GABINETE NACIONAL DE SEGURANÇA

De acordo com o artigo 1.º n.º 1 do Decreto-Lei n.º 3/2012 de 16 de janeiro, o Gabinete Nacional de Segurança é um serviço central da administração do Estado, dotado de autonomia administrativa, na dependência do Primeiro-Ministro ou do membro do Governo em quem aquele delegar. O n.º 2 do mesmo artigo estipula que a Autoridade Nacional de Segurança, dirige o GNS e é a entidade que exerce, em exclusivo, a proteção e a salvaguarda da informação classificada.

O artigo 2.º n.º 1 do mesmo diploma refere que o GNS tem por missão garantir a segurança da informação classificada no âmbito nacional e das organizações internacionais de que Portugal é parte e exerce a função de autoridade de credenciação de pessoas e empresas para o acesso e manuseamento de informação classificada, bem como a de autoridade credenciadora e de fiscalização de entidades que atuem no âmbito do Sistema de Certificação Eletrónica do Estado – Infraestrutura de Chaves Públicas (SCEE).

É de referir ainda a Resolução do Conselho de Ministros n.º 5/90 de 28 de fevereiro que contém as normas para a segurança nacional, salvaguarda e defesa de matérias classificadas. Constitui um documento relevante e ainda em vigor, mas já algo desfasado face à evolução avassaladora das redes e sistemas de informação. Por exemplo, o glossário de termos de informações e segurança nacional em anexo à resolução já não responde às necessidades, por se encontrar desatualizado.

Aborda, no entanto, questões muito relevantes que apenas precisarão de alguma atualização em termos de nomenclatura e de contextualização, como sejam o estudo da ameaça e as medidas de segurança; a credenciação dos centros de informática do Estado, dos privados e do seu pessoal; a segurança física de instalações; a segurança de suportes físicos; a segurança lógica; a classificação, preparação e segurança de dados e programas classificados; a reprodução, transferência, controlo de segurança e destruição de dados e programas classificados.

A Resolução do Conselho de Ministros n.º 12/2012 atribui ao Gabinete Nacional de Segurança, no âmbito da medida 4 do plano global estratégico de racionalização e redução de custos com as Tecnologias da Informação e Comunicação, a missão de coordenação com as entidades relevantes da definição e implementação de uma Estratégia Nacional de Segurança da Informação, que compreende, entre outras medidas.

5. CENTRO NACIONAL DE CIBERSEGURANÇA

A Comissão Instaladora do Centro Nacional de Cibersegurança (CNCSeg), no cumprimento do mandato que lhe foi atribuído pela Resolução do Conselho de Ministros no 42/2012, aprovou no mês de julho de 2012 um relatório com uma proposta para a criação de um Centro Nacional de Cibersegurança com a missão contribuir para que Portugal use o ciberespaço de uma forma mais livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional.

Com a segunda alteração ao Decreto-Lei n.º 3/2012, efetuada pelo Decreto-Lei n.o 69/2014 de 9 de maio, foi formalmente atribuída a responsabilidade ao GNS pelo Centro Nacional de Cibersegurança. Nos termos do artigo 2.º A do Decreto-Lei n.o 3/2012 de 16 de janeiro , as competências do CNCSeg são as seguintes:

- desenvolver as capacidades nacionais de prevenção, monitorização, deteção, reação, análise e correção destinadas a fazer face a incidentes de cibersegurança e ciberataques;
- promover a formação e a qualificação de recursos humanos na área da cibersegurança, com vista à formação de uma comunidade de conhecimento e de uma cultura nacional de cibersegurança;
- exercer os poderes de autoridade nacional competente em maté- ria de cibersegurança, relativamente ao Estado e aos operadores de infraestruturas críticas nacionais;
- contribuir para assegurar a segurança dos sistemas de informação e comunicação do Estado e das infraestruturas críticas nacionais;
- promover e assegurar a articulação e a cooperação entre os vários intervenientes e responsáveis nacionais na área da cibersegurança;
- assegurar a produção de referenciais normativos em matéria de cibersegurança;
- apoiar o desenvolvimento das capacidades técnicas, científicas e industriais, promovendo projetos de inovação e desenvolvimento na área da cibersegurança;
- assegurar o planeamento da utilização do ciberespaço em situação de crise e de guerra no âmbito do planeamento civil de emergência, no quadro definido pelo Decreto-Lei n.º 73/2013, de 31 de maio;
- coordenar a cooperação internacional em matérias da cibersegurança, em articulação com o Ministério dos Negócios Estrangeiros.

O artigo 2.º n.º 2 do mesmo diploma estipula que o CNCSeg que tem por missão contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais.

6. CENTRO DE CIBERDEFESA

Na sequência da Declaração de Praga de 21 de novembro de 2002, os Estados-membros da OTAN tomaram a decisão de reforçar as capacidades de defesa contra cibercrimes e ciberataques, criando e treinando equipas de resposta a eventos ocorridos no espaço cibernético, estabelecendo Capacidades de Resposta a Incidentes de Segurança Informática (CRISIs). Como órgão de coordenação das CRISIs dos diferentes ramos das Forças Armadas temos a Direção de Comunicações e Sistemas de Informação (DIRCSI), sob a alçada do Estado-Maior-General das Forças Armadas (EMGFA) criado pelo Decreto-Lei n.º 184/2014 de 29 de dezembro de 2014, com a missão de "*planear, estudar, dirigir, coordenar e executar as atividades inerentes aos sistemas de informação (SI) e tecnologias de informação e comunicação (TIC) necessários ao exercício do comando e controlo nas Forças Armadas*". O mesmo documento define ainda que no que concerne à ciberdefesa a DIRCSI contempla a missão de "*coordenar a proteção dos valores da integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação das Forças Armadas. Conforme preceituado no artigo 30.o, ponto 6 alínea d) do Decreto-Lei no184/2014 de 29 de dezembro de 2014, compete ao DIRCSI "assegurar a coordenação e o trabalho colaborativo e integrado com os Núcleos Computer Incident Response Capability (CIRC) dos ramos das Forças Armadas e do EMGFA*".

O Centro de Ciberdefesa foi criado pelo Despacho n.º 13692/2013, de 11 de outubro de 2013 do Ministro da Defesa Nacional. Constitui o órgão, na dependência do CEMGFA, responsável pela condução de operações no ciberespaço e pela resposta a incidentes informáticos e ciberataques, com responsabilidades de coordenação, operacionais e técnicas.

Considera-se, porém, relevante "distinguir a esfera de atuação da DIRCSI e da rede de ciberdefesa do CNCS e da rede CSIRT nacional, que apresentam linhas de ação semelhantes, mas com objetivos distintos, tendo sido atribuída ao CNCS a missão de manutenção da cibersegurança a nível nacional, estando incumbido da proteção de entidades do Estado e infraestruturas críticas, em questões relacionadas com eventos no ciberespaço. Por outro lado, a DIRCSI e as várias CRISIs dos diferentes ramos das Forças Armadas asseguram a proteção do Estado num cenário de ciberguerra, prevenindo e estando pronto a responder a qualquer ciberataque que lhes seja dirigido" (Goncalves, 2016: 76).

7. UNIDADE NACIONAL DE COMBATE AO CIBERCRIME E À CRIMINALIDADE TECNOLÓGICA

Nos termos da alínea l), do n.º 3, do artigo 7.º da Lei da Organização de Investigação Criminal (LOIC) (Lei n.o 49/2008 de 27 de agosto) constitui competência reservada da Polícia Judiciária a investigação dos crimes informáticos e praticados com recurso a tecnologia informática, sem prejuízo da possibilidade de competência deferida a outro órgão de polícia criminal nos termos do seu artigo 8º.

Salienta-se que o Decreto-Lei n.o 81/2016, de 28 de novembro criou a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) no seio da Polícia Judiciária, segundo consta do preâmbulo, "à semelhança da congénere da EUROPOL – EC3", substituindo a Unidade Nacional da Investigação da Criminalidade Informática, a qual foi extinta, alterando assim o Decreto-Lei n.o 42/2009 de 12 de fevereiro que estabelece as competências das unidades da Polícia Judiciária.

Neste diploma são definidas como atribuições da UNC3T as seguintes:

- prevenção, deteção, investigação criminal e coadjuvação das autoridades judiciárias relativamente aos crimes previstos na Lei n.o 109/2009, de 15 de setembro;

- prevenção, deteção, investigação criminal e coadjuvação das autoridades judiciárias quanto aos crimes praticados com recurso ou por meio de tecnologias ou de meios informáticos, previstos, designadamente:

i) na Lei de Proteção dos Dados Pessoais; ii) no Código dos Direitos de Autor e Direitos Conexos, incluindo a interferência e o desbloqueio de formas de proteção tecnológica de bens e de serviços;

- prevenção, deteção, investigação criminal e coadjuvação das autoridades judiciárias quanto aos crimes:

i) contra a liberdade e autodeterminação sexual, sempre que praticados por meio ou através de sistema informático; ii) de devassa por meio da informática; iii) de burla informática e nas comunicações; iv) relativos à interferência e manipulação ilegítima de meios de pagamento eletrónicos e virtuais; v) de espionagem, quando cometido na forma de um qualquer programa informático concebido para executar ações nocivas que constituam uma ameaça avançada e permanente.

A UNC3T assegura, no âmbito da cooperação internacional, o ponto de contacto operacional permanente e colabora e apoia de forma direta as ações de prevenção, deteção e

mitigação desenvolvidas pelas entidades nacionais com competências definidas por lei para a segurança nacional do ciberespaço. Cabe ainda à UNC3T:

- assegurar o regular funcionamento de um grupo consultivo informal para debate e aconselhamento estratégico, formativo, jurídico, técnico e científico de questões relacionadas com o cibercrime, com a criminalidade tecnológica e a cibersegurança;

- assegurar a colaboração e participação direta na formação inicial e contínua sobre cibercrime aos quadros do pessoal de investigação criminal e de apoio da Polícia Judiciária, designadamente, nas áreas da segurança da informação e da cibersegurança.

Na UNC3T e sob a dependência da sua direção é criada uma equipa técnica e de investigação digital com as seguintes funções:

- otimizar e gerir as infraestruturas e meios tecnológicos atribuídos à Unidade;

- apoiar e assessorar nos planos técnico, tecnológico e jurídico, o pessoal de investigação criminal nas suas investigações;

- testar e desenvolver ferramentas específicas para a investigação do cibercrime, da criminalidade tecnológica e da decifragem de dados;

- recolher, tratar e difundir dados relativos a ciber-intelligence para apoio às investigações, à cooperação policial internacional e à prevenção de atos de cibercrime;

- desenvolver ações de contrainformação criminal;

- dar apoio em ações de caráter técnico para recolha de prova digital, nomeadamente, ações encobertas e interceção de dados;

- apoiar investigações que exijam conhecimentos técnicos especializados, nomeadamente, redes de anonimização, mercados virtuais, moedas virtuais, análise de programas maliciosos.

A criação desta unidade especializada na PJ está em linha com as diretivas e recomendações da U.E. e permitirá, certamente, melhorar a eficácia da investigação de organizações criminosas e de indivíduos que se dedicam a diversas práticas delituosas na rede, diminuir o impacto económico da cibercriminalidade e incrementar a segurança nas redes e sistemas de informação.

8. LEI DO CIBERCRIME

No artigo 2.º da Lei n.º 109/2009, de 15 de setembro, que aprova a Lei do Cibercrime, transpondo 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 e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa, encontramos algumas definições úteis para caraterizar a complexidade do ciberespaço.

Assim, «sistema informático» é qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção.

Os «dados informáticos» são qualquer representação de factos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função.

Os «dados de trafego» são os dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.

O «fornecedor de serviço» é qualquer entidade, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, bem como qualquer outra entidade que trate ou armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviço ou dos respetivos utilizadores.

«Interceção» consiste no ato destinado a captar informações contidas num sistema informático, através de dispositivos eletromagnéticos, acústicos, mecânicos ou outros.

A «topografia» trata-se uma serie de imagens ligadas entre si, independentemente do modo como são fixadas ou codificadas, que representam a configuração tridimensional das camadas que compõem um produto semicondutor e na qual cada imagem reproduz o desenho, ou parte dele, de uma superfície do produto semicondutor, independente- mente da fase do respetivo fabrico.

O «produto semicondutor» é a forma final ou intermedia de qualquer produto, composto por um substrato que inclua uma camada de material semicondutor e constituído por uma ou várias camadas de matérias condutoras, isolantes ou semicondutoras, segundo uma disposição

conforme a uma configuração tridimensional e destinada a cumprir, exclusivamente ou não, uma função electrónica.

Existem diversas tipologias e modi operandi para cometer crimes cibernéticos, podendo uma rede ou sistema ser o meio do ataque ou o alvo do mesmo. Em Portugal, a já referida Lei do Cibercrime, tipifica uma série de ilícitos criminais que se enquadram na definição de cibercriminalidade: a falsidade informática (artigo 3.º), o dano relativo a programas ou outros dados informáticos (artigo 4.º), a sabotagem informática (artigo 5.º), o acesso ilegítimo (artigo 6.º), a interceção ilegítima (artigo 7.º), a reprodução ilegítima de programa protegido (artigo 8.º). Esta tipificação de ilícitos criminais poderá ter que ser revista no futuro, em função da evolução contínua da cibercriminalidade.

Os crimes relativos a pornografia infantil, referenciados na Convenção sobre o Cibercrime, não são contemplados neste diploma visto que se encontram legislados pelo Código Penal Português na alínea c) do artigo 176º, Pornografia de menores, introduzido após a alteração imposta pela Lei nº 59/2007 de 4 de Setembro de 2007, que afirma que quem "*produzir, distribuir, importar, exportar, divulgar, exibir ou ceder, a qualquer título ou por qualquer meio*", fotografias, filmes ou gravações pornográficas é punido com pena de prisão de 1 a 5 anos.

9. TENDÊNCIAS DAS CIBERAMEAÇAS E DA CIBERCRIMINALIDADE

Para a classificação de incidentes de segurança, o CNCS utiliza a taxonomia da Rede Nacional de CSIRTs que estabelece a classe dos incidentes e os tipos de incidentes. Neste sentido, o 'código malicioso' pode resultar em infeção, distribuição, C & C ou outro. Para a classe de incidente 'disponibilidade', podem surgir incidentes como DoS/DDoS e sabotagem. A 'recolha de informação' pode resultar de incidentes como *scan*, *sniffing* e *phishing*. A 'tentativa de intrusão' é causada por exploração de vulnerabilidades e tentativas de *login*. A 'intrusão' resulta da exploração das vulnerabilidades e de compromissos de conta. A 'segurança da informação' está relacionada com incidentes como acesso não autorizado e modificação/remoção não autorizada. A 'fraude' resulta de incidentes como utilização indevida ou não autorizada de recursos e da utilização ilegítima de nome de terceiros. O conteúdo abusivo consubstancia-se em incidentes como *SPAM*, direitos de autor, pornografia infantil, racismo e apologia da violência.

A motivação de base para a maior parte dos cibercrimes em Portugal continua a ser económica (extorsão, *phishing*, fraude) e *hacktivista* (*anonymous* e movimentos semelhantes), sendo que alguns dos principais atores criminais continuam ligados a fraude com cartões de crédito (*carding*). Das investigações em curso parece resultar um aumento significativo dos expedientes que tiram partido de produtos e serviços bancários, como é o caso dos cartões virtuais, também designados de "pré-pagos". Os crimes de extorsão (*ransomware*) registam uma tendência crescente. Em Portugal, não foram detetadas até hoje ocorrências com recurso ao modus operandi designado por "*APT*" (*Advanced Persistent Threat*). A partir dos casos acompanhados, indica-se um crescimento dos danos provocados da atividade de *phishing* com recurso a meios virtuais (incluindo empresas internacionais) e a estabilização do uso de moedas virtuais (*bitcoins* e outras).

Os dados pessoais poderão constituir um alvo crescente dos grupos criminosos. Cabreiro da UN3CT da Polícia Judiciária considera que o crime informático está em permanente mutação, por exemplo, neste momento está a alterar plataformas, passando dos computadores pessoais, para os *iPads* e *smartphones*, com capacidade de recolha de fotos e vídeo. Segundo Cabreiro, "*a generalização da internet torna difícil encontrar um perfil do autor e da vítima de crime informático*". Acrescenta que se pode encontrar "*um escalão etário mais vulnerável devido às tecnologias não fazerem parte da sua rotina*". As crianças utilizadoras de novas tecnologias podem ser vítimas de pornografia infantil e de abuso sexual *online*. Existe um

mercado de produção e distribuição de filmes, encontrando-se Portugal também na rota de circulação e residualmente de produção destes vídeos.

A utilização das plataformas de transmissão de vídeos – por exemplo, o *Facebook Live* ou o *Periscope* do *Twitter*, entre outras – para fins ilícitos, tem tido um grande crescimento em termos internacionais, nomeadamente por predadores sexuais, exibicionistas, *voyeurs* e outro tipo de agressores que assediam menores e vítimas com perfis muito diversificados, transmitem mensagens de ódio, de incitamento à violência, ao suicídio, por exemplo. A empresa *Facebook* refere estar a procurar melhorar a resposta tecnológica para reagir mais eficazmente às denúncias e a recrutar mais pessoal para as equipas que analisam as queixas e monitorizam os vídeos em direto, por compreender a enorme sensibilidade em termos de direitos individuais que decorre da exibição de imagens em tempo real. Quando um vídeo ou um *post* tem várias denúncias, o algoritmo vai alertar os moderadores. A tecnologia pode ser melhorada, admite o *Facebook*, que depende muito da combinação entre inteligência artificial, moderadores humanos e alertas dos utilizadores para monitorizar toda a rede.

No relatório da EUROPOL designado Internet Organised Crime Threat Assessment (IOCTA) de 2017 as infraestruturas críticas encontram-se na atualidade com um grau extremamente elevado de informatização e de automação, sendo, por isso, alvos potenciais de ataques cibernéticos os diversos setores prioritários e respetivas infraestruturas: energia (eletricidade, combustível, gás), transportes (aéreos, ferroviários, marítimos, terrestres), bancos, mercados financeiros, saúde (hospitais públicos e privados), redes de distribuição de água e infraestruturas digitais. Quanto aos tipos de serviços digitais igualmente cobiçados pelos piratas informáticos, salientam-se os mercados *online*, os motores de busca online e os serviços de armazenagem (*cloud*).

No que concerne à criminalidade cibernética, de referir ainda como principais tendências na U.E. as seguintes:

– o *ransomware* é, ao nível global, a ameaça mais proeminente em termos de diversidade das vítimas e da dimensão dos danos provocados. O número de ataques *DDoS* de larga escala tem tendência a agravar-se, sendo originado pela expansão de aparelhos inseguros de uso doméstico e comercial (*internet of things – IoT*). A segurança ineficaz da internet em muitas empresas, instituições e nas residências particulares, resulta no acesso ilegal, na exfiltração e na substração de dados ou informação; as burlas ou fraudes com cartões de crédito estão também em expansão, afetando em particular as companhias aéreas e a indústria hoteleira e facilitando operações de tráfico de seres humanos, de tráfico de droga e de imigração ilegal. Os ataques às redes bancárias, com vista a manipularem os movimentos das contas, a

controlarem as caixas *ATM* ou a transferirem fundos diretamente, representam uma das ameaças emergentes;

- a exploração e coação sexual de crianças na internet continua a expandir-se, quer visando o acesso físico às vítimas, quer a gravação de conteúdos sexuais em vídeo ou fotogramas. A partilha destes conteúdos é efetuada através de redes de ponto a ponto, das redes sociais ou em comunidades de predadores e agressores sexuais alojados na darknet.

- Os mercados criminais *online* utilizam sobretudo a *darknet*, permitindo-lhes uma interconexão com uma vasta quantidade de redes de criminalidade organizada, garantindo o acesso a dados de contas pessoais, documentos falsos, formas fraudulentas de pagamento. Um número sem precedentes de cibernautas utiliza o *TOR* e outros programas similares para navegarem de forma anónima e para o comércio ilegal de estupefacientes, armas e conteúdos relacionados com o abuso sexual de crianças.

A convergência da cibercriminalidade e do terrorismo é outra das tendências hodiernas. Os terroristas continuam a usar sobretudo a internet e as aplicações de comunicação *online* (exemplo: *Whatsapp* e *Telegram*) para a coordenação de ações violentas, propaganda e troca de conhecimentos. A capacidade dos grupos terroristas para lançarem ciberataques, segundo a EUROPOL, aparenta ser ainda limitada. A atividade das organizações terroristas tem sido centrada na internet livre, mas a darknet começa a ser cada vez mais utilizada pelos terroristas para campanhas de angariação de fundos, para o uso de mercados ilegais e para a difusão de ações de propaganda desencadeadas nas redes sociais *mainstream*.

Segundo Klimburg, "*cibercrime, ciberterrorismo e ciber-guerra partilham uma base tecnológica comum, ferramentas, logística e instrumentos. Podem também partilhar as mesmas redes sociais e ter objetivos similares. As diferenças entre estas duas categorias de ciba atividades são frequentemente ténues (...). Na perspetiva de um ciberguerreiro, o cibercrime pode oferecer uma base técnica (ferramentas de software e apoio logístico) e o ciberterrorismo a base social (redes pessoais e motivação) com as quais podem ser executados ataques às redes de computadores de grupos inimigos ou nações*" (Klimburg, 2011: 41).

Os *modi operandi* utilizados pelos piratas informáticos apontam para a transversalidade e transdisciplinaridade dos crimes. A utilização de técnicas de engenharia social é apontada pela EUROPOL como uma tática para o cometimento de crimes informáticos, na medida em que permite a análise do perfil, hábitos, rotinas, locais de residência e de lazer, familiares e amigos, das potenciais vítimas, aumentando as possibilidades de concretização da ação criminosa e respetivo impacto.

O *Bitcoin* continua a ser um facilitador-chave para a cibercriminalidade, aparecendo, entretanto, outras criptomoedas que começam a ganhar popularidade no submundo digital, como a *Monero*, *Ethereum* e a *Zcash*. A facilidade em abrir contas bancárias em alguns países, em particular contas *online*, está a incrementar o branqueamento de capitais.

Os fóruns criminais e as plataformas digitais de comunicação têm-se consolidado como um ambiente ideal para os criminosos cibernéticos, disponibilizando locais de encontro, mercados e acesso a competências e perícia de outros membros da comunidade de cibercriminalidade transnacional.

A utilização de aplicações seguras por criminosos – normalmente de livre acesso e populares entre os cidadãos em geral -, nos mais diversos mercados ilícitos (tráficos, criminalidade violenta, criminalidade financeira, terrorismo, extremismo político-social), proporciona a rapidez e imediatismo dos fluxos de informação, a camuflagem da identidade, a transferência de grandes quantidades de dados e maiores oportunidades de negócio.

Finalmente, segundo a EUROPOL, uma combinação de fatores de ordem legal e técnica, negam aos órgãos de polícia criminal, o acesso, de forma atempada, às comunicações eletrónicas suspeitas e a possibilidade de execução de perícias forenses. Em muitos casos, as dificuldades colocadas pelos sistemas de encriptação e de retenção de dados, reduzem a possibilidade de prossecução das investigações e a recolha da prova digital de forma célere, eficaz e eficiente.

10. CONCLUSÕES

As infraestruturas de informação e o ciberespaço "*são indispensáveis na nossa sociedade, e o seu correto funcionamento assume importância crucial para a livre circulação da informação e dos processos e serviços dependentes desse fluxo*" (Nunes, 2010: 1194).

A cibersegurança foi integrada nas estruturas securitárias preexistentes (nas Forças Armadas, nas Forças e Serviços de Segurança e Autoridades Judiciárias) em muitos países ocidentais, tendo potenciado a adoção de Estratégias Nacionais e ainda a criação de Centros Nacionais para a deteção de ameaças cibernéticas, para apoiarem operações de investigação criminal. Em alguns países, verifica-se o controlo por parte do Estado de redes organizadas de *hackers* que atuam em nome do regime (caso da China) ou numa lógica de *outsourcing* destes peritos para desenvolverem ações de ataque e defesa (Rússia).

A cibersegurança salienta o esbatimento entre o público e o privado. O setor privado está no centro da cibersegurança mundial, sendo proprietário de grande parte das infraestruturas críticas a nível global e parceiro indispensável de Estados e outros atores (incluindo a U.E. e a ONU) no combate às ciberameaças.

A cibersegurança está ainda relacionada com a dificuldade de atribuição de responsabilidades pelos ataques informáticos. Permite a existência de relações internacionais de forma anónima, escondidas do espaço público e sem conhecimento dos resultados, o que é preocupante numa perspetiva de responsabilização política nacional e internacional. O ciberespaço levanta a questão do conceito de poder nas relações internacionais. Não se trata de uma nova forma de poder, nem desafia ainda a integridade da soberania nacional, mas sim de uma certa difusão do poder por novos atores e entidades, o que há pouco tempo era limitado aos governos dos principais Estados do sistema internacional (Barrinha & Carrapiço, 2016: 256-257).

As ciberameaças e a cibercriminalidade em concreto, estão cada vez mais organizadas e transvazam fronteiras geográficas, de soberania política, de origem social e económica e tecnológicas. É, no entanto, necessário pensar em uma estrutura que coordene as diversas dimensões da segurança no ciberespaço em Portugal, evitando iniciativas casuísticas e parcelares. Revemo-nos "na necessidade de prever a existência de um órgão coordenador das áreas ligadas à Cibersegurança e Ciberdefesa do Estado (Conselho Nacional de Cibersegurança), facilitando a definição não só de uma orientação política e estratégica mais coordenada e sinérgica como também uma gestão de crises mais eficaz" (Nunes, 2012: 115). O Conselho Superior de Segurança do Ciberespaço criado através da RCM n.º 115/2017 de

24 de agosto procura fazer essa ligação entre as diversas estruturas do Estado (Forças Armadas, Serviços de Informações, Centro Nacional de Cibersegurança, Polícia Judiciária, Autoridade Tributária e Aduaneira, entre outros), não contemplando, na nossa perspetiva, incorretamente as duas Forças de Segurança com maior implantação territorial (GNR e PSP) e com um papel primordial na prevenção da criminalidade, na sensibilização junto das populações (nomeadamente, as escolas), na ordem pública e na investigação criminal.

A sociedade em rede e a revolução tecnológica em curso criam novas oportunidades e vulnerabilidades decorrentes das interdependências estruturais e funcionais entre setores considerados críticos para o funcionamento da nossa sociedade. Por um lado, as oportunidades podem ser potenciadas pela redundância entre infraestruturas e respetivos sistemas de alerta de segurança, fortalecendo a resiliência global do sistema. Permitem a troca de conhecimentos ao nível global e a cooperação entre as redes internacionais de aplicação da lei. Por outro, aumentam o potencial das ameaças e riscos afetarem mais alvos e os cidadãos em geral, na medida em que podem aproveitar-se das redes e dos sistemas informáticos desprotegidos, afetando instituições estatais, empresas e comunidades. A interdependência entre setores distintos e da rede de ligações, não minimiza o impacto das quebras de segurança, poderá sim contribuir para o amplificar.

Estas organizações criminosas assumem caraterísticas de grande complexidade, de sofisticação, de pesquisa científica e de desenvolvimento de novas ferramentas tecnológicas, de *modi operandi*, de novas formas de iludir os sistemas de segurança e os investigadores criminais, procuram parcerias, fornecedores, clientes, peritos e vítimas para obterem elevados proventos financeiros.

As redes financeiras e as redes multimédia globais "*estão intimamente relacionadas, e esta meta-rede em particular tem um poder extraordinário. Mas não o poder todo (...) ela própria é dependente de outras grandes redes, como a rede política, a rede de produção cultural (...), a rede militar e de segurança, a rede global criminal e a rede global decisiva de produção e aplicação de ciência, tecnologia e gestão do conhecimento. Estas redes não se fundem (...), envolvem-se em estratégias de parceria e de competição, formando redes ad-hoc em torno de projetos específicos. Mas todas elas partilham um interesse em comum: controlar a capacidade de definir as regras e as normas da sociedade através de um sistema político que primariamente responda aos seus interesses e valores*" (Castells, 2013: 25).

A cibercriminalidade irá explorar intensivamente o novo paradigma da computação na nuvem, a computação móvel (por exemplo, os dispositivos moveis de pagamento), as estratégias *DIY, DIWM*, *BYOD* e a *IoT*

A *Big Data* afigura-se igualmente como uma oportunidade para as empresas, para as Polícias, mas também para a cibercriminalidade, consistindo em informação agregada e combinada de forma global e perspetivando o desenvolvimento de sistemas de análise preditiva e a inteligência artificial associada à videovigilância ou a nano-drones que poderão ser *the next big thing* no setor da segurança eletrónica, mas também para os piratas informáticos.

O estilo de vida digital liga os consumidores cada vez mais à internet e leva-os a adquirir novas tecnologias: computadores pessoais, telemóveis, veículos automóveis com sistemas de navegação eletrónica, eletrodomésticos inteligentes, serviços *online* (contas bancárias, compras eletrónicas), robots domésticos, ou outros. A integração de sistemas de georreferenciação e de informação geográfica (como o *GPS*) e outros aparelhos, como os computadores, telemóveis, automóveis, a armazenagem em nuvens (*clouds*), as redes de acesso sem fios (wifi), criam um novo campo para o comprometimento da nossa segurança e da nossa privacidade.

A obsolescência dos regimes legais dos Estados para fazer face ao desenvolvimento tecnológico, às ciberameaças e em concreto à cibercriminalidade e à sua permanente mutação e capacidade adaptativa, é uma realidade. Os Estados autoritários recrutam peritos para desenvolver capacidades na área da ciberguerra. Torna-se difícil estabelecer com exatidão a base territorial das organizações ou dos peritos que em concreto cometem o crime ou a série de crimes, o meio utilizado, o servidor, as consequências da ação (prejuízos, lucros, informação subtraída, a existência de cavalos de Troia).

Por outro lado, existem regiões no mundo que se constituem como um autêntico paraíso para a atividade destas organizações, devido à falência ou desregulação dos respetivos sistemas de segurança e justiça. A cooperação internacional entre os Estados (e das respetivas entidades judiciais e policiais), assim como a aposta e empenhamento das Organizações Internacionais (ONU, OTAN, U.E.) e das multinacionais privadas na prevenção, proteção, deteção, reação e investigação das novas ameaças e riscos informáticos é crucial.

À medida que a tecnologia avança, surgem novas ferramentas e formas de iludir as autoridades; "*as limitações tecnológicas na deteção, classificação, e vestígios dos ataques, irão (...) complicar, ainda mais, a decisão estadual durante a análise de um ciberataque (...). A responsabilidade de um Estado deve ser julgada pelos factos disponíveis, mesmo se esta resulta numa atribuição errada. Primeiro, enquanto um Estado avalia um ataque com o melhor da sua capacidade técnica e atua com boa-fé face à informação disponível, este cumpre as suas obrigações internacionais. Segundo, Estados que recusam atuar em*

conformidade com o seu dever internacional de prevenir que o seu território seja usado para cometer ciberataques escolheram o risco de serem considerados indiretamente responsáveis, por acidente" (Sklerov, 2009: 76-78).

O século XXI necessita que os Governos e em concreto as Forças Armadas, as Polícias e os Serviços de Informações sejam versáteis, imaginativas, criativas e que adotem estratégias inovadoras para além das conceções tradicionais de segurança. Os desafios da tecnologia são e continuarão a ser avassaladores, dado que podem impactar nos direitos, liberdades e garantias dos cidadãos, mas também na melhoria da segurança coletiva, cabendo às instituições transnacionais e aos governos nacionais a consensualização e coordenação de políticas, o incremento da investigação cientifica de forma a garantirem a liberdade, a reforçarem a segurança e melhorarem a qualidade de vida nas sociedades modernas.

BIBLIOGRAFIA

Aquilla, John & Ronfeldt, David (2013), Ciberwar is Coming in Comparative Strategy, vol. 12, n.o 2 Spring, 141-165.

Barlow, John Perry (2006). Declaração de independência do ciberespaço. Brasília: Ministério da Cultura.

Barrinha, André & Carrapiço, Helena, Cibersegurança. In Segurança Contemporânea (Lisboa: Pactor, 2016)

Benkler, Yochai, Hacks of Valor. Why Anonymous is not a Threat to National Security in Foreign Affairs. April 4, 2012.

Disponível em: http://www.foreignaffairs.com/articles/137382/yochai-benkler/hacks-of- -valor. Consultado em 19 de outubro de 2017.

Castells, Manuel (2013), Redes de Indignação e Esperança. Movimentos Sociais na Era da Internet. Lisboa: Fundação Calouste Gulbenkian.

Fernandes, José Pedro Teixeira (2012). A Ciberguerra como Nova Dimensão dos Conflitos do Século XXI, In RI, n.o 33, março.

Fernandes, José Pedro Teixeira (2014). Ciberguerra. Quando a Utopia Se Transforma em Realidade. Vila do Conde: Verso da História.

Gibson, William, (1984). Neuromancer. Nova Iorque, Ace Books.

Goncalves, João Pinto (2016). Enquadramento legal da Cibersegurança em Portugal e no Mundo O impacto dos crimes cibernéticos no Direito Internacional. Alfeite: Escola Naval.

Kierkegaard, Sylvia (2007). EU Tackles Cybercrime. In Cyber Warfare and Cyber Terrorism. Editors Andrew M. Colarik, Lech Janczewski. Publisher Idea Group Inc (IG)): 431-432.

Klimburg, Alexander (2011). Mobilizing Cyber Power. In Survival: Global Politics and Strategy, vol. 53, n.o 1, fevereiro-março, pp. 41-60.

Kuehl, D.T. (2009). From Cyberspace to Cyberpower: Defining the Problem. F.D. Kramer et al., eds. Potomac Books, Inc. 24–42.

Harari, Yuval Noah (2018). 21 Lições para o Século XXI. Amadora Elsinore.

Leigh, David & Harding, Luke, Wikileaks. Inside Julian Assange's War on Secrecy. London: Guardian Books, 2011.

Mathews, Jessica T., Power Shift. In Foreign Affairs, 76:1, 1997, p. 50-66. Disponível em: http://www.polsci.wvu.edu/faculty/hauser/PS293B/MathewsPowerShiftForA-ff1997.pdf – Consultado em 15 de outubro de 2017.

Natário, Rui (2013), O Combate ao Cibercrime: Anarquia e Ordem no Ciberespaço. Lisboa: Revista Militar n.o 2541.

NATO (2010). Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organization. Disponível em: http://www.nato.int/lisbon2010/ strategic-concept-2010-eng.pdf. Consultado em 18 de outubro de 2017-10-22

Nunes, Paulo Viegas, (2010). Mundos Virtuais, Riscos Reais: Fundamentos para a definição de uma Estratégia de Informação Nacional. In: Revista Militar. Lisboa: Empresa da Revista Militar, pp. 1169-1198.

Nunes, Paulo Viegas, (2012). A Definição de uma Estratégia Nacional de Cibersegurança. In: Nação e Defesa – Revista Quadrimestral n.o 133. Lisboa: Instituto da Defesa Nacional, pp. 113-127.

Nunes, Paulo Viegas, (2015). Sociedade em Rede, Ciberespaço e Guerra de Informação. Contributos para o Enquadramento e Construção de uma Estratégia Nacional de Informação (Lisboa: Instituto de Defesa Nacional, 2015)

Ralo, Jorge (2013). CiberSegurança e CiberDefesa. In Direcção-Geral de Política de Defesa Nacional. Disponível em: http://dgpdn.blogspot.pt/2013/03/artigo-de-opiniao- -ciberseguranca-e.html. Consultado a 09/11/2015.

Ramonet, Ignacio (1998). Geopolítica do Caos. Petrópolis. Editora Vozes.

Schjolberg, S. (2012). An International Criminal Court or Tribunal for Cyberspace ICTC). East West Institute.

Sklerov, Matthew J. (2009), Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Which Neglect Their Duty to Prevent. In Military Law Revue, vol. 201, pp. 1-85.

Disponível em: http: //www.loc.gov./rr/frd/Military Law/Military_Law_Review/pdf-files/201-fall-2009. pdf Consultado em: 19 de outubro de 2017.

Utsonomiya, Fred Izumi & Reis, Mariza de Fátima. Reflexões sobre o alcance do agir comunicativo da sociedade civil em redes sociais: o ciberativismo em questão. In SIMSOCIAL – Simpósio em Tecnologias Digitais e Sociabilidade – Mídias Sociais, Saberes e Representações – Anais. Salvador, outubro de 2011. Disponível em: http://gitsufba.net/simposio/wp-content/uploads/2011/09/Reflexoes-sobre-o-al- cance-do-agir-comunicativo-da-sociedade-civil-em-redes-sociais-UTSUNOMIYA- -Fred-REIS-Mariza.pdf. Consultado em 14 de outubro de 2017.

Convenção do Conselho da Europa (CCE), de 23 de novembro de 2001 (designada por Convenção de Budapeste), ratificada por Portugal em 2009, através da Resolução da Assembleia da República n.o 88/2009, de 15 de setembro

Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

Estratégia Nacional de Segurança do Ciberespaço (Resolução do Conselho de Ministros n.o 36/2015 de 12 de junho).

A CIBERSEGURANÇA À LUZ DA CRIMINOLOGIA MODERNA

NUNO CAETANO LOPES DE BARROS POIARES [1]

1 Diretor do ICPOL-ISCPSI. Professor do Instituto Superior de Ciências Policiais e Segurança Interna e do Instituto Politécnico de Beja. Título de Especialista em Direito Penal e Doutor em Sociologia Política. Membro da Associação Portuguesa de Criminologia. Endereço eletrónico*:* ncpoiares@psp.pt
O presente estudo representa o desenvolvimento da comunicação apresentada no Curso de Pós-Graduação sobre Direito do Ciberespaço, organizado pelo Instituto de Ciências Jurídico-Políticas e pelo CIJIC da Faculdade de Direito da Universidade de Lisboa.

RESUMO

No presente artigo o autor desenvolve uma análise teórica sobre os desafios que se colocam aos cidadãos face a (in)segurança no ciberespaço à luz da criminologia moderna, demonstrando a relevância do conhecimento científico prospetivo e multidisciplinar, capaz de antever cenários, diminuir a probabilidade de vitimização e propor respostas de apoio à governança na sociedade de risco.

Palavras-Chave: cibersegurança, ciberpoliciamento, problemas sociais, criminologia moderna, criminologia ambiental.

1. INTRODUÇÃO

O filósofo Herbert Marshall McLuhan (1964) formulou o conceito de aldeia global e previu uma sociedade tomada pelos meios de comunicação que atuariam por via eletrónica[1]. Na verdade, a segurança cibernética passou a constituir um dos principais desafios para os Estados, desde logo porque a criminalidade informática tem vindo a aumentar, sendo possível extrapolar que, dentro de cerca de uma década, possa atingir mais de 10% da totalidade dos crimes cometidos em Portugal. Acresce que, todos os anos, no mundo inteiro, as vítimas perdem cerca de 290 biliões de euros, como resultado do cibercrime[2]. Em Portugal, a estratégia definida no âmbito da segurança do ciberespaço assenta na coordenação das estruturas nacionais com o Centro Nacional de Cibersegurança, desenvolvimento da capacidade de ciberdefesa e de resposta a incidentes; revisão e atualização da legislação[3], melhoria das capacidades da Polícia Judiciária (PJ); maior robustez dos sistemas de deteção antecipada de ameaças; educação, sensibilização e prevenção[4], através da promoção da utilização segura das Tecnologias de Informação e Comunicação; investigação e desenvolvimento e cooperação entre parceiros nacionais e internacionais[5].

Os desafios da sociedade de risco mundial[6] e em rede[7] apresentam-se como problemas complexos que exigem respostas inter(multi)disciplinares, permitindo colmatar e partilhar as *ignorâncias*[8] e, por essa via, encontrar as melhores soluções de apoio à decisão. A sociedade em rede e a revolução tecnológica criam novas oportunidades e vulnerabilidades[9] decorrentes

1 Georgiadou, E. (1995), *Marshall McLuhan's "global village" and the internet*, Master of Arts in Image Studies, University of Kent at Canterbury; e Leite, A. M. (2016), "A problemática da cibersegurança e os seus desafios", *CEDIS Working Papers*, n.º 49, setembro de 2016, p. 3, Lisboa: FDUNL.

2 https://www.europol.europa.eu/ec/cybercrime-growing *in* Santos, D. G. (2014), *A Cibersegurança em Portugal: a ação política em matéria de cibersegurança*, dissertação de mestrado, p. 1, Lisboa: ISCTE-IUL.

3 Recentemente foi aprovada a Lei n.º 44/2018, de 9 de agosto, que consubstancia a 46.ª alteração ao Código Penal, aprovado pelo Decreto-Lei n.º 400/82, de 23 de setembro, que reforça a proteção jurídico-penal da intimidade da vida privada na internet, alterando o artigo 152.º - Violência Doméstica e o artigo 197.º - Agravação das penas previstas nos artigos 190.º a 195.º.

4 Áreas de atuação privilegiadas da PSP e GNR, sobretudo a sensibilização dos públicos mais vulneráveis.

5 Santos, D. G. (2014), *A Cibersegurança em Portugal: a ação política em matéria de cibersegurança*, dissertação de mestrado, Lisboa: ISCTE-IUL.

6 Beck, Ulrich (2015), *Sociedade de risco mundial: em busca da segurança perdida*, Lisboa: edições 70.

7 Castells, M. (2002), *A Era da Informação: Economia, Sociedade e Cultura*, vol. I – A Sociedade em Rede. Lisboa: Fundação Calouste Gulbenkian.

8 Expressão do juiz conselheiro Laborinho Lúcio aquando de uma aula no ISCPSI no ano letivo 2015-2016.

9 As vulnerabilidades têm levado à procura de diversas soluções, inclusivamente ao nível da regulação do ciberespaço, o que tem demonstrado fragilidades no regime de proteção dos direitos, liberdades e garantias

das interdependências entre setores considerados críticos para o funcionamento da nossa sociedade[10], o que reforça a necessidade de interdisciplinaridade que encontra eco em diversas evidências, desde logo, no apelo materializado no processo de Bolonha, mas também em programas doutorais inovadores[11], a existência de uma licenciatura em Estudos Gerais[12] e uma área do saber designada como Criminologia, cuja *existência* depende da convergência de diversos ramos do conhecimento, fundidos no crisol da multidisciplinaridade[13], pois é uma ciência de confluentes, que interessa que aqueles que a ela aportam venham disponíveis para aprender e partilhar informação[14].

Os cientistas e a *Academia* do século XXI têm procurado contrariar aquilo a que Santos[15] designa como *ignorância especializada*, ao criticar a excessiva especialização visível em grande parte do século XX. Hoje a Ciência deve surgir com uma orientação de apoio à governança, um forte sentido de utilidade para a comunidade, os cidadãos e as instituições, assente numa análise multidisciplinar e prospetiva. Em finais do século XIX von Liszt concebeu a ciência do Direito Penal Total, a qual conjugava as três vertentes fundamentais para a prossecução da tarefa de controlo social do crime: o Direito Penal propriamente dito, a Criminologia e a Política Criminal[16], o que obrigava a uma triangulação de áreas do conhecimento que, atualmente, são estudadas, muitas das vezes, de forma isolada, olvidando que só fazem sentido à luz de uma convergência, como peças de um puzzle para uma melhor leitura da realidade. Fenómenos como a globalização e o surgimento de uma sociedade interconectada obrigam essa convergência.

(Castro, 2017).

10 Elias, L. (2018), *Ciências Policiais e Segurança Interna*, p. 343, Lisboa: ICPOL-ISCPSI.

11 *E.g.* o programa de doutoramento OpenSoc em *Sociologia* ministrado em consórcio pelo ICS-UL, o ISCSP-UL, Lisbon School of Economics & Management; FCSH-UNL; a U. Évora e a U. Algarve; o programa de doutoramento em *Filosofia da Ciência, Tecnologia, Arte e Sociedade*, ministrado em conjunto pelas Faculdades de Belas-Artes, Direito, Letras, ICS-UL e IST-UL; ou o programa doutoral em *Ciências da Sustentabilidade* ministrado pelas Faculdades de Arquitetura, Ciências, Direito, Farmácia, Letras, Medicina, Medicina Veterinária, IGOT, ICS, ISA e ISEG-UL.

12 Curso de Licenciatura em *Estudos Gerais*, inaugurado em 2011 pela Faculdade de Belas-Artes, FCUL e FLUL; e expandida à FDUL, FMH-UL, FPUL, ISCSP-UL e ISEG-UL. *In* https://www.ulisboa.pt/curso/licenciatura/estudos-gerais (consulta em 16.07.2018).

13 Szabo, D.; Le Blanc, M.; e Ouimet, M. (2008), "Introdução: orientações da investigação criminológica ao longo da década de 1990", *in* Le Blanc, Marc; Ouimet, Marc e Szabo, Denis (direção), *Tratado de Criminologia Empírica*, p. 21, Lisboa: Climepsi Editores.

14 Poiares, C. A. (2008), "Nota à Edição Portuguesa" *in* Le Blanc, M.; Ouimet, M. e Szabo, D. (Dir.), *Tratado de Criminologia Empírica*, p. 15, Lisboa: Climepsi Editores.

15 Santos, B. S. (2002), *Um Discurso Sobre as Ciências*, 13.ª edição, Porto, edições Afrontamento.

16 Costa, José de Faria (2007), *Noções Fundamentais de Direito Penal*, p. 28, Coimbra: Coimbra Editora.

2. DA CRIMINOLOGIA CLÁSSICA À CRIMINOLOGIA MODERNA

Para compreendermos o contributo da Criminologia para a compreensão holística da segurança no ciberespaço importa tecer uma (brevíssima) análise diacrónica relativamente ao quadro conceptual. Alguns autores defendem que o *fundador* da criminologia moderna foi Cesare Lombroso, com a publicação, em 1876, de seu livro *O homem delinquente*. Para outros, foi o antropólogo francês Paul Topinard que, em 1883, terá empregue pela primeira vez a palavra criminologia e há os que defendem a tese de que foi Raffaele Garofalo quem usou o termo como nome de um livro (*Criminologia*, 1885). Mas, independentemente dessa *discussão*, conseguimos balizar os diversos momentos que corporizam a consolidação da Criminologia na comunidade científica. Desde logo, um período pré-científico, desde a antiguidade, com um forte pendor religioso e uma etiologia sobrenatural; e um período científico que inicia com os estudos de Lombroso, com a sua obra (1876) como o marco inicial da criminologia científica, cuja tese principal era o delinquente sem livre arbítrio. A Criminologia, por sua vez, ramifica-se em dois universos: a Criminologia Clínica (de raiz bioantropológica) que procura uma explicação endógena do crime e do seu agente, procurando apontar uma causa da conduta criminosa que estaria no próprio sujeito, enquanto forma de anormalidade física e/ou psíquica; e a Criminologia Geral (de matriz sociológica) que coloca o foco da abordagem nas influências ambientais ou exógenas para a génese do crime, ou seja, a identificação do meio criminógeno em que o sujeito se encontra inserido.

Como principais escolas teóricas encontramos a Criminologia Clássica, a Criminologia Positiva e a Criminologia Moderna. A Criminologia Clássica[17] (que predomina essencialmente no século XVIII) não se preocupa com a ressocialização do delinquente, pois coloca o seu foco na visão da prevenção em torno do rigor da pena, defendendo que os meios de prevenir o delito precisam de ter natureza penal consubstanciada na ameaça do castigo; e procurava estabelecer limites ao *jus puniendi* do Estado, defendendo que a pena devia ser proporcional ao delito. Segundo a Criminologia Clássica o fundamento da responsabilidade penal encontra-se no livre-arbítrio e a metodologia é sobretudo lógico-dedutiva, não existindo a observação empírica dos factos. Como exemplos de pensadores da Escola Clássica encontramos Cesare Beccaria e, ainda, Francesco Carrara e Giovanni Carmignani. Mas outros

17 Dias, Jorge de Figueiredo e Andrade, Manuel da Costa (1997), *Criminologia: O Homem delinquente e a Sociedade Criminógena*, pp. 5-10, Coimbra, Coimbra Editora.

autores já tinham tratado de reflexões afins como Hobbes, Montesquieu, Voltaire e Rousseau.

O ano de 1764 marca, assim, o momento do nascimento da moderna racionalidade penal. Com a obra *Dos delitos e das penas* de Beccaria, o Direito Penal surge nas vestes que perduraram até aos dias de hoje[18]. Por outro lado, a Criminologia Neoclássica, apesar de também demonstrar uma preocupação com a dissuasão penal, colocou o acento tónico no funcionamento do sistema normativo, ou seja, a forma como os delinquentes percecionam o sistema normativo e as consequências. No entanto, foi com a Escola Positiva que se abandonou a centralização na figura do crime, passando o foco da pesquisa para o delinquente, com base no empirismo (observação e experimentação). A explicação da criminalidade passou a ser procurada na predisposição para a prática de comportamentos desviantes. Neste modelo teórico, a Criminologia explica as diferenças físicas, psicológicas e sociais entre delinquentes e não delinquentes. Os comportamentos humanos estão sujeitos ao determinismo, inexistindo o livre-arbítrio. Nesta corrente teórica destacam-se Lombroso, Ferri e Garofalo, referências da escola positiva italiana. Lombroso, por meio de pesquisa empírica, tentou comprovar que fatores biológicos estariam relacionados na etiologia do crime, defendendo o atavismo[19], ou seja, o reaparecimento de uma certa característica no organismo depois de várias gerações de ausência[20]. Mas já em 1775, Lavater concebe o Homem como reunindo vida animal, intelectual e moral. Como tal, pode ser objeto de uma ciência de superfície, a fisionomia, que busca no corpo as manifestações exteriores das capacidades interiores do ser humano[21].

O século XX verifica um alargamento do espetro de análise através da Criminologia Moderna, que tem como finalidade explicar e prevenir o fenómeno criminal, avaliar os diferentes modelos de controlo social e intervir na pessoa do delinquente e da vítima, mas também refletir sobre as políticas de segurança, criminais e prisionais (Poiares, 2014). Atualmente existem conceitos paralelos como Criminologia Aplicada, Criminologia Radical, Criminologia Ambiental e Criminologia Forense enquanto estudo científico do crime e dos criminosos com o objetivo de informar os processos investigativo e penal, interessando-se pelos aspetos da Criminologia diretamente relacionados com os tribunais, como é o caso

18 Agra, Cândido e Faria, Rita (2012) "História Epistemológica da Criminologia", *in* Agra, Cândido da (Dir.), *A Criminologia: Um arquipélago Interdisciplinar*, p. 33, Porto: U. Porto Editorial.
19 Cusson, M. (2011), *Criminologia*, 3.ª edição, p. 61, Alfragide: casa das letras. Atavismo tem origem na expressão em latim *atavus*, ancestral.
20 Em Portugal a Escola Positiva também teve adeptos em fins do século XIX (Poiares, 2016).
21 Agra, Cândido e Faria, Rita (2012) "História Epistemológica da Criminologia", *in* Agra, Cândido da (Dir.), *A Criminologia: Um arquipélago Interdisciplinar*, p. 47, Porto: U. Porto Editorial.

do *Profilling* Criminal[22]. Hodiernamente a Criminologia encontra-se perante uma crise de identidade como descreve Agra e Faria (2012). A diversidade dos objetos de estudo da Criminologia, a multiplicidade de métodos de investigação empírica e a sua proximidade a outras disciplinas que igualmente produzem conhecimento sobre os mesmos objetos, fazem com que a autonomia científica da Criminologia seja muitas vezes posta em causa, acerca das suas autonomia, identidade, método e aplicação[23]. Esta *crise* intensifica-se quando autores como Giddens defendem que a Criminologia trata somente das formas de comportamento sancionadas pela lei penal e algumas questões colaterais, como as tendências dos índices criminais, as técnicas que permitem medir o crime e as políticas conduzidas com o intuito de reduzir o crime no seio das comunidades; e que, por outro lado, a Sociologia do Desvio tem um objeto de estudo mais alargado, na medida em que se interessa pela pesquisa criminológica, mas também pela conduta que está fora do âmbito do Direito Penal[24], visão que não é totalmente pacífica.

22 *In* http://profilingcriminal.com/websites/profilingcriminal/?page_id=20 (consultado em 02.02.2016).
23 Agra, Cândido e Faria, Rita (2012) "História Epistemológica da Criminologia", *in* Agra, Cândido da (Dir.), *A Criminologia: Um arquipélago Interdisciplinar*, pp. 27-62, Porto: U. Porto Editorial.
24 Giddens, A. (2009) (2001), *Sociologia*, p. 206, 7.ª edição, Lisboa: Fundação Calouste Gulbenkian.

3. DA CRIMINOLOGIA AMBIENTAL

A crescente dificuldade do Estado na inversão das tendências do crime levou a que, a partir dos anos 50 do século XX, ganhasse expressão o ramo preventivo da Criminologia. Surgem diversas correntes empíricas que alargam o seu objeto de estudo da figura do delinquente para a análise das causas da criminalidade, que são de natureza ambiental e social. A prevenção situacional (ou da insegurança) surge nos anos 60 do século XX, como reação ao *boom* da pequena criminalidade na sociedade de consumo. Nos Estados Unidos, Cohen e Marcus explicam que, nesse período, o aumento dos assaltos a residências fica a dever-se ao concurso de dois eventos: a miniaturização dos aparelhos de uso doméstico (alvos mais apropriados) e o aumento da taxa de atividade feminina (dissuasão insuficiente nos lares)[25]. A prevenção situacional coloca o acento tónico na redução das oportunidades: parte-se do pressuposto que o crime resulta tanto da emergência de uma ocasião, como da motivação do autor. Nessa senda, surge o policiamento orientado para o problema que direciona a atividade para a sinalização de problemas policiais repetitivos (padrões/*clusters*), a análise das suas causas e a resolução e avaliação dos resultados alcançados[26].

No entanto, a criminologia tradicional tem revelado algum distanciamento da prática policial, surgindo, assim, teorias vinculadas à criminologia ambiental, que se revelam muito úteis, pois lidam com as causas situacionais imediatas dos eventos relacionados com o crime, incluindo as oportunidades e a inadequada proteção das vítimas e alvos; e os padrões do fenómeno da criminalidade, tendo em conta o espaço e o impacto das suas variáveis sobre as perceções e ações de potenciais vítimas e criminosos. As suas abordagens incluem as perceções e as respostas em relação a estereótipos da insegurança (beco sem saída, rua mal iluminada, arbustos altos, etc.). A preocupação recai na forma como o crime é praticado, procurando-se formas de reduzir as oportunidades e tentações para o crime e aumentar a perceção dos riscos associados à prisão. Para isso, recorre a áreas do conhecimento como a Geografia, Urbanismo, Arquitetura, etc., emergindo, assim, um grupo teórico explicativo do crime, mormente as correntes que defendem explicações do crime em função de fatores

25 Gomes, Paulo Valente (2005), "A prevenção situacional na moderna criminologia", *Volume Comemorativo dos 20 anos do ISCPSI*, pp. 161-172, Coimbra: Almedina.
26 Ramos, Óscar e Cardoso, C. (2012), "Questões de segurança em superfícies comerciais: Estado da Arte Criminológica", *in* Agra, C. (Dir.), *A Criminologia: Um arquipélago Interdisciplinar*, p. 249-280, Porto: U. Porto Editorial.

situacionais: a teoria das atividades rotineiras[27], a teoria da escolha racional, a teoria do padrão criminal e a teoria da oportunidade[28].

27 Esta teoria questiona-se relativamente aos elementos essenciais para ocorrer a química de um crime, ou seja, a convergência de tempo e espaço em, pelo menos, três elementos: um agressor motivado, um alvo adequado e a ausência de um guardião capaz de impedir o crime (UNIDAVI, 2010).

28 UNIDAVI (2010) *Policiamento orientado a soluções de problemas*: t*eorias do crime baseadas na Criminologia Ambiental*, Curso Superior de Tecnologia de Segurança Pública, Brasil.

4. PROBLEMAS SOCIAIS CONTEMPORÂNEOS

No início do século XXI Giddens identificou os nove tipos de crimes mais frequentes baseados na tecnologia associados aos crimes do futuro, destacando as fraudes efetuadas na internet na Grã-Bretanha em 1999, alertando para a necessidade de novas respostas de combate ao cibercrime[29]. A criminologia ambiental pode contribuir decisivamente para a diminuição da cibercriminalidade, através da dialética entre a procura de diminuição da probabilidade de ocorrência de crime e a criação de condições que contribuam para esse desiderato. Mas, ao fazê-lo, a criminologia deve acompanhar, de uma forma prospetiva, os novos fenómenos sociais que podem contribuir para alterar o contexto e, por essa via, gerar novos desafios securitários, nomeadamente a diminuição da natalidade, o envelhecimento da população; o crescendo de pessoas que vivem sozinhas[30] ou a mono-residencialidade[31] e a incapacidade de resposta nas instituições[32]; o abandonado dos idosos, a atribuição de personalidade jurídica a autómatos[33] e as consequências da síndrome *Wilson*[34], a consolidação da Irmandade Muçulmana na Europa[35] e a dialetica entre os conceitos de Segurança Interna e Defesa Nacional, sem olvidar as questões – não menos importantes – relacionadas com as alterações climatéricas e a escassez dos recursos como a água[36]. Acresce que, neste cenário, a segurança do ciberespaço surge como um dos pilares de qualquer estratégia nacional com a internet como palco de disputa global pelo Conhecimento e Poder. Hoje discute-se a

29 Giddens, A. (2001) (2009), *Sociologia*, pp. 236-239, 7.ª edição, Lisboa: Fundação Calouste Gulbenkian.
30 Poiares, N. (2018b), "Cibersegurança, literacia e resiliência digital dos idosos", *Janus: Anuário de Relações Internacionais*, Lisboa: Observare-UAL (no prelo).
31 Guerreiro, Maria das Dores (2003), "Pessoas sós: múltiplas realidades", *Sociologia: Problemas e Práticas*, n.º 43, pp. 31-49, Lisboa: CIES-IUL. *https://www.sabado.pt/vida/detalhe/20171019_1708_ha-cada-vez-mais-pessoas-a-viverem-sozinhas* (consulta em 13.05.2018).
32 Pocinho, R. (2018), *Investigador alerta para a falta de profissionais nas instituições de idosos*, entrevista à Agência Lusa. In https://lifestyle.sapo.pt/saude/noticias-saude/artigos/investigador-alerta-para-a-falta-de-profissionais-nas-instituicoes-de-idosos (consultado em 23.03.2018).
33 Em maio de 2018 a PLMJ Advogados discutiu a atribuição de personalidade jurídica a autómatos, no âmbito do Curso Avançado sobre *Inteligência Artificial & Direito*; e a FDUCP organizou, em 12 de novembro de 2018, a Conferência *A Inteligência Artificial no Diálogo de Saberes*.
34 No filme "O náufrago" (2000) o protagonista (Tom Hanks), após um acidente de avião, vive durante vários anos sozinho numa ilha do Pacífico Sul, tendo como única *companhia* uma bola de voleibol, à qual atribuiu o nome Wilson e com quem passou a ter conversas regulares. No fim do filme o protagonista perde Wilson no meio do oceano e sofre como se tivesse falecido um ser vivo.
35 Kassam, Raheem (2017), *No Go Zones: How Sharia Law is Coming to a Neighborhood near You*, United States: Regnery Publishing; e Aziz, Ramy (2018), "Political Islam in Europe: the case of the muslim brotherhood", *in* Poiares, N. e Marta, R. (Coord.), *Segurança Interna: desafios na sociedade de risco mundial*, pp. 7-19, Lisboa: ISCPSI.
36 Pereira, David Marcos (2018), "Alterações climáticas e subida do nível médio das águas do mar: fenómeno, impactos e segurança" *in* Poiares, N. e Marta, R. (Coord.), *Segurança Interna: desafios na sociedade de risco mundial*, pp. 21-39, Lisboa: ISCPSI.

necessidade de um reforço da cibereducação, em higiene digital, numa educação para a prevenção, no controlo da exposição da família ao mundo digital, assim como em certificação da cibersegurança, cibersoberania, ciberpoliciamento e que as guerras do futuro vão iniciar com um ciberataque massivo[37]. São variáveis essenciais em particular quando se pensa em públicos mais vulneráveis (*e.g.* menores e idosos[38]) que diariamente são vítimas no ciberespaço. Segundo dados oficiais da Polícia Judiciária as burlas através da internet são aquelas em que se prevê um aumento mais expressivo até ao final do ano de 2018. Em 2017 foram registados 335 inquéritos desta natureza – principalmente ligados à compra e venda de produtos online – e a projeção da PJ é que cresçam para 1340 em 2018[39].

Este tipo legal de crime é somente uma das categorias de desvios que podemos assistir no ciberespaço, palco privilegiado para a transposição dos desvios da sociedade hodierna. Essa projeção é potenciada por fenómenos como o envelhecimento da população, uma das transformações sociais mais significativas do século XXI, com implicações em todos os setores da sociedade, incluindo na estrutura familiar e nos laços intergeracionais. As pessoas que moram sozinhas em Portugal representam 21,4% do total de agregados domésticos, uma percentagem que é quase o dobro do que se verificava em 1991 (13,8%) (Censos, 2011). Perspetiva-se que, globalmente, o n.º de pessoas acima dos 60 anos vá duplicar em 2050 e triplicar em 2100[40]. Portugal passou de 708.569 idosos em 1960 para 2.010.064 idosos em 2011. Quando analisamos o número de pessoas com 65 e mais anos por cada 100 pessoas em idade ativa (com 15 a 64 anos) verificamos o seguinte: 1961 (27,5%), 1980 (43,8%), 2000 (98,8%) e 2016 (148,7%). Acresce que as projeções feitas pelo INE revelam que a população de Portugal pode passar, se a tendência atual não se alterar, de 10,292 milhões de habitantes em 2017 para 7,478 milhões em 2080.

37 Conferência *Resiliência Digital de um Estado Democrático*, integrada nas Conferências de Lisboa da Assembleia Parlamentar da Organização para a Segurança e Cooperação na Europa (08.05.2018).
38 Guimarães, Filipa (2018), *Os mais velhos e o engodo das ciberburlas românticas*, 04.02.2018, pp. 18-21, ano XXVIII, n.º 10.151, edição Lisboa: jornal Público.
39 *In* https://www.dn.pt/pais/interior/burlas-continuam-a-dominar-subidas-na-criminalidade-9627903.html (consultado em 24.07.2018).
40 *In* http://www.un.org/en/sections/issues-depth/ageing/ (ONU, consulta em 06.05.2018).

5. QUESTÕES PARA DEBATE

Vimos que a Ciência deve surgir, cada vez mais, como um instrumento de apoio à governança, na busca de uma sociedade de equilíbrios. Nessa lógica, a Criminologia surge como campo do conhecimento privilegiado para a compreensão das novas dinâmicas criminógenas e das medidas que deverão ser adotadas no sentido de prevenir e combater comportamentos desviantes. A criminologia ambiental ensina-nos que é possível articularmos a cibersegurança e a teoria das atividades rotineiras, colocando o enfoque na redução das oportunidades[41], o que obriga a uma higiene digital, uma educação para a prevenção e um controlo da exposição da família ao mundo digital. E se não existem dúvidas relativamente a quem deve assumir o papel de *front-line* e legítimo guardião no caso dos menores, menos pacífica é a definição desse papel relativamente aos idosos.

O mundo apresenta um conjunto de novas ameaças multivariáveis, colocando-se diversas questões para reflexão: caminhamos para um mundo envelhecido, de pessoas isoladas fisicamente e acompanhadas por coisas com personalidade jurídica? E, se isso for uma realidade, que desafios se colocam às forças e serviços de segurança? A Sociologia vai ter de repensar o seu objeto de estudo[42]? Quem deve assumir o papel de guardião no ciberespaço: o ciberpolícia? O ciberespaço é um campo de intervenção policial ou militar? Existem diferenças entre cibercrime e ciberdefesa que obrigam a separação entre campos de competências?[43]

41 Implica, inclusivamente, repensar o espaço urbano – *Crime Prevention Through Environmental Design* (CPTED). A este propósito *vide* Guerreiro, Maria J. et al (2007), "A gestão dos espaços urbanos e a criação de trajectos orientadores" in Nunes, Laura M. et al, *Crime e Segurança nas cidades contemporâneas*, pp. 175-187, Porto: Fronteira do Caos Editores.

42 É certo que a Sociologia trata dos problemas da sociedade, mas a sociedade é formada por nós e pelos outros seres humanos, apesar de ser usual dizermos que a sociedade é a *coisa* que os sociólogos estudam. Para aprofundamento *vide* Elias, Norbert (2008), *Introdução à Sociologia*, reimpressão da 3.ª edição, pp. 13-14, Lisboa: Edições 70.

43 No dia 18 de julho de 2018 realizou-se a Conferência *L'engagement des forces armées sur le territoire national – l'expérience française*, tendo como orador o Chefe de Estado Maior do Exército Francês a convite do Chefe do Estado Maior Português Português, na Academia Militar. Tratou-se de mais um *movimento* para reforçar o posicionamento dos militares relativamente ao seu papel na Segurança Interna. A este propósito *vide* Queffelec, Christian (2018), "O papel das Forças Armadas Francesas sobre o território nacional no âmbito do terrorismo" *in* Poiares, N. e Marta, R. (Coord.), *Segurança Interna: desafios na sociedade de risco mundial*, pp. 67-75, Lisboa: ISCPSI.

6. BIBLIOGRAFIA

Agra, Cândido e Faria, Rita (2012) "História Epistemológica da Criminologia", *in* Agra, Cândido da (Dir.) (2012), *A Criminologia: Um arquipélago Interdisciplinar*, pp. 27-62, Porto: U. Porto Editorial.

Aziz, Ramy (2018), "Political Islam in Europe: the case of the muslim brotherhood", *in* Poiares, N. e Marta, R. (Coord.), *Segurança Interna: desafios na sociedade de risco mundial*, pp. 7-19, Lisboa: ISCPSI.

Beck, Ulrich (2015), *Sociedade de risco mundial: em busca da segurança perdida*, Lisboa: edições 70.

Castells, Manuel (2002), *A Era da Informação: Economia, Sociedade e Cultura*, Volume I – A Sociedade em Rede. Lisboa: Fundação Calouste Gulbenkian.

Castro, Raquel Brízida (2017), "Ciberespaço e Constituição" - Opinião, in Boletim da Ordem dos Advogados, julho de 2017; http://boletim.oa.pt/oa-02/opiniao_raquel-alexandra-brizida-castro (consultado em 15.05.2018)

Correia, Pedro M. A. R.; Santos, Susana I. S.; Bilhim, João A. F. (2017), "Proposta de modelo explicativo das perceções sobre gestão e políticas públicas em matéria de cibersegurança e cibercrime" *Sociologia: Revista da Faculdade de Letras da Universidade do Porto*, Vol. XXXIII, pp. 95-113.

Costa, José de Faria (2007), *Noções Fundamentais de Direito Penal (Fragmenta iuris poenalis) - Introdução*, Coimbra: Coimbra Editora.

Cusson, Maurice (2011), *Criminologia*, 3.ª edição, Alfragide: casa das letras.

Dias, Jorge de Figueiredo e Andrade, Manuel da Costa (1997), *Criminologia: O Homem delinquente e a Sociedade Criminógena*, Coimbra, Coimbra Editora.

Elias, Norbert (2006), *O Processo Civilizacional*, 2.ª edição, Lisboa, publicações Dom Quixote.

Elias, Norbert (2008), *Introdução à Sociologia*, reimpressão da 3.ª edição, Lisboa: Edições 70.

Elias, Luís (2018), *Ciências Policiais e Segurança Interna: Desafios e Prospetiva*, Lisboa: ICPOL-ISCPSI.

Georgiadou, Elisabeth (1995), *Marshall McLuhan's "global village" and the internet*, Master Thesis (Master of Arts in Image Studies), Canterbury: University of Kent.

Gomes, Paulo Valente (2005), "A prevenção situacional na moderna criminologia", *Volume Comemorativo dos 20 anos do ISCPSI*, pp. 161-172, Coimbra: Almedina.

Giddens, Anthony (2001) (2009), *Sociologia*, 7.ª edição, Lisboa: Fundação Calouste Gulbenkian

Guerreiro, Maria J. et al (2007), "A gestão dos espaços urbanos e a criação de trajectos orientadores" *in* Nunes, Laura M. *et al*, *Crime e Segurança nas cidades contemporâneas*, pp. 175-187, Porto: Fronteira do Caos Editores.

Guimarães, Filipa (2018), *Os mais velhos e o engodo das ciberburlas românticas*, 04.02.2018, pp. 18-21, ano XXVIII, n.º 10.151, edição Lisboa: jornal Público.

Kassam, Raheem (2017), *No Go Zones: How Sharia Law is Coming to a Neighborhood near You*, United States: Regnery Publishing.

Leite, Ana Marta (2016), *A problemática da cibersegurança e os seus desafios*, CEDIS *Working Papers* | Direito, Segurança e Democracia, n.º 49, setembro de 2016, Lisboa: FDUNL.

Lombroso, Cesare (1876) (2013), *O homem delinquente*, 2.ª reimpressão, São Paulo: Ícone Editora.

Maria J. et al (2007), "A gestão dos espaços urbanos e a criação de trajectos orientadores" in Nunes, Laura M. et al, *Crime e Segurança nas cidades contemporâneas*, pp. 175-187, Porto: Fronteira do Caos Editores.

Penteado Filho, Nestor S. (2012), *Manual Esquemático de Criminologia*, 2.ª ed., São Paulo: editora Saraiva.

Pereira, David Marcos (2018), "Alterações climáticas e subida do nível médio das águas do mar: fenómeno, impactos e segurança" *in* Poiares, N. e Marta, R. (Coord.), *Segurança Interna: desafios na sociedade de risco mundial*, pp. 21-39, Lisboa: ISCPSI.

Poiares, Carlos Alberto (2008), "Nota à Edição Portuguesa" *in* Le Blanc, M.; Ouimet, M. e Szabo, D. (Dir.), *Tratado de Criminologia Empírica*, p. 13-15, Lisboa: Climepsi Editores.

Poiares, Nuno (2014), "A criminologia como ciência auxiliar da governança", *revista científica do ISCTAC*, vol. I, ano I, edição n.º 2, pp. 5-15, Beira, Moçambique.

Poiares, Nuno (2016), "Revisitando a Galeria de Criminosos Célebres em Portugal. História da Criminologia Contemporânea (1896-1908)", *Politeia*, pp. 405-420, vol. I – *Studia Varia*, Lisboa: ISCPSI.

Poiares, Nuno e Marta, Rui (Coord.) (2018a), *Segurança Interna: desafios na sociedade de risco mundial*, Lisboa: ICPOL-ISCPSI.

Poiares, Nuno (2018b), "Cibersegurança, literacia e resiliência digital dos idosos", *Janus: Anuário de Relações Internacionais*, Lisboa: Observare-UAL (no prelo).

Queffelec, Christian (2018), "O papel das Forças Armadas Francesas sobre o território nacional no âmbito do terrorismo" *in* Poiares, N. e Marta, R. (Coord.), *Segurança Interna: desafios na sociedade de risco mundial*, pp. 67-75, Lisboa: ISCPSI.

Santos, Boaventura S. (2002), *Um Discurso Sobre as Ciências*, 13.ª edição, Porto, edições Afrontamento.

Santos, Daniela Guerreiro (2014), *A Cibersegurança em Portugal: a ação política em matéria de cibersegurança*, dissertação de mestrado em Políticas Públicas, Lisboa: ISCTE-IUL.

UNIDAVI (2010) *Policiamento orientado a soluções de problemas*: t*eorias do crime baseadas na Criminologia Ambiental*, Curso Superior de Tecnologia de Segurança Pública, Brasil.

AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS

BRUNO PEREIRA [1]

E

JOÃO ORVALHO [2]

1 Instituto Politécnico de Beja
2 Instituto Politécnico de Beja

RESUMO

Uma Avaliação de Impacto sobre a Protecção de Dados (AIPD) é um processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais, avaliando-os e determinando as medidas necessárias para fazer face a esses riscos.

Palavras-Chave: Dados pessoais; tratamento de dados pessoais; AIPD; Regulamento Geral de protecção de dados.

1.INTRODUÇÃO

Como é sabido, o RGPD - Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dado) veio revogar a Diretiva 95/46/CE, 24 de outubro de 1995, assim como Lei n.º 67/98, de 26 de outubro, a Lei da Proteção de Dados Pessoais, nas matérias com ele conflituantes (Monteiro, 2017).

Uma das principais inovações do RGPD consiste na previsão da obrigatoriedade de realização de avaliações de impacto sobre a proteção de dados (AIPD), ou em inglês *Data Protection Impact Assessment* (DPIA), quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares (artigo n.º 35, n.º 1 do RGPD) (Ramalho & Costa, 2017).

Esta técnica de avaliação de riscos no procedimento de tratamento de dados pessoais não é, em absoluto, inovadora, pois é bastante conceituada e utilizada nos países anglo-saxónicos, no entanto a sua regulamentação expressa no plano Europeu configura-se como uma das principais novidades do RGPD (Pica, 2018).

Em síntese, uma AIPD é um processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais, avaliando-os e determinando as medidas necessárias para fazer face a esses riscos.

Assim, estas avaliações de impacto são instrumentos importantes em matéria de responsabilização, uma vez que ajudam os responsáveis pelo tratamento não apenas a cumprir os requisitos do RGPD, mas também a demonstrar que foram tomadas medidas adequa- das para assegurar a conformidade com o regulamento (dando resposta ao artigo n.º 24 do RGPD). Por outras palavras, uma AIPD é um processo que visa estabelecer e demonstrar conformidade (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

As avaliações de impacto são da responsabilidade das próprias empresas ou organismos estatais que gerem os dados pessoais de clientes, fornecedores, parceiros ou trabalhadores. Logo, nestas avaliações de impacto, deverão ser descritas as finalidades da recolha e

tratamento de dados, os riscos inerentes à perda de informação, e a eventuais danos para as liberdades e garantias dos cidadãos (JusNet, 2018).

2. DOCUMENTO DE AVALIAÇÃO DE IMPACTO SOBRE PROTEÇÃO DE DADOS

Se Segundo o Grupo de Trabalho do Artigo 29.º (G29) [1] as AIPDs são definidas como: "*Um processo destinado a descrever o tratamento, avaliar a necessidade e proporcionalidade do tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares resultantes do tratamento de dados pessoais (avaliando-os e determinando as medidas para lidar com os mesmos)*" (Ramalho & Costa, 2017).

Embora, o RGPD não apresente uma definição direta de "risco", o Considerando 75 liga o conceito de risco ao dano potencial aos indivíduos, permitindo ao responsável pelos dados construir uma referência que o irá guiar pelo processo de avaliação do impacto.

De qualquer modo, o RGPD não exige a realização de uma avaliação de impacto para todas as operações de tratamento de dados. A realização de uma AIPD é obrigatória somente quando o tratamento for "suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares" (artigo n.º 35, n.º 1 do RGPD), incluindo explicitamente alguma das três situações: "*avaliação sistémica e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado*" que sirva como base para "*decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar*", "*operações de tratamento em grande escala de categorias especiais de dados*" que são mencionados nos artigos n.º 9, n.º 1 e n.º 10, e "*controlo sistemático de zonas acessíveis ao público em grande escala*" (artigo n.º 35, n.º 3).

Para além dos três tipos de situações referidas no n.º 3 do artigo 35.º do RGPD, exige-se que as autoridades de controlo no território respetivo elaborem, tornem público e comuniquem uma lista das operações de tratamento sujeitas ao requisito de AIPD ao Comité Europeu para a Proteção de Dados (CEPD) (n.º 4 do artigo 35.º e alínea k do n.º 1 do artigo 57.º do RGPD) (CNPD, 2018; Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017). É possível encontrar a lista da Comissão Nacional de Proteção de Dados (CNPD) de tratamentos de dados pessoais sujeitos a avaliações de impacto em (Diário da República, 2018).

Tal como referido (CNPD, 2018), a lista não é exaustiva, podendo ainda surgir, designadamente em função do desenvolvimento tecnológico, outras situações em que se justifique, nos termos do n.º 1 do artigo 35.º, realizar obrigatoriamente a AIPD. Por isso,

esta é uma lista dinâmica, sendo atualizada sempre que se entender necessário (CNPD, 2018). Esta lista também preenche os pressupostos do n.º 1 do artigo 35.º, e tem por referência os critérios presentes (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017) nas páginas 10 a 12 (CNPD, 2018).

Entre os critérios a ter em consideração para aferir da necessidade de realização de uma avaliação de impacto, incluem-se o tratamento de dados destinados a (I) avaliação e classificação dos titulares, designadamente *profiling* (ex: uma empresa que define perfis comportamentais baseados na navegação dos utilizadores do seu *website*), (II) tomadas de decisão automatizadas com efeito jurídico ou análogo, (III) monitorização sistemática, (IV) tratamento de dados sensíveis, que incluem os dados relativos a comunicações, a localização, a saúde, bem como os dados financeiros e, em certos casos, dados tratados para fins puramente pessoais (como em matéria de serviços de armazenamento na nuvem de informação pessoal ou de *apps* com registo de informação diária do utilizador), (V) tratamento de dados em grande escala, (VI) tratamentos de dados resultantes de uma interconexão; (VII) tratamento de dados relativos a indivíduos especialmente vulneráveis; (VIII) utilização inovadora ou aplicação de soluções tecnológicas ou organizacionais, tal como a combinação do uso de impressões digitais com reconhecimento facial para controlo de acessos; (IX) transferência de dados para países terceiros, (X) ou quando o tratamento impede o titular dos dados de exercer um direito ou utilizar um serviço ou contrato (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017; Ramalho & Costa, 2017).

No entanto, deve-se salientar que o Considerando 91 do RGPD dispõe, expressamente, que o "tratamento de dados pessoais não deverá ser considerado de grande escala se disser respeito aos dados pessoais de pacientes ou clientes de um determinado médico, profissional de cuidados de saúde, hospital ou advogado. Nesses casos, a realização de uma avaliação de impacto não deverá ser obrigatória.". No que toca à "grande escala", o G29 refere que "apesar de o considerando dar exemplos relativos aos extremos da escala (tratamento por um médico por oposição ao tratamento de dados de um país inteiro ou à escala da Europa), existe uma extensa zona cinzenta entre estes dois extremos" (Grupo do Artigo 29.º para a Proteção de Dados, 2017).

De acordo com o G29, a verificação de mais do que um dos critérios deverá funcionar como indício da necessidade de realização de uma AIPD, sem prejuízo de essa necessidade de se poder verificar quando apenas um seja verificado (Ramalho & Costa, 2017). Na verdade, é considerada uma boa prática a realização de uma avaliação de impacto nestas condições. Por outro lado, uma operação de tratamento pode corresponder aos casos mencionados e

continuar a ser considerada pelo responsável como uma operação que não é suscetível de implicar um elevado risco. Consequentemente, este deve justificar e documentar as razões que o levam a não realizar uma AIPD e mencionar os pontos de vista do encarregado da proteção de dados (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

Sempre que não seja claro se a realização de uma AIPD é necessária, o G29 recomenda que, ainda assim, seja realizado o procedimento, uma vez que é um instrumento útil para ajudar os responsáveis pelo tratamento a cumprir a legislação relativa à proteção de dados (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

O G29 considera que uma avaliação de impacto não é obrigatória nos seguintes casos (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017):

- quando o tratamento não for "suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares" (artigo n.º 35, n.º 1);

- quando a natureza, o âmbito, o contexto e as finalidades do tratamento forem muito semelhantes ao tratamento em relação ao qual tenha sido realizada uma AIPD;

- quando as operações de tratamento tiverem sido previamente controladas por uma autoridade de controlo antes de maio de 2018 em condições específicas que não se tenham alterado. Em contrapartida, algumas alterações também podem fazer baixar os riscos. Neste caso, a revisão da análise do risco efetuada pode revelar que a realização de uma AIPD deixa de ser obrigatória;

- quando uma operação de tratamento, nos termos do artigo n.º 6, n.º 1, alíneas

c) ou e), tiver um fundamento jurídico no direito da UE ou de um Estado-Membro, em que o direito regule a operação de tratamento específica e em que a AIPD já tenha sido realizada como parte da adoção desse fundamento jurídico (artigo n.º 35, n.º 10), salvo se o Estado-Membro considerar necessário proceder a essa avaliação antes das atividades de tratamento;

- quando o tratamento estiver incluído na lista opcional (definida pela autoridade de controlo) de operações de tratamento para as quais não é obrigatória uma AIPD (artigo n.º 35, n.º 5).

É importante referir que o simples facto de as condições que conduzem à obrigação de realizar uma AIPD não terem sido satisfeitas não os dispensa do cumprimento das restantes obrigações previstas no RGPD ou em legislação especial (CNPD, 2018). Na prática, tal significa que os responsáveis pelo tratamento devem avaliar continuamente os riscos criados

pelas suas atividades de tratamento por forma a identificarem quando um certo tipo de tratamento é "suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares" (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

A AIPD deve ser realizada "antes de iniciar o tratamento" (artigo n.º 35, números 1 e 10, e Considerandos 90 e 93 do RGPD). O que ocorre em coerência com os princípios da proteção de dados desde a conceção e por defeito (artigo n.º 25 e considerando 78 do RGPD). Além de que, estas avaliações de impacto devem ser encaradas como instrumentos de apoio à tomada de decisão em relação ao tratamento (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

Tal como referido em (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017), uma avaliação de impacto deve ser iniciada o mais cedo possível na conceção da operação de tratamento, mesmo que algumas das operações de tratamento ainda sejam desconhecidas, sendo que deve existir uma atualização da mesma (AIPD) ao longo do ciclo de vida do projeto de modo a garantir que a proteção dos dados e a privacidade sejam consideradas e que seja incentivada a criação de soluções que promovem a conformidade. O facto de a AIPD poder necessitar de ser atualizada após o tratamento ter efetivamente sido iniciado não é uma razão válida para adiar ou não realizar a avaliação de impacto, visto que a mesma é um processo contínuo, especialmente quando uma operação de tratamento é dinâmica e está sujeita a mudanças permanentes.

Feita esta análise é possível, previamente, determinar as medidas que devem ser implementadas a fim de eliminar ou mitigar os riscos detetados, permitindo adotá-los no tratamento dos dados pessoais a fim de concretizar a tutela dos direitos fundamentais dos titulares destes (Pica, 2018).

Com base no artigo n.º 36, n.º 1, no caso da avaliação de impacto resultar que as operações a realizar colocam em risco a esfera jurídica do titular destes dados pessoais, e na ausência de medidas que afastam ou atenuem o risco (através de medidas razoáveis, atendendo à tecnologia disponível e aos custos de aplicação (Magalhães & Pereira, 2018), deve o responsável pelo tratamento consultar, previamente às operações de tratamento, a entidade de controlo (a CNPD em Portugal) devendo comunicar-lhe quem é o responsável pelo tratamento, as finalidades e os meios de tratamento previstos, as medidas e garantias previstas para salvaguardar os direitos e liberdades dos titulares dos dados pessoais, os contactos do encarregado dos dados pessoais (caso este exista na entidade responsável), o resultado da avaliação de impacto e, ainda, todas as informações que a entidade de controlo venha a solicitar (Pica, 2018).

De acordo com o G29, estão em causa casos em que os riscos identificados não podem ser suficientemente endereçados pelo responsável pelo tratamento (ex: quando os riscos residuais se mantêm elevados), como, a título de exemplo, situações em que os titulares dos dados se podem deparar com consequências significativas (ou até irreversíveis) que não podem ultrapassar, e/ou quando aparenta ser óbvio que o risco ocorrerá (Coutinho & Moniz, 2018).

Caso a autoridade de controlo considerar que o tratamento viola o previsto no RGDP, nomeadamente se o responsável pelo tratamento não tiver identificado ou atenuado suficientemente os riscos, deverá, no prazo de oito semanas a contar da receção do pedido de consulta, emitir orientações a este responsável ou, quando aplicável, ao subcontratante, podendo recorrer a todos os seus poderes referidos no artigo 58.º (artigo 36.º, n.º 2) (Coutinho & Moniz, 2018).

Na Figura 1 (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017) é possível verificar uma ilustração dos princípios básicos relacionados com a AIPD no RGPD.

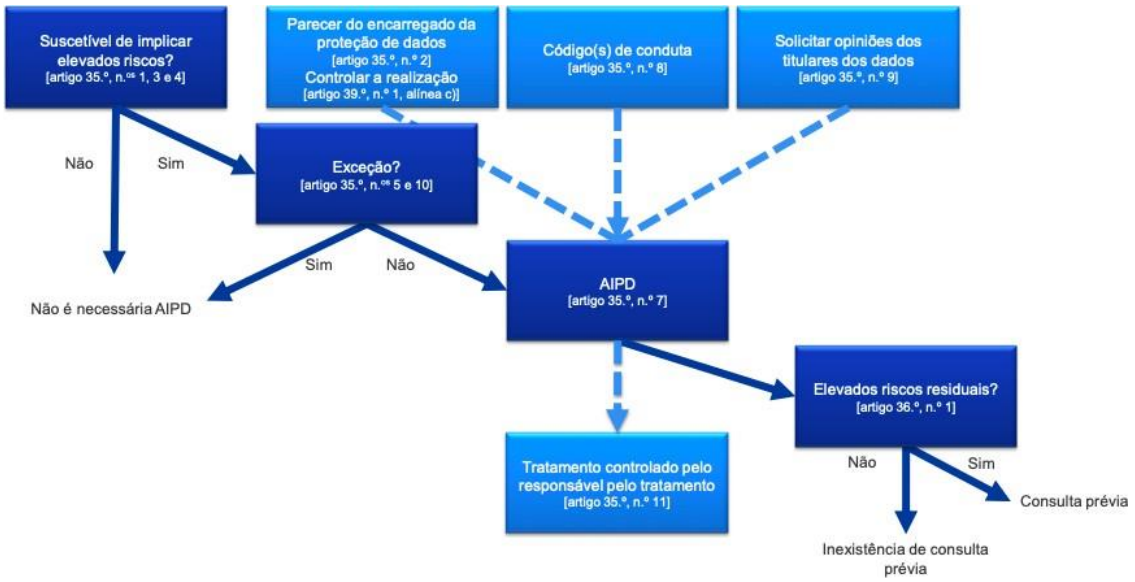

Figura 1. Princípios básicos relacionados com a AIPD no RGPD

Antes de mais, é preciso acentuar que o responsável pelo tratamento está incumbido de garantir a realização da AIPD (artigo n.º 35, n.º 2). Ainda que a realização da avaliação de impacto possa ser efetuada por outrem, dentro ou fora da organização, este responsável continua a ser o responsável último por essa tarefa (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017). Este responsável deve também solicitar o parecer do

encarregado da proteção de dados, nos casos em que este tenha sido designado (artigo n.º 35, n.º 2), sendo que o seu parecer e as decisões tomadas pelo responsável pelo tratamento devem ser documentadas na AIPD (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

No caso de o tratamento ser total ou parcialmente efetuado por um subcontratante, o subcontratante deve auxiliar o responsável pelo tratamento na realização da AIPD e fornecer todas as informações necessárias (em consonância com o artigo n.º 28, n.º 3, alínea f) (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

Nos termos do RGPD, a não conformidade com os requisitos de uma AIPD pode conduzir à imposição de coimas pela autoridade de controlo competente. Não realizar uma AIPD quando o tratamento está sujeito a uma avaliação de impacto (artigo 35.º, n.º 1 e números 3 a 4), realizar uma AIPD de forma incorreta (artigo 35.º, n.º 2 e n.ºs 7 a 9) ou não consultar a autoridade de controlo competente quando necessário (artigo 36.º, n.º 3, alínea e), pode resultar numa coima administrativa de até 10 milhões de euros ou, no caso de uma empresa, até 2% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

3.ABRANGÊNCIA DE AIPD

Por outro lado uma única avaliação de impacto pode ser utilizada para avaliar múltiplas operações de tratamento que sejam semelhantes em termos de natureza, âmbito, contexto, finalidade e riscos. A título de exemplo, se as autoridades ou organismos públicos pretendessem criar uma aplicação de tratamento comum, esta poderia ser abrangida apenas com uma AIPD (Pinheiro, Gonçalves, Gonçalves, Coelho, & Duarte, 2018).

Na verdade, as avaliações de impacto visam estudar sistematicamente novas situações que possam ser suscetíveis de implicar riscos elevados para os direitos e as liberdades das pessoas singulares, não havendo necessidade de realizar uma AIPD para os casos que já foram estudados (ou seja, operações de tratamento realizadas num contexto específico e com uma finalidade específica). Pode também ser aplicável a operações de tratamento semelhantes aplicadas por vários responsáveis pelo tratamento de dados. Nestes casos, deve ser partilhada ou disponibilizada ao público uma AIPD de referência, devem ser adotadas as medidas descritas na avaliação de impacto e deve ser fornecida uma justificação para a realização de uma única avaliação de impacto (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

Quando a operação de tratamento envolve responsáveis conjuntos pelo tratamento, estes devem definir detalhadamente as respetivas obrigações. A AIPD deve definir qual das partes é responsável pelas várias medidas concebidas para dar resposta aos riscos e proteger os direitos e as liberdades dos titulares dos dados. Cada responsável pelo tratamento de dados deve exprimir as suas necessidades e partilhar informações úteis sem comprometer segredos (ex: proteção de segredos comerciais, propriedade intelectual, informações empresariais confidenciais) ou revelar vulnerabilidades (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

4. METODOLOGIA PARA REALIZAÇÃO DE UMA AIPD

Existem metodologias diferentes, todavia os critérios (presentes no anexo 2 de (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017)) são comuns. O RGPD define os elementos mínimos de uma avaliação de impacto (artigo n.º 35, n.º 7, e considerandos 84 e 90), sendo eles:

- Uma descrição das operações de tratamento previstas e a finalidade do tratamento;
- Uma avaliação da necessidade e proporcionalidade das operações de tratamento;
- Uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos;

E as medidas previstas para:

- fazer face aos riscos;
- demonstrar a conformidade com o Regulamento.

Recordemos que uma AIPD, ao abrigo do RGPD, é um instrumento que visa gerir os riscos para os direitos dos titulares dos dados e, como tal, avalia-os na perspetiva destes últimos, como acontece em determinados domínios. Em contrapartida, a gestão dos ris- cos noutros domínios (ex: segurança da informação) centra-se na organização (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

Numa perspetiva organizacional, a execução de uma AIPD serve não só para estar em harmonia com a lei, evitando coimas avultadas, mas também para melhorar a reputação da empresa aos olhos dos indivíduos cujos dados são processados, demonstrando um maior nível de transparência do que se verificava no passado. Podem também surgir benefícios financeiros, tendo em conta que identificar um problema cedo significa, de forma geral, que a sua solução será menos cara do que se o mesmo problema fosse descoberto mais tarde.

As avaliações de impacto servem, assim, como uma parte vital da proteção por *design*, pois visam garantir que se está em conformidade perante a proteção de dados desde o início de um projeto.

Procurando facilitar a tarefa dos responsáveis, o G29 disponibilizou um anexo com os critérios mínimos para uma AIPD aceitável, tendo como base quatro pilares: um descrição sistemática das operações de tratamento dos dados, uma avaliação da necessidade e proporcionalidade dos tratamentos para os efeitos desejados, a garantia de que os riscos para

os direitos e liberdades dos titulares dos dados são geridos e que as partes interessadas (encarregado da proteção de dados, titulares dos dados) são envolvidas no processo (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

No entanto, e tendo em conta que não existe nenhum modelo totalmente padronizado para realização de uma avaliação de impacto, é possível, e até desejável em algumas ocasiões, a utilização de um *template* existente do que a criação de um novo documento de raiz, apenas baseado nos critérios.

Por sua vez e por exemplo, no Reino Unido, um órgão independente, a *Information Commissioner's Office* (ICO), disponibiliza um modelo de realização de uma AIPD (Information Comissioner's Office, 2018b), composto por sete passos, muito completo, e que deverá ser suficiente para uma primeira abordagem às AIPDs. A tabela 1 representa e explica os conteúdos dos passos do modelo.

Tabela 1

Passos do Modelo AIPD da ICO

Passos	**Pontos Importantes**
1. Identificação da necessidade para realização de uma AIPD	Em que consiste o projeto: - objetivo; - tipo de tratamento. Usado em conjunto com a lista de casos em que uma AIPD deve ser realizada, fundamentando cada ponto.

2. Descrição do tratamento	Natureza do tratamento: - como se vão coletar, usar, armazenar e eliminar dados; - qual é a fonte dos dados; - partilha de dados. *Scope* do tratamento: - natureza dos dados (inclui categorias especiais ou registos criminais?); - quantidade de dados coletados e usados; - frequência do tratamento; - duração do armazenamento; - número de titulares possivelmente afetados; - área geográfica que o tratamento cobre. Contexto do tratamento: - natureza da relação com os titulares; - quantidade de controlo por parte dos titulares; - expectativas dos titulares em relação ao tratamento; - inclusão de grupos vulneráveis; - preocupações relativamente ao tipo de tratamento ou possíveis falhas de segurança - utilização de novas tecnologias; - existência de questões de interesse

	público; - códigos de conduta ou certificações estabelecidas. <u>Propósito do tratamento:</u> - interesses legítimos; - resultado pretendido para os titulares; - benefícios esperados para a organização ou sociedade em geral.

3. Consulta	Consulta dos titulares: - quando e como se vão procurar e documentar as opiniões dos titulares. Consulta de outros: - consulta de intervenientes internos; - consulta de pessoal externo, caso necessário - peritos em lei, IT, etc.
4. Avaliação da necessidade e proporcionalidade	Descrição de medidas de conformidade e proporcionalidade: - base legal para o tratamento; - cumprimento do objetivo estabelecido; - possíveis formas alternativas de cumprir o objetivo; - prevenção contra *function creep*; - medidas para garantir a qualidade dos dados; - medidas para limitar o uso dos dados; - como se informam os titulares relativamente à privacidade; - como se implementam os direitos dos titulares; - salvaguardas relativamente a transferências internacionais.

5. Identificação e avaliação de riscos	<u>Descrição da fonte dos riscos e possíveis impactos nos titulares, em particular no que possa contribuir para:</u> - inabilidade de exercer direitos; - inabilidade de aceder a serviços ou oportunidades; - perda de controlo sobre o uso dos dados pessoais; - discriminação; - roubo de identidade ou fraude; - perdas financeiras; - danos reputacionais; - dano físico; - perda de confidencialidade; - qualquer outra desvantagem económica ou social. Construir uma matriz que cruze a gravidade do impacto com a probabilidade de ocorrência.
6. Identificação de medidas de mitigação	Medidas para reduzir ou eliminar os riscos identificados no passo n.º 5.

7. Assinaturas e resultados	Registar: - medidas adicionais a tomar; - se cada risco foi eliminado, reduzido ou aceite; - o nível geral de risco após implementação das medidas; - necessidade de consultar a CNPD; - aconselhamento do encarregado da proteção de dados.

Este modelo, em conjunto com os recursos disponibilizados pela CNPD, coloca os parâmetros para realizar uma avaliação de impacto competente.

Num esforço para simplificar a compreensão do que consiste uma AIPD, Pinheiro *et al.* dividem o processo em três fases: descritiva, onde se descrevem as operações de tratamento, a finalidade e os interesses legítimos do responsável; avaliativa, com base no princípio da proporcionalidade, em que se avaliam a relação entre as operações e os objetivos, bem como os riscos para os direitos e liberdades dos titulares; decisória, centrando-se nas medidas previstas para fazer face aos riscos (Pinheiro et al., 2018).

Já Saldanha (Saldanha, 2018) divide o procedimento em quatro partes: iniciação do projeto, onde se define o objetivo da AIPD, antes do começo do tratamento; análise do fluxo de dados, levando-se a cabo o mapeamento de informações pessoais, "criando um fluxograma de como a informação pessoal atravessa a organização, como resultado das atividades"; análise de privacidade, com recurso a questionários; relatório de avaliação de impacto de privacidade, onde se apresentam a avaliação dos riscos de privacidade, para além da implicação desses riscos e formas de mitigação, se possível.

Existem também soluções de *software* pagas cujo objetivo é facilitar o processo de realização de avaliações de impacto, como os produtos da *OneTrust* (OneTrust, 2018) e *Vigilant Software* (Vigilant Software, 2018), com recurso a ferramentas automatizadas que são integradas nos ciclos de vida dos projetos.

É importante também referir que a ISO/IEC 29134:2017 fornece uma diretriz detalhada sobre como executar uma AIPD e como manter evidências disso (Ruehl & Harvey, 2018).

5. DISCUSSÃO

Como já abordado, a AIPD é uma forma útil de garantir que existe conformidade perante a lei desde o início de um projeto. É possível, desta forma, evitar coimas avultadas que poderiam terminar pequenas e médias empresas sem capacidade financeira suficiente para as suportar. No entanto, na nossa opinião, são de facto estas empresas que estão em maior risco de cometer infrações, ainda que sem intenção.

Com esta análise de impacto consegue-se desde logo identificar os possíveis riscos para a proteção dos dados pessoais dos afetados e a valorização da probabilidade de ocorrerem, bem como os danos que causariam se se materializassem (Pica, 2018). É ainda importante considerar que o risco pode resultar não só da ineficiência das medidas de segurança adotadas, mas também de espetos inerentes à própria natureza dos dados do tratamento em questão (Coutinho & Moniz, 2018).

Isto sem esquecer que os responsáveis pelo tratamento de dados devem ter em conta um conjunto de considerações éticas no momento de conceção do próprio processo de tratamento, devendo interromper o mesmo, caso os riscos para os direitos e liberdades do indivíduos inerentes ao processo sejam elevados (Coutinho & Moniz, 2018).

No que se refere à frequência da realização de avaliações de impacto, é recomendado que seja um processo contínuo, integrado na metodologia de desenvolvimento adotada pela empresa, o que leva à questão: o que acontece quando uma pequena empresa não segue nenhuma metodologia específica?

A ausência de um bom planeamento ou estrutura numa empresa pode levar a que as AIPDs não sejam realizadas periodicamente, o que significa que podem surgir casos onde é feito o tratamento de dados pessoais entre AIPDs, sem que tal seja explícito nas mesmas. Nestas situações, as organizações correm o risco de não estar em concordância com o RGPD. Por esta perspetiva, as avaliações de impacto servem como motivação para até as pequenas empresas terem uma estrutura sólida que lhes permita desenvolver os seus projetos de forma organizada, demonstrando conformidade pelo caminho, construindo uma base para a evolução da empresa.

Além disso, os limitados recursos financeiros das pequenas empresas também impõem um obstáculo no que toca à consulta de peritos que possam garantir uma AIPD bem feita. Neste procedimento há muitos pontos que podem falhar, tendo em conta a lista de condições que compõem uma AIPD competente. Em pequenas empresas, especialmente naquelas onde não

existe um encarregado da proteção de dados, recai sobre o responsável pelo tratamento a grande maioria da realização da avaliação de impacto, levando a que possa escapar algo que vá contra o RGPD. Sem recurso a peritos externos nem a *software* pago, esta situação poderá acontecer facilmente.

Algo que poderia ajudar qualquer tipo de empresa/organização a realizar boas AIPDs seria a publicação de relatórios por parte de desenvolvedores de *software*, onde seriam enumerados todos os pontos cujo *software* poderá infringir sem as devidas precauções. Deste modo, os responsáveis sobre tratamento de dados teriam acesso a uma lista mais restrita de critérios a ter em conta, tendo em vista os *softwares* usados no projeto.

Resumindo, existem diversos desafios aquando da realização de uma AIPD, nomeadamente: o medo de ao realizar uma AIPD estar a restringir as opções e práticas de negócio, a falta de informação para permitir uma AIPD ser criada completamente, a conotação negativa da AIPD por estar associada a um trabalho árduo e que requer bastante tempo, a resistência à mudança (por parte das pessoas) que frequentemente está presente, entre outros desafios (Shad, 2018).

Os obstáculos impostos pela obrigatoriedade da realização de avaliações de impacto podem levar a que os responsáveis pelo tratamento de dados as interpretem como custos adicionais e tarefas desnecessárias, e não apenas como algo útil tanto para a organização, como também para os titulares dos dados.

6. CONCLUSÕES

Uma AIPD, tal como a maioria dos exercícios de avaliação de risco, encoraja a verificar cuidadosamente: o que se está a fazer, porque se está a fazer, os riscos envolvidos e como se está a controlar esses riscos a um nível aceitável (Macaskill, 2018; Messenger-Clark, 2017).

As avaliações de impacto são uma forma útil de os responsáveis pelo tratamento de dados aplicarem sistemas de tratamento de dados que estejam em conformidade com o RGPD, podendo ser obrigatórias para alguns tipos de operações de tratamento. Os responsáveis pelo tratamento de dados devem encarar a realização de uma AIPD como uma atividade útil e positiva que ajuda à conformidade jurídica (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

Visto que a realização da AIPD implica a avaliação do impacto das operações de tratamento, tem também a vantagem de promover implicitamente o cumprimento do Código de Conduta estabelecido no artigo 40.º do RGPD. Com esta análise de impacto é possível identificar os possíveis riscos para a proteção dos dados pessoais dos afetados e a valorização da probabilidade de ocorrerem, bem como os danos que causariam se se materializassem. Feita análise é possível, previamente, determinar as medidas que devem ser implementadas com vista a eliminar ou mitigar os riscos detetados, permitindo adotá-los no tratamento dos dados pessoais a fim de concretizar a tutela dos direitos fundamentais dos titulares destes (Pica, 2018).

A realização de uma avaliação de impacto é um processo contínuo e não um exer- cício que acontece uma única vez. Por uma questão de boa prática, uma AIPD deve ser continuamente revista e regularmente reavaliada (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017). Como o tratamento de dados é uma realidade mutável, é recomendável que as AIPDs sejam continuamente realizadas para tratamentos de dados em curso, devendo ser reavaliadas no prazo máximo de três anos, sem prejuízo de prazo inferior se impor em função das circunstâncias do caso (Ramalho & Costa, 2017).

Algumas empresas identificam corretamente situações onde é necessário a realização de uma AIPD, todavia apenas a fazem quando um projeto já muito progrediu, levando a que seja menos provável de ajudar a respeitar totalmente os requisitos do RGPD aquando da realização da avaliação de impacto. Além disso, os custos podem aumentar, no caso de um sistema necessitar de ser re-especificado ou corrigido (Clarke, 2018).

O RGPD dá aos responsáveis pelo tratamento de dados a flexibilidade necessária para determinar a estrutura e a forma precisas da AIPD com vista a que esta se encaixe nas práticas de trabalho existentes (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

As avaliações de impacto tratam-se de um mecanismo de gestão de risco dos direitos dos titulares dos dados e não da organização, devendo ser adaptada à realidade de cada organização (Ramalho & Costa, 2017). A publicação de uma avaliação de impacto não é um requisito jurídico do RGPD, essa decisão recai sobre o responsável pelo tratamento. Contudo, os responsáveis pelo tratamento devem considerar, pelo menos, a publicação parcial da AIPD, por exemplo, um resumo ou uma conclusão. Porém, esta publicação parcial ajuda a fomentar a confiança nas operações de tratamento de dados do responsável e a demonstrar responsabilidade e transparência (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

REFERÊNCIAS BIBLIOGRÁFICAS

Clarke, O. (2018). *Data Protection Impact Assessments under GDPR - Osborne Clarke | Osborne Clarke.* Consultado em 2019-01-22. Disponível: http://www.osborneclarke.com/insights/data-protection-impact-assessments-under-gdpr/CNPD. (2018). *Regulamento n.º 1/2018 relativo à lista de tratamentos de dados pessoais sujeitos a avaliação de impacto sobre a proteção de dados* (Tech. Rep.). Disponível: https://www.cnpd.pt/bin/decisoes/regulamentos/regulamento_1_2018.pdf

Coutinho, F., & Moniz, G. (2018). *Anuário de Protecção de Dados*. CEDIS.

Diário da República. (2018). *Regulamento 798/2018, 2018-11-30 - DRE.* Consultado em 2018-12-17. Disponível: https://dre.pt/web/guest/pesquisa//search/117182365/details/normal?l=1

European Data Protection Board. (2018). *Grupo de Trabalho do Artigo 29.º*. Consultado em 2019-01-24. Disponível: https://edpb.europa.eu/our-work-tools/article-29-working-party

Grupo de Trabalho do Artigo 29.º para a Proteção de Dados. (2017). *Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679* (Tech. Rep.). Disponível: https://www.cnpd.pt/bin/rgpd/docs/wp248rev.01_pt.pdf

Grupo do Artigo 29.º para a Proteção de Dados. (2017). *Orientações sobre os encarregados da proteção de dados (EPD)* (Tech. Rep.). Disponível: https://www.cnpd.pt/bin/rgpd/docs/wp243rev01_pt.pdf

Information Comissioner's Office. (2018a). Data Protection Impact Assessments (DPIAs). Disponível: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

Information Comissioner's Office. (2018b). *Sample DPIA template* (Tech. Rep.). Disponível: https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf

JusNet. (2018). *Jusjornal - Documento.* Consultado em 2018-12-17. Disponível: http://jusnet.wolterskluwer.pt/Content/DocumentMag.aspx?params=H4sIAAAAAAAAEAMtMSbH1czUAASMDQxNLtbLUouLM_DxbIM_CwNzQAiSQmVbpkp8cUlmQapuWmFOcqpaYVJyfU1qSGlqUaRtSVJoKADuZV9BGAAAAWKE

Macaskill, R. (2018). *So, What is a Data Protection Impact Assessment and Why Should Organizations Care? - DATAVERSITY.* Consultado em 2019-01-22. Disponível: https:// www.dataversity.net/data-privacy-impact-assessment-organizations-care/

Magalhães, F., & Pereira, M. (2018). *Regulamento Geral de Protecção de Dados* (2nd ed.). Porto: VidaEconómica.

Messenger-Clark, R. (2017). *Data Protection Impact Assessment* (Tech. Rep.). Disponível: http:// www.leeds.ac.uk/secretariat/documents/dpia.pdf

Monteiro, P. (2017). *Está preparado para o novo Regulamento Geral sobre a Protecção de Dados?| Human Resources.* Consultado em 2018-12-13. Disponível: https://hrportugal.pt/esta-preparado-para-o-novo-regulamento-geral-sobre-a-proteccao-de-dados/

OneTrust. (2018). *PIA & DPIA Automation | Products | OneTrust.* Consultado em 2019-01-03. Disponível: https://www.onetrust.com/products/assessment-automation/

Pica, L. (2018). *As avaliações de impacto, o encarregado de dados pessoais e a certificação no novo regulamento europeu de proteção de dados pessoais*. CYBERLAW by CIJIC. Disponível: https://www.cijic.org/wp-content/uploads/2018/03/3_AS-AVALIA%C3%87%C3%95ES-DE-IMPACTO-O-ENCARREGADO-DE-DADOS-PESSOAIS-E-A-CERTIFICA%C3%87%C3%83O-NO-NOVO-REGULAMENTO-EUROPEU-DE-PROTE%C3%87%C3%83O-DE-DADOS-PESSOAIS.pdf

Pinheiro, A., Gonçalves, C., Gonçalves, C., Coelho, C., & Duarte, T. (2018). *Comentário ao Regulamento Geral de Proteção de Dados* (12-2018 ed.). Edições Almedina.

Ramalho, D., & Costa, T. (2017). *LEGAL ALERT* (Tech. Rep.). Disponível: https://www.mlgts.pt/xms/files/v1/Publicacoes/Newsletters_Boletins/2017/Legal_Alert_-_Nova_orientacao_do_grupo_de_trabalho_do_artgio_29.pdf

Ruehl, U., & Harvey, J. (2018). *Data Protection Management Systems and the GDPR - General Data Protection Regulation (GDPR) | TUV USA*.Consultado em 2019-01-22. Disponível: https://www.tuv-ord.com/us/en/technology-it/general-data-protection-regulation-gdpr/data-protection-management-systems-and-the-gdpr/

Saldanha, N. (2018). *Novo Regulamento Geral de Proteção de Dados* (1st ed.). FCA - Editora de Informática.

Shad, A. (2018). *Do I need a Data Protection Impact Assessment to avoid GDPR fines? | ECOM- PLY.io*. Consultado em 2019-01-22. Disponível: https://ecomply.io/do-i-need-a-data-protection-impact-assessment-to-avoid-gdpr-fines/

Vigilant Software. (2018). *Data Protection Impact Assessment Tool | Vigilant Software*. Consultado em 2019-01-03. Disponível: https://www.vigilantsoftware.co.uk/topic/dpia

DIREITO AO ESQUECIMENTO

RUI PAULO COUTINHO DE MASCARENHAS ATAÍDE [1]

1 Professor Auxiliar da Faculdade de Direito da Universidade de Lisboa. O presente estudo representa o desenvolvimento da comunicação sobre o mesmo tema, apresentada no dia 26 de Abril de 2018 no Curso de Pós-Graduação sobre Cibersegurança e Ciberespaço, organizado pelo Instituto de Ciências Jurídico-Políticas, da Faculdade de Direito da Universidade de Lisboa.
Nota: versão actualizada que leva em linha de conta o Acórdão do Tribunal de Justiça de 24 de Setembro de 2019 (C-507/17) que negou carácter extraterritorial ao direito ao esquecimento.

RESUMO

Abordaremos algumas colisões entre valores constitucionais, procurando fazer a devida referência a casos emblemáticos quanto ao direito ao esquecimento no meio digital, nomeadamente o significado do acórdão "*Mario Costeja González*" e bem como dos desenvolvimentos subsequentes.

Espaço ainda para a relação entre o direito ao esquecimento e o direito à informação; e, o direito ao esquecimento versus direito à memória e à verdade histórica.

Por último, algumas implicações aduzidas pelo novo regulamento europeu sobre protecção de dados pessoais.

Palavras-Chave: Direito ao esquecimento; direito à informação; direito à memória; direito à verdade histórica; o RGPD.

1. A IDEIA JURÍDICA CENTRAL

I. O ideário que comanda o direito ao esquecimento não é uma criação recente, antes inspira diversas figuras normativas tradicionais como a prescrição, o indulto, a amnistia e ainda a própria duração das inscrições de condenações no registo criminal, visando impedir que estejam permanentemente em liça factos que já não têm relevância social. [1]

Com efeito, o direito ao esquecimento discute-se há largos anos na Europa e nos EUA. A título meramente exemplificativo, reproduz-se um extracto de uma interessante decisão, proferida em 1983 pelo Tribunal de Última Instância de Paris (Mme. Filipachi Cogedipresse), na qual esse direito restou assegurado nos seguintes termos:

"(...) qualquer pessoa que se tenha envolvido em acontecimentos públicos pode, com o passar do tempo, reivindicar o direito ao esquecimento; a lembrança destes acontecimentos e do papel que ela possa ter desempenhado é ilegítima se não for fundada nas necessidades da história ou se for de natureza a ferir sua sensibilidade; visto que o direito ao esquecimento, que se impõe a todos, inclusive aos jornalistas, deve igualmente beneficiar a todos, inclusive aos condenados que pagaram sua dívida para com a sociedade e tentam reinserir-se nela."

O que deu maior actualidade e acuidade ao tema do direito ao esquecimento foi a utilização massiva da Internet, que torna os conteúdos reproduzidos permanentemente acessíveis para sempre e a toda e qualquer pessoa, ao contrário do que sucede com os meios de comunicação tradicionais (jornais, revistas e livros). De facto, qualquer conteúdo que inclua dados pessoais pode ser disponibilizado de forma instantânea e permanente em formato digital ao nível mundial. Além disso, o uso crescente do *facebook*, principal rede social, popularizou a divulgação de dados pessoais pelos próprios usuários da rede, sem que tenham noção da real gravidade da exposição a que procedem da sua própria intimidade.

---

1 A informação sobre as inscrições de condenações permanece no registo criminal pelo prazo estabelecido na lei, contado a partir da data da extinção da pena aplicada. Os prazos legais estabelecidos são os seguintes (Lei nº 37/2015, de 5/5, art.º 11º e Lei nº 113/2009, de 17/9, art.º 4º):

a) Condenação por crime contra a liberdade e autodeterminação sexual: 25 anos;
b) Condenação por outro crime em pena de prisão superior a 8 anos: 10 anos;
c) Condenação por outro crime em pena de prisão entre 5 e 8 anos: 7 anos;
d) Condenação por outro crime em pena de prisão inferior a 5 anos, ou em pena de multa principal: 5 anos;
e) Condenação por outro crime em pena substitutiva da pena principal: 5 anos;
f) Decisões de dispensa de pena ou admoestação: 5 anos.

II. A ideia jurídica central da figura do direito ao esquecimento reside na protecção da vida privada e intimidade das pessoas, bem como a reabilitação e a ressocialização dos indivíduos, que seriam impedidas ou consideravelmente dificultadas pela lembrança indefinida dos factos cometidos. O direito ao esquecimento pode assim ser considerado como um desmembramento do direito à reserva de intimidade da vida privada (artigo 80º, CC), como se revelou de forma sintomática no caso de uma apresentadora brasileira que, no passado, fez um determinado filme do qual mais tarde se arrependeu e que ela não mais deseja que seja exibido ou rememorado por lhe causar prejuízos profissionais e transtornos pessoais.

2. NOÇÃO. COLISÃO ENTRE VALORES CONSTITUCIONAIS

Deste modo, o direito ao esquecimento pode ser definido como um direito fundamental de personalidade amparado no princípio da dignidade humana, segundo o qual o titular, pessoa individual ou colectiva, tem o direito à autodeterminação informativa, isto é, pode requerer o apagamento, retirada ou bloqueio da divulgação de dados, lícitos ou não, que lhe digam respeito, encontrados nos diversos meios de comunicação e que não tenham mais interesse público, judicial, histórico ou estatístico ou ainda que não sejam vedados por lei. Não se trata portanto de eliminar todas as referências a factos ocorridos no passado mas apenas de evitar a exposição desnecessária e lesiva de acontecimentos desprovidos de interesse público actual. Exprime em suma um poder de autocontrolo dos próprios dados pessoais.

Do ponto de vista da teoria jurídico-constitucional, o debate sobre o direito ao esquecimento configura uma colisão entre valores constitucionais, mormente, a liberdade de expressão/informação *versus* atributos basilares da pessoa humana, como a intimidade, privacidade e a honra e, por outro lado, conflitua com o direito à memória e à verdade histórica. Importa por isso convocar os elementos que se revelem necessários para fundamentar a final uma proposta de resolução destes dilemas.

3. CASOS EMBLEMÁTICOS

Esse propósito vai ser auxiliado pelo relato dos contornos factuais de alguns casos exemplares que servem para delimitar os precisos termos em que na actualidade se discute o direito ao esquecimento.

"*Caso Lebach*".

Em 1969, quatro soldados alemães foram assassinados numa cidade da Alemanha, chamada Lebach. Após o processo, três réus foram condenados, sendo dois à prisão perpétua e o terceiro a seis anos de reclusão. Esse terceiro condenado cumpriu integralmente a sua pena e, dias antes de deixar a prisão, tomou conhecimento que um canal de TV iria exibir um programa especial sobre o crime no qual seriam mostradas, inclusive, fotos dos condenados e detalhes sobre a vida privada dos acusados, designadamente, a insinuação de que eram homossexuais.

Em face disso, ele ingressou com uma acção inibitória para impedir a exibição do programa, a qual chegou até ao Tribunal Constitucional Alemão, que decidiu que a protecção constitucional da personalidade prevalecia sobre o direito à informação, pois haveria um prejuízo social à imagem do condenado, já que ele teria cumprido toda a pena e precisava de ter condições para se ressocializar, não sendo admissível que esse propósito fosse dificultado pela exploração, por tempo ilimitado, da pessoa do criminoso e da sua vida privada. Além disso, já não haveria mais interesse actual naquela informação, em virtude de o crime estar julgado e decidido há anos.

Em 1999, o Tribunal Constitucional Alemão permitiu a exibição de um programa sobre o caso, por considerar que a ressocialização dos indivíduos já estava conseguida duas décadas passadas.

"Chacina da Candelária"

Determinado homem foi denunciado por ter, supostamente, participado na conhecida "chacina da Candelária" (ocorrida em 1993 no Rio de Janeiro). No final do processo, ele foi absolvido.

Anos após a absolvição, a rede Globo de televisão realizou um programa chamado "Linha Directa", no qual contou como ocorreu a "chacina da Candelária" e apontou o nome desse homem como uma das pessoas envolvidas nos crimes.

O indivíduo instaurou então uma acção de indemnização, argumentando que a sua exposição no programa para milhões de telespectadores, em rede nacional, reacendeu na comunidade onde residia a imagem de que ele seria um assassino, violando os seus direitos à paz, anonimato e privacidade pessoal. Alegou, inclusive, que foi obrigado a abandonar a comunidade em que morava para preservar a sua segurança e a de seus familiares.

O Supremo Tribunal Federal (STF) reconheceu que esse indivíduo possuía o direito ao esquecimento e que o programa poderia muito bem ter sido exibido sem que fossem mostrados o nome e a fotografia da pessoa absolvida. Se assim fosse feito, não haveria ofensa à liberdade de expressão nem à honra do homem em questão.

O STF entendeu que o réu condenado ou absolvido pela prática de um crime tem o direito de ser esquecido, pois se a legislação garante aos condenados que já cumpriram a pena o direito ao sigilo da folha de antecedentes e a exclusão dos registros da condenação no instituto de identificação (art. 748 do CPP), logo, com maior razão, aqueles que foram absolvidos não podem permanecer com esse estigma, devendo ser-lhes assegurado o direito de serem esquecidos.

Como o programa já havia sido exibido, o STF condenou a rede Globo ao pagamento de uma indemnização por danos morais em virtude da violação ao direito ao esquecimento.

"Caso Aída Curi"

O segundo caso analisado foi o dos familiares de Aída Curi, abusada sexualmente e morta em 1958 no Rio de Janeiro.

A história desse crime, um dos mais famosos do noticiário policial brasileiro, foi apresentada pela rede Globo, também no programa "Linha Directa", tendo sido feita a divulgação do nome da vítima e de fotos reais, o que, segundo seus familiares, trouxe a lembrança do crime e todo sofrimento que o envolve.

Em razão da exibição do programa, os irmãos da vítima moveram uma acção de responsabilidade civil contra a emissora, com o objectivo de serem reparados dos danos morais, materiais e à imagem que haviam sofrido.

O STF entendeu que não seria devida indemnização, considerando que, nesse caso, o crime em questão foi um facto histórico, de interesse público e que seria impossível contar esse crime sem mencionar o nome da vítima, a exemplo do que ocorre com os crimes históricos, como os casos "Dorothy Stang" e "Vladimir Herzog".

Mesmo reconhecendo que a reportagem trouxe de volta antigos sentimentos de angústia, revolta e dor diante do crime, que aconteceu quase 60 anos atrás, o Tribunal entendeu

que o tempo, que se encarregou de tirar o caso da memória do povo, também fez o trabalho de abrandar seus efeitos sobre a honra e a dignidade dos familiares.

Na decisão, consignou-se: " (...) o direito ao esquecimento que ora se reconhece para todos, ofensor e ofendidos, não alcança o caso dos autos, em que se reviveu, décadas depois do crime, um acontecimento que entrou para o domínio público, de modo que se tornaria impraticável a actividade da imprensa para o desiderato de retractar o caso Aída Curi, sem Aída Curi."

4. O DIREITO AO ESQUECIMENTO NO MEIO DIGITAL

Trata-se agora do direito de eliminar ou tornar inacessíveis certos dados ou informações divulgados no ambiente digital que constem dos resultados de pesquisas efectuadas através de motores de busca da Internet, como ficou paradigmaticamente evidenciado no caso *Mario Costeja González*.

Em Março de 2010, Mario Costeja apresentou uma queixa na Agência Espanhola de Protecção de Dados (AEPD) contra o jornal La Vanguardia e o *Google Inc.* e o *Google Spain, SL*, baseada no facto de, quando um internauta inseria o seu nome no motor de busca do «Google Search», serem obtidas ligações a duas páginas do jornal da La Vanguardia de, respectivamente, 19 de Janeiro e 9 de Março de 1998, nas quais figurava um anúncio da venda da sua própria casa em hasta pública decorrente de um arresto com vista à recuperação de dívidas de M. Costeja González à Segurança Social. O queixoso alegou que, estando já paga há vários anos essa dívida à Segurança Social, tal informação não era actual e estava desprovida de toda a relevância.

O queixoso pretendia que o jornal La Vanguardia suprimisse ou alterasse as páginas em que constava o seu nome, para que os seus dados pessoais deixassem de aparecer ou que usasse ferramentas dos motores de busca para obstar o acesso a essas informações.

Em relação ao Google, solicitou a ocultação ou supressão das informações pessoais para que deixassem de aparecer nos resultados da pesquisa, deixando também de figurar nas ligações relacionadas com o referido jornal La Vanguardia.

Por decisão de 30 de Julho de 2010, a AEPD indeferiu a reclamação na parte que dizia respeito à La Vanguardia, tendo considerado que a publicação por esta das informações em causa estava legalmente justificada, dado que tinha sido efectuada por ordem do Ministério do Trabalho e dos Assuntos Sociais e teve por finalidade publicitar ao máximo a venda em hasta pública, a fim de reunir o maior número possível de licitantes.

Em contrapartida, deferiu esta mesma reclamação na parte concernente ao Google Spain e Google Inc. A este respeito, a AEPD considerou que os operadores de motores de busca estão sujeitos à legislação em matéria de protecção de dados, uma vez que realizam um tratamento de dados pelo qual são responsáveis e atuam como intermediários da sociedade de informação. A AEPD considerou que estava habilitada a ordenar a retirada dos dados e a interdição de aceder a determinados dados por parte dos operadores de motores de busca, quando considere que a sua localização e difusão são susceptíveis de lesar o direito fundamental de protecção dos dados e a dignidade das pessoas em sentido amplo, o que abrange também a simples vontade da pessoa interessada de que esses dados não sejam conhecidos por terceiros. A AEPD considerou que esta obrigação pode incumbir directamente aos operadores de motores de busca, sem que seja necessário suprimir os dados ou as informações do sítio *web* onde figuram, designadamente, quando a manutenção dessas informações nesse sítio seja justificada por uma disposição legal.

Inconformadas, o *Google Inc.* e o *Google Spain, SL* intentaram, em separado, recursos de anulação desta decisão para a Audiencia Nacional, que decidiu suspender o pleito e submeter ao TJUE a título de decisão prejudicial a interpretação dos artigos 2.º, alíneas b) e d), 4.º, n.º 1, alíneas a) e c), 12.º, alínea b) e 14.º, primeiro parágrafo, alínea a) da Directiva 95/46/CE, mas, também, do art.º 8.º da Carta dos Direitos Fundamentais da União Europeia.

O Advogado Geral considerou que o prestador de serviços de motor de busca não podia ser considerado responsável pelo tratamento de dados, acrescentando que o direito ao apagamento e bloqueio de dados constantes dos artigos 12º e 14º da Directiva não conferiam ao autor o direito de se dirigir directamente aos motores de pesquisa para impedir a indexação de informações referentes à sua pessoa.

Por seu lado, o TJUE declarou que:

1) A indexação de informação é uma actividade de tratamento de dados pessoais e o operador de motor de busca deve ser considerado Responsável pelo Tratamento.

2) A actividade de tratamento acima descrita, tem como condição de legitimidade o artigo 7.º, alínea f) da já citada Directiva, permitindo o tratamento de dados pessoais sempre que seja necessário prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, nomeadamente o direito ao respeito pela sua vida privada.

3) Para verificar a prevalência de interesses ou direitos e liberdades fundamentais da pessoa em causa, é necessário verificar não só o interesse económico do operador de tal motor nesse tratamento mas também o interesse legítimo dos internautas potencialmente interessados em ter acesso à informação indexada, tendo por exemplo em consideração a natureza da informação em questão e da sua sensibilidade para a vida privada da pessoa em causa, bem como do interesse do público em dispor dessa informação, que pode variar, designadamente, em função do papel desempenhado por essa pessoa na vida pública.

4) As actividades de um operador de um motor de busca, ao contrário das actividades de um editor de uma página web, não beneficiam das excepções previstas para as actividades para fins exclusivamente jornalísticos.

Deste modo, o operador de um motor de busca é obrigado a suprimir da lista de resultados, exibida na sequência de uma pesquisa efectuada a partir do nome de uma pessoa, as ligações a outras páginas web publicadas por terceiros e que contenham informações sobre esse sujeito, também na hipótese de esse nome ou de essas informações não serem prévia ou simultaneamente apagadas dessas páginas web, isto, se for caso disso, mesmo quando a sua publicação nas referidas páginas seja, em si mesma, lícita.

O individuo em causa tem o direito de a informação em questão sobre a sua pessoa deixar de ser associada ao seu nome através de uma lista de resultados exibida na sequência de uma pesquisa efectuada a partir do seu nome, sem que, todavia, a constatação desse direito pressuponha que a inclusão de tal informação nessa lista causa prejuízo a essa pessoa. Na medida em que esta pode, tendo em conta os seus direitos fundamentais nos termos dos artigos 7.° e 8.° da Carta, requerer que a informação em questão deixe de estar à disposição do grande público devido à sua inclusão nessa lista de resultados, esses direitos prevalecem, em princípio, não só sobre o interesse económico do operador do motor de busca mas também sobre o interesse desse público em aceder à informação numa pesquisa sobre o nome dessa pessoa. No entanto, não será esse o caso quando se afigure que, por razões especiais como, por exemplo, o papel desempenhado por essa pessoa na vida pública, a ingerência nos seus direitos fundamentais é justificada pelo interesse preponderante do referido público em ter acesso à informação em questão, em virtude dessa inclusão.

5. O SIGNIFICADO DO ACÓRDÃO *"MARIO COSTEJA GONZÁLEZ"*. DESENVOLVIMENTOS SUBSEQUENTES

Chamado a pronunciar-se pela primeira vez sobre a actividade dos motores de busca da internet na União Europeia no domínio dos direitos fundamentais da privacidade e da protecção de dados pessoais, o TJUE decidiu configurar o direito ao esquecimento no meio digital como um verdadeiro direito à autodeterminação informativa que permite controlar os dados pessoais e decidir os que poderão ser consultados e tratados por terceiras pessoas.

De toda a maneira, a expressão "direito ao esquecimento" talvez seja pouco rigorosa, sendo preferível falar-se de "direito à desindexação", porque não implica a supressão de informação da internet, mas apenas previne a disponibilização de certos resultados nas pesquisas dos motores de busca efectuadas com base no nome da pessoa. Portanto a informação mantém-se acessível directamente no website-fonte ou na pesquisa por outros temas, apenas desaparecendo uma espécie de facilitador de acesso a toda a informação que existe *online* sobre aquela pessoa, a qual pode ser consultada quando se saiba lá chegar sem ser através da pesquisa de um nome no motor de busca. Caso, por exemplo, seja aprovado o pedido de remoção de um artigo sobre Manuel Augusto e a sua viagem a Roma, não seriam apresentados os resultados de consultas com o nome Manuel Augusto, mas apresentar-se-ia os resultados de uma consulta como viagem a Roma.

Logo em 2014, foi criado o *Conselho Consultivo da Google para o Direito a Ser Esquecido* com o intuito de estabelecer critérios uniformizadores na ponderação do justo equilíbrio de direitos, em cumprimento da Sentença do TJUE de 13 de maio de 2014, o qual foi composto por oito conceituados especialistas independentes: Luciano Floridi (*Professor of Philosophy and Ethics of Information at the University of Oxford*), Sylvie Kauffman (*Editorial Director, Le Monde*), Lidia Kolucka-Zuk (*Director of the Trust for Civil Society in Central and Eastern Europe*), Frank La Rue (*UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*), Sabine Leutheusser-Schnarrenberger (*former Federal Minister of Justice in Germany*), José-Luis Piñar (*academic at Universidad CEU San Pablo in Madrid and former Director of the Spanish Data Protection Agency (AEPD*), Peggy Valcke (*Professor of Law at University of Leuven*) e Jimmy Wales (*Founder and Chair Emeritus, Board of Trustees, Wikimedia Foundation*).

O Relatório final com a interpretação e a definição de critérios respeitantes ao direito ao esquecimento pelo *Google* na aplicação a casos concretos, formulou as seguintes conclusões:[2]

- Em primeiro lugar, da jurisprudência do TJUE resulta que esta não consagra um Direito ao Esquecimento em geral e é preferível utilizar a expressão desindexação;
- O TJUE apenas refere a remoção de lista de resultados de busca pelo nome de uma pessoa, se os dados forem inadequados, irrelevantes ou deixaram de ser relevantes, ou excessivos.
- O TJUE invoca vários Direitos, tais como os Direitos à vida privada e à protecção de dados, Direito à liberdade de expressão, Direito de acesso à informação, os quais devem ser analisados num quadro global dos diversos instrumentos legais sobre Direitos e Liberdades Fundamentais na União Europeia.
- Tais Direitos dos titulares de oposição existem independentemente de danos.
- A avaliação do dano causado ao titular deve ser efectuada numa base prática, legal e ética.
- O operador do motor de busca deve ponderar, num justo equilíbrio, o interesse preponderante entre: os Direitos do titular, o interesse económico do operador e interesse do público em geral no acesso à informação.

Para avaliar o pedido de remoção ("delisting"), são apontados quatro critérios principais, sendo que nenhum é determinante em si, nem existe qualquer hierarquia:

1. Papel do titular na vida pública.

São identificadas três categorias:

a) Um papel claro na vida pública, por ex. Políticos, celebridades, artistas, desportistas, etc., em que o interesse do público geralmente prevalece;

b) Sem qualquer papel na vida pública, em que os direitos dos titulares geralmente justificam a remoção;

c) Um papel limitado na vida pública ou num contexto específico, tais como directores de escolas, alguns funcionários públicos, em que a especificidade da informação é determinante normalmente para a decisão de remoção

2 No respeitante ao enunciado das conclusões, segue-se de perto JOÃO MIGUEL JARDIM DE ABREU FERREIRA PINTO, *Direito ao esquecimento digital 2.0: Motores de busca da Internet após o Acórdão Google Spain (C-131/12)*, 2015, Lisboa (Tese de Mestrado), pp. 53 ss.

2. Natureza da informação.

Tipo de informação que indicia uma preponderância dos direitos do indivíduo:

a) Informação relacionada com a vida íntima ou sexual;

b) Informação financeira pessoal;

c) Contactos particulares e identificação

d) Informação considerada sensível nos termos da Legislação sobre protecção e dados;

e) Informação privada sobre menores;

f) Informação falsa, com associações incorrectas ou que coloca o titular em perigo;

g) Informação sobre a forma de imagem ou vídeo

Tipo de informação que indicia uma preponderância do interesse público:

a) Informação política, orientações e opiniões políticas;

b) Informação sobre opiniões religiosas ou filosóficas;

c) Informação relacionada com saúde pública e protecção do consumidor;

d) Informação sobre actividades criminosas;

e) Informação que contribui para o debate sobre matérias do interesse geral;

f) Informação factual e verdadeira;

g) Informação integral sobre registos históricos;

h) Informação integral sobre questões científicas ou expressão artística.

3. Fonte

Importa considerar a fonte da informação e a motivação da publicação, por exemplo, se é publicada por reputados *bloggers*, autores publicamente considerados ou informação publicada com o consentimento do próprio titular.

4. Tempo.

A sentença refere informação que em determinando momento era relevante, mas com a alteração das circunstâncias deixou de ser relevante. Por exemplo este critério pode ser determinante nos casos de titulares que tiveram um papel público activo e deixaram de ter. Este critério é particularmente relevante nos antecedentes criminais.

6. RELAÇÃO ENTRE O DIREITO AO ESQUECIMENTO E O DIREITO À INFORMAÇÃO. DIREITO AO ESQUECIMENTO *VERSUS* DIREITO À MEMÓRIA E À VERDADE HISTÓRICA

O direito ao esquecimento não constitui um direito fundamental absoluto. Deve-se sempre analisar se ainda existe um interesse público actual na divulgação daquela informação. Caso persista, o direito ao esquecimento subalterniza-se, sendo lícita a publicidade da notícia em causa. É o caso, por exemplo, de crimes genuinamente históricos, quando se tornar impraticável a narração dos factos dissociada das pessoas envolvidas. Ou seja, o direito à memória e à verdade histórica prevalecem sobre o direito ao esquecimento nos casos em que o interesse público da informação se sobrepõe à defesa da honra e da vida privada.

Consequentemente, prevalecem em princípio os direitos à privacidade e à protecção de dados do indivíduo, que só devem ser sacrificados em caso de manifesta relevância, actualidade e interesse público dos dados pessoais da pessoa em causa.

Imagine-se, por exemplo, que um indivíduo deseje simplesmente ser esquecido, deixado em paz. Será o caso de uma pessoa famosa (um artista, desportista, político, etc.) que, em determinado momento de sua vida, decide voltar a ser um anónimo e não mais ser incomodado com reportagens, entrevistas ou qualquer outra forma de exposição pública. Em certa medida, isso aconteceu na década de 90 com alguns ex-actores que, mesmo tendo carreiras de muito sucesso na televisão, optaram por voltar ao anonimato. Essa é, portanto, uma das expressões do direito ao esquecimento, que deve ser juridicamente assegurada.

Assim, se um veículo de comunicação realizar um programa ou documentário que mostre a vida actual dessas ex-actrizes, com fotógrafos e câmaras acompanhando o seu dia-a-dia, entrevistando pessoas que as conheciam na época e mostrando lugares que actualmente frequentam, etc., elas poderão requerer medidas que impeçam essa violação do seu direito ao esquecimento.

7. O NOVO REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO DE 27 DE ABRIL DE 2016 E A LEI N.º 58/2019, DE 8 DE AGOSTO

I. Em 25 de Maio de 2018, entrou em vigor o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de Abril de 2016 (Regulamento Geral sobre a Protecção de Dados), relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Directiva 95/46/CE. [3]

Destarte, e conforme se explica na exposição de motivos, os titulares dos dados têm direito a que os dados que lhes digam respeito sejam rectificados, assim como o «direito a serem esquecidos» quando a conservação desses dados violar o Regulamento ou o direito da União ou dos Estados-Membros aplicável ao responsável pelo tratamento. Em especial, os titulares de dados devem ter direito a que os seus dados pessoais sejam apagados e deixem de ser objecto de tratamento se não forem mais necessários para assegurar a finalidade que determinou a sua recolha ou tratamento, se os titulares dos dados retirarem o seu consentimento ou se opuserem ao tratamento de dados pessoais que lhes digam respeito ou se o tratamento dos seus dados pessoais não respeitar o disposto no Regulamento. Esse direito assume particular importância quando o titular dos dados tiver dado o seu consentimento quando era criança e não estava totalmente ciente dos riscos inerentes ao tratamento, e mais tarde deseje suprimir esses dados pessoais, especialmente na Internet. O titular dos dados deverá ter a possibilidade de exercer esse direito independentemente do facto de já ser adulto. No entanto, o prolongamento da conservação dos dados pessoais deverá ser efectuado de forma lícita quando tal se revele necessário para o exercício do direito de liberdade de expressão e informação, para o cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, por razões de interesse público no domínio da saúde pública, para fins de arquivo

---

3 Assinale-se que a protecção dos dados pessoais já era garantida pelo artigo 8º da Carta dos Direitos Fundamentais da União Europeia:
Artigo 8.º
Protecção de dados pessoais

1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.
2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.
3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

Para reforçar o direito a ser esquecido no ambiente por via electrónica, o âmbito do direito ao apagamento é alargado através da imposição ao responsável pelo tratamento que tenha tornado públicos os dados pessoais, da adopção de medidas razoáveis, incluindo a aplicação de medidas técnicas, para informar os responsáveis que estejam a tratar esses dados pessoais de que os titulares dos dados solicitaram a supressão de quaisquer ligações para esses dados pessoais ou de cópias ou reproduções dos mesmos. Ao fazê-lo, esse responsável pelo tratamento deverá adoptar as medidas que se afigurarem razoáveis, tendo em conta a tecnologia disponível e os meios ao seu dispor, incluindo medidas técnicas, para informar do pedido do titular dos dados pessoais os responsáveis que estejam a tratar os dados.[4]

II. Por seu lado, a Lei n.º 58/2019, de 8 de Agosto que veio assegurar a execução, na ordem jurídica interna, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho,

---

4 O direito ao esquecimento está consagrado nos seguintes termos do artigo 17º do Regulamento:

Artigo 17.º
Direito ao apagamento dos dados («direito a ser esquecido»)

1.O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos:
a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento;
b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.o, n.o 1, alínea a), ou do artigo 9.º, n.º 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento;
c) O titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 2;
d) Os dados pessoais foram tratados ilicitamente;
e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito;
f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8.º, n.º 1.
2.Quando o responsável pelo tratamento tiver tornado públicos os dados pessoais e for obrigado a apagá-los nos termos do n.º 1, toma as medidas que forem razoáveis, incluindo de carácter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efectivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos.
3.Os n.º s 1 e 2 não se aplicam na medida em que o tratamento se revele necessário:
a) Ao exercício da liberdade de expressão e de informação;
b)Ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado--Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento;
c) Por motivos de interesse público no domínio da saúde pública, nos termos do artigo 9.º, n.º 2, alíneas h) e i), bem como do artigo 9.º, n.º 3;
d) Para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89.º, n.º 1, na medida em que o direito referido no n.º 1 seja susceptível de tornar impossível ou prejudicar gravemente a obtenção dos objectivos desse tratamento; ou
e) Para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

de 27 de Abril de 2016, contém algumas disposições pertinentes em matéria de direito ao esquecimento.

Com respeito à protecção dos dados das pessoas falecidas, o artigo 17.º, n.º 2, estabelece que o direito de apagamento é exercido por quem a pessoa falecida haja designado para o efeito ou, na sua falta, pelos respectivos herdeiros.

Sobre o prazo de conservação de dados pessoais, o artigo 21,º, n.º 2, determina que, sendo esse prazo imposto por lei, o direito ao apagamento previsto no artigo 17.º do RGPD apenas pode ser exercido findo esse prazo.

Por seu lado, quando os dados pessoais estiverem publicados em jornal oficial, o direito ao apagamento tem natureza excepcional, apenas se podendo concretizar nas condições previstas no artigo 17.º do RGPD, quando essa for a única forma de acautelar o direito ao esquecimento e ponderados os demais interesses em presença.

Finalmente, o artigo 52.º tipifica o crime de desobediência, estabelecendo o nº 2, alínea b), que será punido com pena de prisão até dois anos ou com pena de multa até 240 dias, o agente que não proceder ao apagamento ou destruição dos dados, quando legalmente exigível, ou findo o prazo de conservação fixado na lei.

8. A NEGAÇÃO DO CARÁCTER EXTRATERRITORIAL DO DIREITO A SER ESQUECIDO[5]

I. O litígio que deu origem a este caso, desencadeou-se na sequência do Acórdão de Maio de 2014, anteriormente analisado, quando o Tribunal de Justiça da União Europeia determinou que os interessados podiam pedir aos motores de busca que removessem informação incorrecta, inadequada ou irrelevante sobre si e que constasse dos resultados apresentados pelas pesquisas dos internautas. Como a Google entendeu que a eficácia da decisão se confinava ao espaço comunitário, a autoridade francesa de protecção de dados – a Comissão Nacional de Informática e das Liberdades (CNIL) – exigiu que a operadora estendesse a supressão de referências a todas as extensões de nome do domínio do seu motor de busca. A Google recusou, limitando-se a instalar uma funcionalidade de bloqueio geográfico que impedia os internautas europeus de ver esses *links* listados. Em consequência, a CNIL impôs-lhe uma multa de 100 mil euros por esta se recusar a aplicar o direito ao esquecimento nas pesquisas fora do território europeu.

5 Acórdão do Tribunal de Justiça (Grande Secção), Acórdão Google LLC, sucessora da Google Inc./ Commission nationale de l'informatique et des libertés (CNIL), de 24 de Setembro de 2019 (C-507/17).

O Conselho de Estado francês considerou que o conflito suscitava dificuldades sérias de interpretação da Directiva 95/46, pelo que decidiu suspender a instância e submeter ao Tribunal de Justiça da União Europeia as seguintes questões prejudiciais:

1) Deve o "direito à [supressão de referências] ", como consagrado pelo [Tribunal de Justiça] no seu Acórdão de 13 de maio de 2014, [Google Spain e Google (C-131/12, EU:C:2014:317),] com fundamento nas disposições dos artigos 12.°, alínea b), e 14.°, [primeiro parágrafo,] alínea a), da [D]iretiva [95/46], ser interpretado no sentido de que o operador de um motor de busca é obrigado, quando acolhe um pedido de [supressão de referências] de uma hiperligação, a efectuar essa [supressão de referências] em todos os nomes de domínio do seu motor, de forma a que as [híper]ligações controvertidas deixem de ser exibidas, seja qual for o local a partir do qual é efectuada a pesquisa com base no nome do requerente, incluindo fora do âmbito de aplicação territorial da [Directiva [95/46]?

2) Em caso de resposta negativa a esta primeira questão, deve o "direito à [supressão de referências] ", como consagrado pelo [Tribunal de Justiça] no seu acórdão *supra* referido, ser interpretado no sentido de que o operador de um motor de busca apenas é obrigado, quando acolhe um pedido de supressão de uma hiperligação, a suprimir as [híper] ligações controvertidas dos resultados exibidos na sequência de uma pesquisa efectuada a partir do nome do requerente no nome de domínio correspondente ao Estado onde se considere que o pedido foi efectuado ou, de forma mais genérica, nos nomes de domínio do motor de busca que correspondem às extensões nacionais desse motor para todos os Estados-Membros [...]?

3) Além disso, em complemento da obrigação invocada na segunda questão, deve o "direito à [supressão de referências] ", como consagrado pelo [Tribunal de Justiça] no seu acórdão *supra* referido, ser interpretado no sentido de que o operador de um motor de busca, quando acolhe um pedido de [supressão de referências] de uma hiperligação, é obrigado, através da técnica designada "bloqueio geográfico", a partir de um endereço IP supostamente localizado no Estado de residência do beneficiário do "direito à [supressão de referências] ", a suprimir os resultados controvertidos das pesquisas efectuadas a partir do seu nome, ou mesmo, de forma mais genérica, a partir de um endereço IP supostamente localizado num dos Estados-Membros aos quais se aplica a [Directiva [95/46], independentemente do nome de domínio utilizado pelo internauta que efectue a busca?»

Embora na data em que o pedido de decisão prejudicial deu entrada fosse aplicável a Directiva 95/46, esta foi revogada com efeitos a partir de 25 de maio de M2018, data a partir da qual o Regulamento 2016/679 passou a vigorar. O Tribunal examinou as questões colocadas sob a perspectiva tanto desta Directiva como do Regulamento, para garantir que as suas

respostas serão, em qualquer hipótese, úteis para o órgão jurisdicional de reenvio. Deste modo, as questões colocadas visavam, em substância, saber se o artigo 12.°, alínea b), e o artigo 14.°, primeiro parágrafo, alínea a), da Directiva 95/46, bem como o artigo 17.°, n.º 1, do Regulamento 2016/679, devem ser interpretados no sentido de que, quando aceita um pedido de supressão de referências ao abrigo destas disposições, o operador de um motor de busca tem de efectuar essa supressão de referências em todas as versões do seu motor ou se, pelo contrário, só tem de efectuar essa supressão de referências nas versões que correspondem a todos os Estados-Membros, ou mesmo, apenas, na versão que corresponde ao Estado-Membro no qual o pedido de supressão de referências foi apresentado, se for caso disso, em conjugação com o recurso à técnica dita de «bloqueio geográfico» para garantir que um internauta não possa, independentemente da versão nacional do motor de busca utilizado, aceder, no âmbito de uma pesquisa efectuada a partir de um endereço IP supostamente localizado no Estado-Membro de residência do titular do direito à supressão de referências ou, de forma mais ampla, num Estado-Membro, às hiperligações abrangidas pela supressão de referências.

O Tribunal entendeu que resultava do considerando 10 da Directiva 95/46 e dos considerandos 10, 11 e 13 do Regulamento 2016/679, cuja adopção se baseou no artigo 16.° TFUE, que esta directiva e este regulamento têm por objectivo garantir um elevado nível de protecção dos dados pessoais em toda a União. Considerou, em seguida que, "num mundo globalizado, o acesso dos internautas, designadamente dos que se encontram fora da União, às referências a dados pessoais de uma hiperligação que remetem para informações sobre uma pessoa cujo centro de interesses se situa na União, é, assim, susceptível de produzir sobre esta efeitos imediatos e substanciais dentro da própria União".

Em contrapartida, sublinhou que em numerosos Estados terceiros o direito à supressão de referências não existe ou é objecto de uma abordagem diferente e, por outro lado, o direito à protecção dos dados pessoais não era um direito absoluto, devendo ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade [v., neste sentido, Acórdão de 9 de Novembro de 2010, Volker und Markus Schecke e Eifert, C-92/09 e C-93/09, EU:C:2010:662, n.° 48, e Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de Julho de 2017, EU:C:2017:592, n.º 136]. Acresce que o equilíbrio entre o direito ao respeito pela vida privada e à protecção dos dados pessoais, por um lado, e a liberdade de informação dos internautas, por outro, pode variar de forma considerável no mundo.

Adiante observou que, embora o legislador da União tivesse, no artigo 17.°, n.º 3, alínea a), do Regulamento 2016/679, procedido a uma ponderação entre este direito e esta liberdade

no que respeita à União, importava constatar que, em contrapartida, não procedeu, na fase actual das coisas, a semelhante ponderação no que respeitava ao âmbito de uma supressão de referências fora da União. "Em especial, não resulta de modo nenhum da redacção do artigo 12.°, alínea b), e do artigo 14.°, primeiro parágrafo, alínea a), da Directiva 95/46 ou do artigo 17.° do Regulamento 2016/679 que, para garantir a realização do objectivo mencionado no n.º 54 do presente acórdão, o legislador da União optou por conferir aos direitos consagrados nestas disposições um âmbito que excede o território dos Estados-Membros e que pretendeu impor a um operador que, como a Google, é abrangido pelo âmbito de aplicação desta directiva ou deste regulamento, uma obrigação de supressão de referências que também abrange as versões nacionais do seu motor de busca que não correspondem aos Estados-Membros".

Daqui resulta que, actualmente, não existe, para o operador de um motor de busca que aceita um pedido de supressão de referências uma obrigação que decorre do direito da União de proceder a essa supressão de referências em todas as versões do seu motor. Atendendo a todas estas considerações, o operador de um motor de busca não pode ser obrigado, ao abrigo do artigo 12.°, alínea b), e do artigo 14.°, primeiro parágrafo, alínea a), da Directiva 95/46, bem como do artigo 17.°, n.º 1, do Regulamento 2016/679, a efectuar uma supressão de referências em todas as versões do seu motor.

No que respeita à questão de saber se essa supressão de referências deve ser efectuada nas versões do motor de busca que correspondem aos Estados-Membros ou apenas na versão desse motor que corresponde ao Estado-Membro de residência do beneficiário da supressão de referências, resulta nomeadamente do facto de o legislador da União ter optado por fixar as regras em matéria de protecção de dados por via de um regulamento, que é directamente aplicável em todos os Estados-Membros, fazendo-o, como sublinha o considerando 10 do Regulamento 2016/679, a fim de assegurar um nível de protecção coerente e elevado em toda a União e eliminar os obstáculos à circulação de dados na União, que, em princípio, a supressão de referências em causa deve ser efectuada para todos os Estados-Membros.

II. Em termos de análise final, a decisão tomada pelo TJUE representou o triunfo da liberdade de expressão a nível global, que estaria claramente ameaçada caso os Tribunais ou as autoridades de protecção de dados de qualquer país comunitário tivessem poder para determinar os resultados de pesquisa a que os utilizadores da internet nos EUA, Paquistão ou Brasil pudessem aceder.

DIREITO APLICÁVEL À PROTEÇÃO DE DADOS PESSOAIS NA INTERNET: ALGUNS ASPETOS DE DIREITO INTERNACIONAL PRIVADO

LUÍS DE LIMA PINHEIRO [1]

1Professor Catedrático da Faculdade de Direito da Universidade de Lisboa.
O presente estudo representa o desenvolvimento da comunicação apresentada no Curso de Pós-Graduação sobre Direito do Ciberespaço, organizado pelo Instituto de Ciências Jurídico-Políticas e pelo CIJIC da Faculdade de Direito da Universidade de Lisboa.

RESUMO

A privacidade é um valor tutelado pela generalidade dos sistemas jurídicos democráticos, mas há diferenças importantes quanto ao conteúdo e à extensão desta proteção, bem como, em particular, quanto à sua conciliação com a liberdade de expressão e informação. Estas diferenças manifestam-se, designadamente, quanto à proteção de dados pessoais.

Na ordem jurídica portuguesa, a proteção dos dados pessoais constitui um direito fundamental, que não só resulta da concretização do direito à privacidade como também é, em certa medida, autonomizado.

Não cabendo examinar neste estudo a controvérsia suscitada por certas soluções materiais, pode afirmar-se que a vasta uniformização do Direito material aplicável à proteção de dados pessoais na UE é, em princípio, justificada. No entanto, o âmbito espacial de aplicação do RGPD parece demasiado amplo, não assegurando que existe sempre uma ligação significativa com a União Europeia.

Palavras-Chave: Dados pessoais; Privacidade; direitos fundamentais; direitos de personalidade; CRP; RGPD; União Europeia.

2. INTRODUÇÃO

Os *dados pessoais* são informações relativas a uma pessoa singular identificada ou identificável, por exemplo, nome, número de identificação, endereço postal ou de correio eletrónico ou qualquer elemento específico da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular ([1]).

A privacidade é um valor tutelado pela generalidade dos sistemas jurídicos democráticos, mas há diferenças importantes quanto ao conteúdo e à extensão desta proteção, bem como, em particular, quanto à sua conciliação com a liberdade de expressão e informação. Estas diferenças manifestam-se, designadamente, quanto à proteção de dados pessoais ([2]).

Em situações com contactos relevantes com mais de um Estado (situações transnacionais), a proteção de dados pessoais coloca um problema de determinação do Direito aplicável. O Direito aplicável tanto pode ser uma lei estadual, como um instrumento supraestadual, que unifique ou uniformize o regime aplicável nos Estados por ele vinculados.

Na ordem jurídica portuguesa, *a proteção dos dados pessoais constitui um direito fundamental*, que não só resulta da concretização do direito à privacidade como também é, em certa medida, autonomizado.

A Constituição portuguesa consagra o direito à reserva da intimidade da vida privada no art. 26.º/1 e determina que a lei estabelecerá garantias efetivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas (art. 26.º/2). A Constituição autonomiza o direito à proteção de dados pessoais informatizados no art. 35.º. Por seu turno, o art. 37.º consagra *a liberdade de expressão e informação*, incluindo o direito de informar, de se informar e de ser informado, sem impedimentos nem discriminações. Todos estes direitos podem ser vistos como projeções da dignidade da pessoa humana ([3]).

Também a Convenção Europeia dos Direitos do Homem protege o direito ao respeito pela vida privada e familiar (art. 8.º) e a liberdade de expressão (art. 10.º) que tem, entre

1 - Ver definição contida no art. 4.º/1 do Regulamento Geral sobre a Proteção de Dados.
2 - Ver Paul SCHWARTZ e Karl-Nicolaus PEIFER – "Transatlantic Data Privacy", *LSN Cyberspace Law eJournal, Vol. 22 No. 85, 11/22/2017* (acessível em SSRN), 121 e segs.
3 - Ver JORGE MIRANDA – *Direitos Fundamentais*, 2.ª ed., Coimbra, Almedina, 2017, 233-234.

outras, como concretizações a liberdade de imprensa e o direito à informação. A jurisprudência do Tribunal Europeu dos Direitos do Homem não parece fornecer indicações inteiramente claras sobre o modo de ponderar estes direitos ([4]), dependendo das circunstâncias do caso qual dos direitos deve prevalecer ([5]).

A nível da UE, o direito à proteção dos dados de caráter pessoal está consagrado no Tratado sobre o Funcionamento da União Europeia (art. 16.º/1) e na Carta dos Direitos Fundamentais da União Europeia. Esta Carta, além de consagrar o direito ao respeito pela vida privada e familiar (art. 7.º), autonomiza o direito à proteção dos dados pessoais no art. 8.º. Esta disposição determina, designadamente, que os dados pessoais devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei (n.º 2).

A liberdade de expressão e de informação também está consagrada na Carta (art. 11.º).

As restrições aos direitos fundamentais reconhecidos na Carta, designadamente no caso de conflitos de direitos, têm de respeitar o princípio da proporcionalidade (art. 52.º/1): "Qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela presente Carta deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades. Na observância do princípio da proporcionalidade, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros".

A UE considerou necessário harmonizar as leis dos Estados-Membros em matéria de proteção de dados pessoais através da *Diretiva 95/46/CE* que foi transposta para a ordem jurídica portuguesa pela *Lei da Proteção de Dados Pessoais* (Lei n.º 67/98, de 26/10).

Esta Diretiva apenas aproximou as legislações dos Estados-Membros e, por conseguinte continha no art. 4.º/1 uma norma sobre o âmbito de aplicação no espaço da legislação de transposição da Diretiva de cada Estado-Membro ([6]), que foi transposta para o n.º 3 do artigo

4 - Ver Fomperosa RIVERO – "Right to Be Forgotten in the European Court of Justice Google Spain Case: The Right Balance of Privacy Rights, Procedure, and Extraterritoriality", *LSN Cyberspace Law eJournal, Vol. 22 No. 19, 03/15/2017* (acessível em SSRN), 22.

5 - Ver Stefan KULK e Frederik Borgesius – "Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe", *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal, Vol. 4 No. 13, 03/09/2017* (acessível em SSRN), 7 e segs.

6 - "1. Cada Estado-membro aplicará as suas disposições nacionais adoptadas por força da presente directiva ao tratamento de dados pessoais quando:
a) O tratamento for efectuado no contexto das actividades de um estabelecimento do responsável pelo tratamento situado no território desse Estado-membro; se o mesmo responsável pelo tratamento estiver estabelecido no território de vários Estados-membros, deverá tomar as medidas necessárias para garantir que cada um desses estabelecimentos cumpra as obrigações estabelecidas no direito nacional que lhe for aplicável;

4.º da Lei de Proteção de Dados Pessoais em termos que não correspondem inteiramente ao disposto na Diretiva, mas que devem ser entendidos no mesmo sentido segundo uma interpretação conforme à Diretiva ([7]).

Das normas de conexão *ad hoc* contidas nesta lei resultava a aplicação das suas normas materiais em matérias que, por dizerem respeito a direitos de personalidade de estrangeiros, são pelo Direito de Conflitos geral submetidas à lei estrangeira, em termos que são adiante referidos. Estas normas materiais eram, por conseguinte, *suscetíveis de aplicação necessária* ([8]).

O Reg. (UE) n.º 2016/679, Relativo à Proteção das Pessoas Singulares no que diz Respeito ao Tratamento de Dados Pessoais e à Livre Circulação desses Dados (*Regulamento Geral sobre a Proteção de Dados*, doravante RGPD) veio estabelecer um desenvolvido complexo de regras materiais uniformes sobre a proteção de dados pessoais.

O RGPD aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados (art. 2.º/1). São excluídos alguns tratamentos de dados pessoais, designadamente o efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas (n.º 2/c) ([9]).

O RGPD abrange por isso, designadamente, o tratamento de dados pessoais por fornecedores de bens e serviços na internet.

O RGPD visa não só a proteção de dados pessoais de pessoas singulares, mas também assegurar a livre circulação desses dados no interior da União (art. 1.º) ([10]).

---

b) O responsável pelo tratamento não estiver estabelecido no território do Estado-membro, mas num local onde a sua legislação nacional seja aplicável por força do direito internacional público;
c) O responsável pelo tratamento não estiver estabelecido no território da Comunidade e recorrer, para tratamento de dados pessoais, a meios, automatizados ou não, situados no território desse Estado-membro, salvo se esses meios só forem utilizados para trânsito no território da Comunidade."

7 - O art. 4.º contém um n.º 4, segundo o qual a "lei aplica-se à videovigilância e outras formas de captação, tratamento e difusão de sons e imagens que permitam identificar pessoas sempre que o responsável pelo tratamento esteja domiciliado ou sedeado em Portugal ou utilize um fornecedor de acesso a redes informáticas e telemáticas estabelecido em território português."

8 - Sobre o conceito de norma suscetível de aplicação necessária, ver Luís de LIMA PINHEIRO – *Direito Internacional Privado*, vol. I – *Introdução e Direito de Conflitos – Parte Geral*, 3.ª ed., Coimbra, Almedina, 270 e segs.

9 - Segundo o Considerando n.º 18, as atividades pessoais ou domésticas poderão incluir a troca de correspondência e a conservação de listas de endereços ou a atividade das redes sociais e do ambiente eletrónico no âmbito dessas atividades. Todavia, o RGPD é aplicável aos responsáveis pelo tratamento e aos subcontratantes que forneçam os meios para o tratamento dos dados pessoais dessas atividades pessoais ou domésticas.

10 - O Considerando n. º 2 relaciona estes objetivos com o objetivo mais geral de contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social, a

O art. 2.º/4 determina que o RGPD não prejudica a aplicação da Diretiva 2000/31/CE (*Diretiva sobre comércio eletrónico*) nomeadamente as normas que limitam a responsabilidade dos prestadores intermediários de serviços nos casos de simples transporte, armazenagem temporária [*caching*] e armazenagem em servidor e estabelecem a ausência de dever geral de vigilância. Mas isto não significa que o regime do RGPD não seja aplicável à proteção de dados pessoais no contexto de serviços da sociedade de informação, até porque essa Diretiva salvaguarda a aplicação plena da legislação europeia sobre proteção de dados pessoais aos serviços da sociedade da informação (Considerando n.º 14) e exclui do seu âmbito de aplicação as questões respeitantes aos serviços da sociedade da informação abrangidas pelo regime europeu da proteção de dados pessoais (art. 1.º/5/b) ([11]).

Já o funcionamento do Direito de Conflitos interno em matéria de responsabilidade extracontratual é limitado pela interpretação dessa Diretiva feita pelo TUE no caso *eDate Advertising,* visto que a matéria parece ser abrangida pelo domínio coordenado (art. 2.º/h/i) ([12]).

De entre *as definições oferecidas pelo art 4.º* importa salientar as de "dados pessoais", já referida, "tratamento", "consentimento" e, mais adiante (II), a de "Estabelecimento principal".

Entende-se por "Tratamento" uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição (2).

Entende-se por "Consentimento" do titular de dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de

---

consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares.

11 - Em sentido diferente, Daphne KELLER – "The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation", *LSN Cyberspace Law eJournal, Vol. 22 No. 19, 03/15/2017* (acessível em SSRN), 66 e segs.

12 - Ver também Pedro MIGUEL ASENSIO – "Competencia y Derecho aplicable en el reglamento general sobre protección de datos de la Unión Europea", *Rev. Española de Derecho Internacional* 69 (2017) 75-108, 106.

tratamento (11). Esta definição torna claro que o conceito de consentimento relevante para o Regulamento é autónomo e não depende da lei reguladora do contrato ([13]).

No célebre caso *Google* (2014) ([14]), o TUE entendeu que o artigo 2º/b e d da Diretiva 95/46/CE, deve ser interpretado no sentido de que, por um lado, a atividade de um motor de busca que consiste em encontrar informações publicadas ou inseridas na Internet por terceiros, indexá-las automaticamente, armazená-las temporariamente e, por último, pô-las à disposição dos internautas por determinada ordem de preferência deve ser qualificada de "tratamento de dados pessoais", na aceção do artigo 2.º/b, quando essas informações contenham dados pessoais, e de que, por outro, o operador desse motor de busca deve ser considerado "responsável" pelo dito tratamento, na aceção do referido artigo 2º/d.

No caso *Wirtschaftsakademie Schleswig-Holstein* (2018) ([15]), o mesmo tribunal interpretou o artigo 2.º/d da mesma Diretiva no sentido de que o conceito de "responsável pelo tratamento" engloba o administrador de uma página de fãs alojada no *Facebook*.

O RGPD também estabelece um *regime de Direito material especial sobre a transferência de dados para Estados terceiros e organizações internacionais*.

O RGPD contém ainda *inúmeras remissões para o Direito dos Estados-Membros*, que constituem em alguns casos normas de conflitos unificadas, *algumas normas de competência internacional* e uma *norma que limita o reconhecimento de decisões judiciais e administrativas de Estados terceiros*.

O RGPD revogou a Diretiva 95/46/CE com efeitos a partir de 25 de maio de 2018 ([16]).

O legislador europeu entendeu que sendo a proteção dos dados pessoais um direito fundamental e tendo a rápida evolução tecnológica e a globalização um impacto nesta matéria se tornou necessário assegurar um nível de proteção coerente e elevado das pessoas singulares e eliminar os obstáculos à circulação de dados pessoais na União através de uma uniformização das principais regras materiais na matéria ([17]).

---

13 - Ver Christian KOHLER – "Conflict of Law Issues in the 2016 Data protection Regulation of the European Union", *RDIPP* (2016) 653-675, 663 e segs.

14 - 13/5/2014 [ECLI:EU:C:2014:317].

15 - TUE 5/6/2018 [ECLI:EU:C:2018:388].

16 - Ver também art. 99.º/2.

17 - Cf. Considerandos n.ºs 1, 6 e 10. RGPD começa por recordar, no seu Considerando n.º 1, que a proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. O Considerando n.º 6 assinala o impacto da rápida evolução tecnológica e da globalização em matéria de proteção de dados pessoais:

- aumento significativo da recolha e da partilha de dados pessoais;
- a utilização de dados pessoais numa escala sem precedentes no exercício das atividades das empresas privadas e das entidades públicas;

Quer isto dizer que não se trata agora apenas de aproximar as legislações dos Estados-Membros, em termos que não dispensam a determinação do Direito estadual aplicável, mas de estabelecer um regime europeu uniforme. E esta uniformidade significa que o mesmo regime passa a ser aplicável às situações internas e às situações transnacionais, contrapondo-se assim a uma mera unificação do regime aplicável a situações transnacionais.

Com isto não se eliminam os problemas de determinação do Direito aplicável. Estes problemas colocam-se principalmente a três níveis. Primeiro, *a determinação do âmbito espacial de aplicação do RGPD* (I). Segundo, *a determinação do Direito aplicável quando o RGPD remete para o Direito dos Estados-Membros* (II). Terceiro, *a determinação do Direito estadual aplicável a questões que o RGPD não regula* (III), ainda que por forma remissiva, como, designadamente, se passa com a maior parte das questões relativas à responsabilidade extracontratual por violação das disposições do RGPD.

O tema do presente estudo abrange estes três problemas. Mas trata-se, inevitavelmente, de uma primeira aproximação a este tema uma vez que este abrange questões que são muito vastas, complexas e controversas e que, em alguns casos, só muito recentemente começaram a ser estudadas.

Fica, em princípio, excluído do âmbito do presente trabalho o problema dos limites colocados pelo Direito Internacional Público às competências legislativa, jurisdicional e de execução dos Estados, sem prejuízo de alusões pontuais suscitadas por certas soluções legislativas ou jurisprudenciais.

- crescente disponibilização das informações pessoais de uma forma pública e global.

O mesmo Considerando afirma que as novas tecnologias devem contribuir para facilitar a livre circulação de dados pessoais na União e a sua transferência para países terceiros e organizações internacionais, assegurando simultaneamente um elevado nível de proteção dos dados pessoais.

Nos termos do Considerando n.º 10, a fim de assegurar um nível de proteção coerente e elevado das pessoas singulares e eliminar os obstáculos à circulação de dados pessoais na União, o nível de proteção dos direitos e liberdades das pessoas singulares relativamente ao tratamento desses dados deverá ser equivalente em todos os Estados-Membros.

I. ÂMBITO ESPACIAL DE APLICAÇÃO DO RGPD

Quanto ao âmbito espacial de aplicação, o art. 3.º/1 começa por determinar que o RGPD se aplica *ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União*, independentemente de o tratamento ocorrer dentro ou fora da União.

As principais questões suscitadas pela interpretação deste preceito dizem respeito ao sentido da expressão "contexto das atividades" e do termo "estabelecimento".

Estas questões também se colocavam perante a Dir. 95/46/CE e foram objeto de decisões do TUE, mormente nos casos *Google*, *Weltimmo*, *Verein für Konsumenteninformation* e *Wirtschaftsakademie Schleswig-Holstein*.

Segundo o Considerando n.º 22 do RGPD, o *estabelecimento* pressupõe o exercício efetivo e real de uma atividade com base numa instalação estável e a forma jurídica de tal estabelecimento, quer se trate de uma sucursal quer de uma filial com personalidade jurídica, não é fator determinante nesse contexto.

O alcance da afirmação de que o tratamento pode ser considerado como inserido no contexto das atividades de um estabelecimento situado na União, mesmo que o tratamento em si não seja realizado na União, é ilustrado pela decisão proferida no já referido caso *Google* sobre o direito de apagamento ([18]).

Segundo o parecer que tinha sido elaborado pelo Grupo de Proteção das Pessoas no que diz respeito ao tratamento de dados pessoais instituído nos termos do art. 29.º da Diretiva, a noção de "contexto das atividades" implica que é aplicável a lei do Estado-Membro onde um estabelecimento do responsável de tratamento está envolvido em atividades relacionadas com o tratamento de dados ([19]). O TUE, porém, entendeu que bastava que a *Google* tivesse uma filial que realizava atividade publicitária do grupo *Google* na Espanha, mas não processava dados, para que se aplicasse o regime espanhol harmonizado pela Diretiva e condenou a

18 - 13/5/2014 [ECLI:EU:C:2014:317].

19 - Parecer n.º 8/2010, 12-14. Posteriormente o Grupo atualizou o parecer tendo em conta a decisão do TUE. Ver também, em sentido crítico, Maja BRKAN – "Data Protection and European Private International Law", *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal, Vol. 2 No. 43, 07/28/2015* (acessível em SSRN), 32.

Google Spain e a *Google Inc* a suprimir os dados pessoais de um nacional espanhol nos resultados do motor de busca ([20]).

No caso *Wirtschaftsakademie Schleswig-Holstein* (2018) ([21]), o TUE reafirmou, relativamente ao *Facebook*, a aplicabilidade do Direito do Estado-Membro em que está situado um estabelecimento que realiza uma atividade publicitária mesmo que o tratamento dos dados pessoais seja feito conjuntamente por estabelecimentos situados num Estado terceiro e noutro Estado-Membro ([22]).

---

20 - Neste caso, o TUE foi confrontado com questões relativas a uma reclamação feita por um nacional espanhol domiciliado em Espanha, contra o editor de um jornal espanhol, a *Google Spain* e a *Google Inc.*, baseada no facto de que, quando um utilizador da internet inseria o nome dessa pessoa motor de busca do grupo *Google* obtinha ligações a duas páginas do jornal, nas quais figurava um anúncio de uma venda de imóveis em hasta pública decorrente de um arresto com vista à recuperação de dívidas à Segurança Social, que mencionava o nome dessa pessoa. A pessoa pedia designadamente que a *Google Spain* ou a *Google Inc.* suprimissem ou ocultassem os seus dados pessoais, para que deixassem de aparecer nos resultados de pesquisa e de figurar nas ligações do jornal.
O TUE interpretou o art. 4.º/1/a da Diretiva 95/46 no sentido de que é efetuado um tratamento de dados pessoais no contexto das atividades de um estabelecimento do responsável por esse tratamento no território de um Estado-Membro, na aceção desta disposição, quando o operador de um motor de busca cria num Estado-Membro uma sucursal ou uma filial destinada a assegurar a promoção e a venda dos espaços publicitários propostos por esse motor de busca, cuja atividade é dirigida aos habitantes desse Estado-Membro.
A *Google Spain* e a *Google Inc.* tinham argumentado que o tratamento de dados pessoais em causa no processo é efetuado exclusivamente pela *Google Inc.*, que explora o *Google Search* sem intervenção alguma da *Google Spain*, cuja atividade se limita a fornecer apoio à atividade publicitária do grupo Google que é distinta do seu serviço de motor de busca.
O TUE contrapôs que resulta designadamente dos considerandos 18 a 20 e do artigo 4.º da Diretiva 95/46 que o legislador da União pretendeu evitar que uma pessoa seja privada da proteção garantida por essa diretiva e que essa proteção seja contornada, estabelecendo um âmbito de aplicação particularmente amplo e que, a esta luz, é suficiente para essa aplicação que as atividades do operador do motor de busca e as do seu estabelecimento situado no Estado-Membro em causa estejam "indissociavelmente ligadas, uma vez que as atividades relativas aos espaços publicitários constituem o meio para tornar o motor de busca em causa economicamente rentável e que esse motor é, ao mesmo tempo, o meio que permite realizar essas atividades" (n.ºs. 54 e 56).
Segundo Geert van CALSTER – "Regulating the Internet. Prescriptive and Jurisdictional Boundaries to the EU's 'Right to Be Forgotten', *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal, Vol. 2 No. 64, 11/12/2015* (acessível em SSRN), 24, referindo RYNGAERT no mesmo sentido, o TUE ter-se-á baseado tecnicamente no critério dos efeitos para justificar a competência do TUE relativamente à situação. Em rigor, porém, o problema não é só de competência jurisdicional e de competência de execução, porque estava em causa o âmbito de aplicação no espaço do regime contido na Diretiva e, por conseguinte, também um problema de competência legislativa da UE. CALSTER, op. cit., 25 e segs., chama atenção para o facto de que a competência legislativa e jurisdicional não é necessariamente acompanhada pela competência de execução e que o TUE não tem competência de execução relativamente ao *site Google.com*. Mas a competência de execução refere-se ao poder de praticar atos de coerção material. Este poder, mesmo no contexto da internet, está em princípio limitado ao território do Estado do foro (cf. *Tallinn Manual 2.0 International Group of Experts and Other Participants*, General Editor Michael Schmitt, Cambridge, Cambridge University Press, 2017, *Rule* 11). Por conseguinte, se a Diretiva puder se aplicada e se houver uma ligação significativa com a UE, o tribunal de um Estado-Membro pode condenar a sociedade-mãe *Google* a suprimir determinados dados, mas não pode praticar atos de coerção material relativamente à sociedade-mãe *Google*. Em sentido diferente, Danial NADEEM – "Territorial Limits to the European Union's Right to be Forgotten: How the CNIL Ignores Jurisdictional Basics in Its March 10, 2016 Decision Against Google", *Creighton Int'l & Comp. L.J.* 8 (2017) 182-199, 191 e segs.; e Dawn NUNZIATO – "The Fourth Year of Forgetting: The Troubling Expansion of the Right to Be Forgotten", *LSN Cyberspace Law eJournal, Vol. 23 No. 49, 07/16/2018* (acessível em SSRN), n.º 4.
21 - TUE 5/6/2018 [ECLI:EU:C:2018:388].
22 - N.ºs 57 e segs. Na mesma decisão, o TUE entendeu que autoridade de controlo desse Estado-Membro é competente para apreciar, de maneira autónoma em relação à autoridade de controlo do Estado-Membro em que está estabelecido o responsável pelo tratamento que violou as regras de proteção dos dados, a legalidade de tal

Penso que a compatibilidade desta solução com os limites colocados pelo Direito Internacional Público à competência legislativa e jurisdicional dos Estados, quando não se exija que o titular de dados seja nacional ou residente no Estado em causa, é duvidosa.

Por outro lado, resulta da decisão no caso *Verein für Konsumenteninformation* que a circunstância de a empresa responsável pelo tratamento de dados não ter filial nem sucursal num Estado-Membro não exclui que possa ter aí um estabelecimento, mas tal estabelecimento não pode existir pelo simples facto de o sítio internet da empresa em questão ser acessível nesse Estado-Membro ([23]).

Nos termos do art. 3.º/2, *o RGPD também se aplica ao tratamento de dados pessoais de titulares que residam no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União*, quando as atividades de tratamento estejam relacionadas com:

- a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento;

- b) O controlo do seu comportamento, desde que esse comportamento tenha lugar na União.

Aparentemente esta norma não está em sintonia com o Considerando n.º 2, retomado pelo Considerando n.º 14, que afirma que os "princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais".

---

tratamento de dados e pode exercer os seus poderes de intervenção em relação ao ente estabelecido no seu território sem ter de solicitar previamente a intervenção da autoridade de controlo do outro Estado-Membro (n.º 74).

23 - TUE 28/7/2016 [ECLI:EU:C:2016:612], n.º 76. Por conseguinte, importa avaliar tanto o grau de estabilidade da instalação como a realidade do exercício das atividades no Estado-Membro em questão (n.º 77, reafirmando decisão no caso *Weltimmo*, TUE 1/10/2015 [EU:C:2015:639], n.° 29). Quanto à questão de saber se o tratamento de dados pessoais em causa é efetuado "no contexto das atividades" desse estabelecimento, na aceção do artigo 4.°/1/a), da Diretiva 95/46, o TUE também reafirmou decisão no caso *Weltimmo* (n.º 35), assinalando que esta disposição exige que o tratamento de dados pessoais em questão seja efetuado não "pelo" próprio estabelecimento em causa, mas apenas "no contexto das atividades" (n.º 78). Nesta mesma decisão foi entendido que o artigo 4.°/1/a da Dir. 95/46/CE deve ser interpretado no sentido de que o tratamento de dados pessoais efetuado por uma empresa de comércio eletrónico é regido pelo Direito do Estado-Membro a que se destinam as atividades dessa empresa, se se constatar que essa empresa procede ao tratamento dos dados em questão no contexto das atividades de um estabelecimento situado nesse Estado-Membro. Este Estado-Membro é aquele em que se situa o estabelecimento (n.º 74). O TUE reafirma ainda o entendimento, adotado no caso *Weltimmo*, que o conceito de "estabelecimento" na aceção do artigo 4.°/1/a, da Dir. 95/46, abrange qualquer atividade real e efetiva, ainda que mínima, exercida através de uma instalação estável (n.º 75).

Há, no entanto, a registar uma divergência entre as várias versões linguísticas do RGPD a este respeito. Enquanto as versões portuguesa e espanhola se referem a titulares que residam na União ["titulares residentes no território da União", "*interesados que residan en la Unión*"], as versões inglesa, francesa, alemã e italiana referem-se a titulares que se encontrem na União ["*who are in the Union*", "*personnes concernées qui se trouvent sur le territoire de l'Union*","*betroffenen Personen, die sich in der Union befinden*", "*interessati che si trovano nell'Unione*"]. Tendo em conta que a Proposta de Regulamento nestas versões linguísticas se referia à residência, e que esta referência foi afastada, e o Considerando n.º 14, é forçoso concluir que basta que os titulares se encontrem no território da União no momento em que os bens ou serviços são oferecidos ou que o comportamento é controlado, o que não garante a existência de uma ligação significativa com a União ([24]).

Estender o âmbito de aplicação do RGPD a casos em que nem o responsável pelo tratamento ou o subcontratante estão estabelecidos na União nem o titular dos dados é nacional ou residente na União, porém, constitui uma solução de duvidosa compatibilidade com os limites colocados pelo Direito Internacional Público à competência legislativa dos Estados. *A tutela do direito à proteção dos dados pessoais pelo Direito da União deve fundamentar-se numa ligação significativa com a União*.

Em todo o caso, importa sublinhar que o RGPD só se aplica ao tratamento efetuado por ente não estabelecido na União quando o titular dos dados se encontrar território da União e se verificar um dos dois pressupostos adicionais anteriormente referidos.

Segundo o Considerando n.º 23, a fim de determinar se o responsável pelo tratamento ou subcontratante oferece ou não bens ou serviços aos titulares dos dados que se encontrem na União, há que determinar em que medida é evidente a sua intenção de oferecer serviços a titulares de dados num ou mais Estados-Membros da União. O mero facto de estar disponível na União um sítio *web* do responsável pelo tratamento ou subcontratante ou de um intermediário, um endereço eletrónico ou outro tipo de contactos, ou de ser utilizada uma língua de uso corrente no país terceiro em que o referido responsável está estabelecido, não é suficiente para determinar a intenção acima referida, mas há fatores, como a utilização de uma língua ou de uma moeda de uso corrente num ou mais Estados-Membros, com a possibilidade de encomendar bens ou serviços nessa outra língua, ou a referência a clientes

24 - Em sentido diferente, MIGUEL ASENSIO, "Competencia y Derecho aplicable…", *loc. cit.*, 84-85.

ou utilizadores que se encontrem na União, que podem ser reveladores de que o responsável pelo tratamento tem a intenção de oferecer bens ou serviços a titulares de dados na União.

Este entendimento encontra-se próximo do critério da atividade dirigida tal como ele tem sido concretizado pela jurisprudência do TUE sobre o regime da competência internacional nos contratos com consumidores, designadamente a decisão proferida nos casos *Peter Pammer e Hotel Alpenhof* relativamente ao art. 15.º/1/c do Regulamento Bruxelas I ([25]).

Há, no entanto, diferenças, designadamente porque o regime especial de competência em matéria de contratos com consumidores, à semelhança da norma de conflitos especial sobre o Direito aplicável aos contratos com consumidores contida no Regulamento Roma I, pressupõe a celebração de um contrato, o que não é o caso do RGPD ([26]).

Por conseguinte, por um lado, não basta para a aplicação do RGPD que haja uma oferta de bens ou serviços num *site* da internet que possam ser adquiridos por titulares de dados que se encontram na União ([27]), sendo necessário demonstrar uma intenção de oferecer estes bens ou serviços a estes titulares. Por outro, porém, subsiste considerável incerteza sobre os indícios que podem ser considerados relevantes para demonstrar tal intenção e sobre o seu peso ([28]).

Segundo o Considerando n.º 24, a fim de determinar se uma atividade de tratamento pode ser considerada "controlo do comportamento" de titulares de dados, deverá determinar-se se essas pessoas são seguidas na internet e a potencial utilização subsequente de técnicas de tratamento de dados pessoais que consistem em definir o perfil de uma pessoa singular,

---

25 - Cf. TUE 7/12/2010, nos casos *Peter Pammer e Hotel Alpenhof* [*in* http://curia.europa.eu]. Ver também Daniel COOPER e Cristopher KUNER – "Data Protection Law and International Dispute Resolution", *RCADI* 382 (2015) 9-174 (publicado em 2017), 123-124.

26 Como observa MIGUEL ASENSIO, "Competencia y Derecho aplicable…", *loc. cit.*, 85.

27 - Como resultava da interpretação da Proposta de Regulamento feita por BRKAN, "Data Protection…", *loc. cit.*, 35.

28 - O art. 1.º/6 do Regulamento sobre Bloqueio Geográfico (Reg. (UE) 2018/302) determina que "não se pode considerar, apenas com base nos elementos a seguir indicados, que o comerciante dirige atividades para o Estado-Membro da residência habitual ou do domicílio do consumidor caso, ao agir em conformidade com os artigos 3.º, 4.º e 5.º do presente regulamento, não bloqueie nem limite o acesso dos consumidores a uma interface em linha, não redirecione os consumidores para uma interface em linha com base na nacionalidade ou no local de residência dos consumidores distinta da interface em linha a que os consumidores tenham tentado aceder inicialmente, não aplique condições gerais de acesso diferentes quando vende bens ou presta serviços nas situações previstas no presente regulamento, ou aceite instrumentos de pagamento emitidos noutro Estado-Membro numa base não discriminatória. Também não se pode considerar, apenas com base nesses elementos, que o comerciante dirige atividades para o Estado-Membro da residência habitual ou do domicílio do consumidor, caso preste informações e assistência ao consumidor após a celebração de um contrato resultante do cumprimento do presente regulamento pelo comerciante".

especialmente para tomar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e as suas atitudes.

BRKAN refere, relativamente à Proposta de Regulamento, que os elementos de interpretação não são conclusivos sobre o sentido que deve ser atribuído a este preceito: uma interpretação restrita, que abrange apenas as empresas estabelecidas em terceiros Estados que tratam a informação para fins económicos (como o *Google* e o *Facebook*), ou uma interpretação ampla, que abrangeria também o processamento de dados por autoridades públicas, como a NSA ([29]).

A este respeito, deve notar-se que o RGPD exclui a sua aplicação ao tratamento efetuado no exercício de atividades não sujeitas ao Direito da União (art. 2.º/2/a) ou efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública (art. 2.º/2/d).

Este pressuposto de aplicação do RGPD parece pensado principalmente para os casos em que a colocação de arquivos e programas informáticos no equipamento do utilizador que permitem o acesso a informação (como os *cookies*) não tem lugar no quadro da oferta de bens e serviços ([30]).

Os casos em que se justifica a aplicação do regime do RGPD apesar do tratamento não ser feito no território de um Estado-Membro estão, em princípio, abrangidos pelos critérios de conexão do art. 3.º/2, razão por que não se deveria manter a interpretação extensiva do "contexto de atividades" de um estabelecimento situado num Estado-Membro feita pelo TUE no caso *Google*.

É importante uma certa contenção no exercício de competências legislativas estaduais em relação à internet, uma vez que leis com um âmbito de aplicação no espaço muito vasto entram facilmente em conflito com leis de outros Estados, originando problemas de conflitos de deveres para os seus destinatários e de reconhecimento noutros Estados de decisões nelas baseadas ([31]).

---

29 - "Data Protection…", *loc. cit.*, 35-36.

30 - Neste sentido, MIGUEL ASENSIO, "Competencia y Derecho aplicable…", *loc. cit.*, 86. Ver ainda KELLER, "The Right Tools…", *loc. cit.*, 58.

31 - Ver as considerações de Christopher KUNER – "The Internet and the Global Reach of EU Law", *LSN Cyberspace Law eJournal, Vol. 22 No. 15, 03/01/2017* (acessível em SSRN), 32-33.

O art. 3.º/3 acrescenta que o RGPD se aplica ao tratamento de dados pessoais por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o Direito de um Estado-Membro por força do Direito Internacional Público.

O Direito de um Estado-Membro é aplicável por força do Direito internacional Público por exemplo numa missão diplomática ou num posto consular de um Estado-Membro (Considerando n.º 25).

O RGPD abandonou o critério de conexão estabelecido no art. 4.º/1/c da Diretiva sobre Proteção de Dados Pessoais – localização de meios para tratamento de dados pessoais, a meios, automatizados ou não, no território de um Estado-Membro, salvo se esses meios só forem utilizados para trânsito no território da Comunidade –, por se entender que este critério conduzia um âmbito de aplicação excessivo do regime europeu, incluindo casos que não têm uma ligação significativa com a UE ([32]).

32 - Ver MIGUEL ASENSIO, "Competencia y Derecho aplicable…", *loc. cit.*, 80-81.

II. DETERMINAÇÃO DO DIREITO APLICÁVEL QUANDO O RGPD REMETE PARA O DIREITO DOS ESTADOS-MEMBROS

O RGPD contém inúmeras remissões para o Direito dos Estados-Membros, que seria fastidioso enumerar aqui.

Em boa parte dos casos, *estas remissões são acompanhadas de uma norma de conflitos que atribui competência do Direito do Estado a que o responsável do tratamento ou o subcontratante estão sujeitos*.

É que se passa nos arts. 6.º/3, 14.º/5/c, 17.º/1/e /3/b, 22.º/2/b, 23.º/1, 26.º/1, 49.º/1/d e /4 e 85.º/2 (conjugado com o Considerando n.º 153).

O responsável pelo tratamento ou o subcontratante estão certamente sujeitos ao Direito do Estado em que estão estabelecidos. Mas suscitam-se dúvidas quando tenham uma pluralidade de estabelecimentos em diferentes Estados-Membros. O art. 4.º/16 contém uma definição de estabelecimento principal que é pelo menos relevante para determinar a autoridade de controlo principal. Segundo esta definição, no "que se refere a um responsável pelo tratamento com estabelecimentos em vários Estados-Membros, o local onde se encontra a sua administração central na União, a menos que as decisões sobre as finalidades e os meios de tratamento dos dados pessoais sejam tomadas noutro estabelecimento do responsável pelo tratamento na União e este último estabelecimento tenha competência para mandar executar tais decisões, sendo neste caso o estabelecimento que tiver tomado as referidas decisões considerado estabelecimento principal" ([33]).

Quando os dados sejam tratados por um estabelecimento secundário considera-se o ente sujeito ao Direito do Estado deste estabelecimento ou ao Direito do Estado de estabelecimento principal?

A favor da competência do Direito do Estado-Membro em que está situado o estabelecimento que trata os dados pode invocar-se o critério em princípio relevante para determinar o âmbito espacial de aplicação do RGPD (art. 3.º/1) e a decisão no caso *Weltimmo* ([34]), relativa ao Direito aplicável à proteção de dados nos termos da Dir. 95/46/CE. Em sentido

33 - Por acréscimo, no "que se refere a um subcontratante com estabelecimentos em vários Estados-Membros, o local onde se encontra a sua administração central na União ou, caso o subcontratante não tenha administração central na União, o estabelecimento do subcontratante na União onde são exercidas as principais atividades de tratamento no contexto das atividades de um estabelecimento do subcontratante, na medida em que se encontre sujeito a obrigações específicas nos termos do presente regulamento".
34 - *Supracit.*, n.ºs 24 e segs.

contrário, pode argumentar-se que o critério relevante para determinar a autoridade de controlo principal para o tratamento transfronteiriço é o do estabelecimento principal. Será desejável que o TUE esclareça o ponto.

Em alguns casos estabelecem-se *critérios de conexão diferentes*.

Assim, no que refere à atuação de membros ou pessoal da autoridade de controlo de um Estado-Membro noutro Estado-Membro, o RGPD determina a aplicação do Direito do Estado-Membro em que atuam, incluindo a responsabilidade por danos causados no decurso de tais atividades (art. 62.º/3 a 5).

Por outro lado, os dados pessoais que constem de documentos oficiais na posse de uma autoridade pública ou de um organismo público ou privado para a prossecução de atribuições de interesse público podem ser divulgados pela autoridade ou organismo nos termos do Direito da União ou do Estado-Membro que for aplicável à autoridade ou organismo público (art. 86.º).

Noutros casos, *a remissão não é acompanhada por um critério de conexão*. Nestes casos, cabe ao Direito interno dos Estados-Membros determinar o âmbito de aplicação da sua lei. Poderão fazê-lo mediante uma mera norma de conflitos unilateral *ad hoc*, i.e., que se limita a definir o âmbito espacial de aplicação das normas materiais em causa, ou, em princípio, formular normas de conflitos bilaterais, que tanto remetam para lei do foro como para a lei de outros Estados-Membros.

Não é inteiramente clara a razão por que, nestes casos, o RGPD não define o critério de conexão relevante. De todo o modo, parece que esta opção não preclude que os Estados-Membros utilizem o critério do estabelecimento do responsável do tratamento ou do subcontratante. No sentido do recurso a este critério, em matérias que digam respeito aos direitos e aos deveres destes entes, pesa o argumento da coerência sistemática com a solução favorecida pelo RGPD. Em sentido contrário, pode argumentar-se que se deveria aplicar uma lei com que os titulares dos dados tenham uma ligação especialmente estreita, visto que o RGPD tem como primeiro objetivo a proteção dos direitos dos titulares. Esta questão será retomada no ponto seguinte.

Já *a localização dos dados eletrónicos é problemática e não me parece constituir um elemento de conexão idóneo para o Direito Internacional Privado*, na determinação do Direito aplicável à proteção de dados pessoais ([35]).

Os dados pessoais são informações, e as informações são criações do espírito e não coisas corpóreas. Os dados, enquanto tais, não têm uma localização física; o que tem uma localização física são os seus suportes materiais. Os dados pessoais eletrónicos podem ser inscritos em diversos suportes, designadamente servidores e discos rígidos de computadores pessoais. No caso dos dados pessoais tratados por empresas, a tendência atual é para estarem armazenados ao abrigo da prestação de serviços de *cloud computing*. Não só o lugar de armazenamento dos ficheiros que contêm esses dados pode resultar de opções meramente técnicas das empresas que prestam serviços na internet, sem qualquer outra conexão com as empresas ou com os titulares de dados, como também segmentos do mesmo ficheiro podem estar armazenados em servidores localizados em diferentes Estados.

Para terminar este ponto, importa assinalar que entre estas remissões para o Direito dos Estados-Membros se conta a do art. 85.º, que determina que *os Estados-Membros conciliam por lei o direito à proteção de dados pessoais nos termos do Regulamento com o direito à liberdade de expressão e de informação* consagrado pelo art. 11.º da Carta, incluindo o tratamento para fins jornalísticos e para fins de expressão académica, artística ou literária (n.º 1 e Considerando n.º 153) ([36]).

Por conseguinte, a ponderação do direito à proteção de dados pessoais com a liberdade de expressão e o direito de informação depende em vasta medida das leis dos Estados-

---

35 - Já é mais controverso se constitui um elemento de conexão idóneo para a delimitação da jurisdição dos Estados ao abrigo do Direito Internacional Público – ver *Tallinn Manual 2.0 International Group of Experts and Other Participants*, Rule 1, n.º 4, e Rule 2, n.º 11; *Microsoft* v. *United States*, decidido em segunda instância pelo *United States Court of Appeals for the Second Circuit* (2016) (acessível em https://cases.justia.com/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.pdf?ts=1468508412); Keane WOODS – "Against Data Exceptionalism", *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal, Vol. 3 No. 16, 03/24/2016* (acessível em SSRN), 734 e segs. e 754 e segs.; CHRISTAKIS, Theodore – "Data, Extraterritoriality and International Solutions to Transatlantic Problems of Access to Digital Evidence. Legal Opinion on the Microsoft Ireland Case (Supreme Court of the United States)", *LSN Cyberspace Law eJournal, Vol. 23 No. 2, 01/10/2018* (acessível em SSRN), 24 e segs., mas vindo a defender soluções que não se baseiam no lugar de armazenamento dos dados nem no lugar de acesso aos dados; e Sean WATTS e Theodore RICHARD – "Baseline Territorial Sovereignty and Cyberspass", *LSN Public International Law: Foreign Relations & Policy Law eJournal, Vol. 5 No. 18, 03/30/2018* e *LSN Cyberspace Law eJournal, Vol. 23 No. 33, 04/05/2018* (acessível em SSRN), 851 e segs.

36 - Tal deverá ser aplicável, em especial, ao tratamento de dados pessoais no domínio do audiovisual e em arquivos de notícias e hemerotecas (Considerando n.º 153). A fim de ter em conta a importância da liberdade de expressão em qualquer sociedade democrática, há que interpretar de forma lata as noções associadas a esta liberdade, como por exemplo o jornalismo (Considerando n.º 153).

Membros, colocando a questão de saber quais as soluções materiais que devem ser adotadas e qual o seu âmbito de aplicação no espaço.

Relativamente ao art 9.º da Diretiva 95/46/CE, que constitui o precedente normativo desta disposição, o TUE decidiu no caso *Satakunnan Markkinapörssi* e *Satamedia* que para obter uma ponderação equilibrada entre os dois direitos fundamentais, as derrogações e limitações à proteção de dados pessoais devem operar dentro dos limites do estritamente necessário ([37]).

A Proposta inicial do Regulamento Roma II Sobre a Lei Aplicável às Obrigações Não Contratuais estabelecia, no art. 6.º/1, que a "lei aplicável à obrigação extracontratual resultante de uma violação do direito à vida privada ou dos direitos de personalidade é a lei do foro quando a aplicação da lei designada pelo artigo 3º seja contrária aos princípios fundamentais do foro em matéria de liberdade de expressão e de informação".

Por conseguinte, aplicar-se-ia à responsabilidade extracontratual por violação da privacidade a regra geral da competência da lei do lugar do dano, mas a lei do foro sobrepor-se-ia à lei estrangeira competente quando tal fosse exigido por princípios fundamentais da lei do foro em matéria de liberdade de expressão e de informação. Esta regra foi excluída da versão final devido a divergências irreconciliáveis com o Parlamento Europeu.

O art. 85.º do RGPD não impõe a aplicação da lei do foro a esta ponderação, como sucedia nessa Proposta. Pelo contrário, o Considerando n.º 153 aponta, quanto às isenções e derrogações relativas ao tratamento realizado para fins jornalísticos ou para fins de expressão académica, artística ou literária (previstas no art. 85.º/2) para a prevalência do Direito do Estado-Membro a que está sujeito o responsável pelo tratamento.

Em todo o caso, parece defensável que estando em causa uma ponderação de direitos fundamentais, se aplique a lei do foro sempre que a situação tenha uma ligação significativa com o Estado do foro ou com outro Estado (Estado-Membro ou terceiro) em que vigorem conceções fundamentais semelhantes.

Para o efeito, parece de preferir a formulação de uma disposição especial tendo por objeto esta questão, e que defina as conexões relevantes com o Estado do foro, atendendo à

37 - TUE 16/12/2008 [ECLI:EU:C:2008:727], n.º 56. Para uma comparação das soluções adotadas pelos Estados-Membros na transposição deste preceito, ver David ERDOS – "European Union Data Protection Law and Media Expression: Fundamentally Off Balance", *Int. Comp. L. Q.* 65 (2016) 139-184, 150 e segs.

interpretação das normas constitucionais em jogo e aos métodos e critérios de ponderação com respeito à colisão de direitos fundamentais.

III. DETERMINAÇÃO DO DIREITO ESTADUAL APLICÁVEL A QUESTÕES QUE O RGPD NÃO REGULA

A determinação do Direito aplicável às questões de Direito privado que o RGPD não regula tem de basear-se no Direito de Conflitos geral.

Na ordem jurídica portuguesa, o art. 27.º/1 CC estabelece que "Aos direitos de personalidade, no que respeita à sua existência e tutela e às restrições impostas ao seu exercício, é também aplicável a lei pessoal."

Daqui decorre que a atribuição dos direitos, o seu conteúdo e as restrições impostas ao seu exercício são regidos pela lei pessoal. No que se refere às restrições impostas ao exercício do direito, a competência da lei pessoal abrange tanto as restrições legais como a validade e efeitos das limitações voluntárias.

Embora o art. 27.º/1 atribua à lei pessoal a tutela do direito, deve entender-se que a tutela geral – responsabilidade civil por violação de direitos de personalidade – está submetida à lei reguladora da responsabilidade extracontratual ([38]).

Quanto às formas de tutela específica, é necessário ter em conta o disposto no n.º 2 do mesmo artigo, segundo o qual "O estrangeiro ou apátrida não goza, porém, de qualquer forma de tutela jurídica que não seja reconhecida na lei portuguesa". Este preceito suscita algumas dúvidas da interpretação. Tem-se entendido que junto aos tribunais portugueses só poderão ser atuadas as formas de tutela específica (providências preventivas ou repressivas) que sejam admitidas quer pela lei pessoal estrangeira quer pela lei portuguesa ([39]), o que representa um caso de conexão cumulativa. Também já se defendeu tratar-se de uma norma de Direito dos Estrangeiros ([40]), o que conduz ao mesmo resultado prático.

Estes entendimentos não levam em linha de conta a delimitação entre questões processuais, que estão submetidas necessariamente à *lex fori*, e questões substantivas. O preceito pode ser entendido em conformidade com a reserva de competência da lei

38 - Cf. J. BAPTISTA MACHADO – *Lições de Direito Internacional Privado*, (apontamentos das aulas teóricas do ano letivo de 1971/1972 na Faculdade de Direito de Coimbra), 2.ª ed., Coimbra, Almedina, 1982, 343. Sobre as normas de conflitos aplicáveis à violação do *right of publicity*, ver ELSA DIAS OLIVEIRA – "A relevância do *right of publicity* no âmbito da propriedade intelectual", *in Est. de Direito Intelectual/José de Oliveira Ascensão*, 209-232, Coimbra, Almedina, 2015, 228 e segs.

39 - BAPTISTA MACHADO, *Lições*…, 343, e Rabindranath CAPELO DE SOUSA – *O Direito Geral de Personalidade*, Coimbra, Coimbra Editora, 1995, 504.

40 - António MARQUES DOS SANTOS – *Direito Internacional Privado. Sumários*, 2.ª ed., Lisboa, AAFDL, 1987, 246 e seg.

portuguesa, enquanto *lex fori*, em matéria processual ([41]). Nesta ordem de ideias, a lei pessoal estrangeira decide sobre quais as pretensões que o interessado pode atuar, a lei portuguesa sobre quais os meios processuais por que estas pretensões podem ser atuadas. As leis em presença são, em princípio, de aplicação distributiva e não cumulativa embora, em resultado, possa acontecer que certas pretensões fundadas na lei pessoal estrangeira não encontrem meio processual adequado para a sua atuação em tribunais portugueses.

Este raciocínio já não vale para as formas de autotutela. Estas formas de autotutela têm de ser concedidas pela lei pessoal estrangeira; quando envolvam a utilização de meios coercivos têm também de ser permitidas pela lei portuguesa, uma vez que a utilização de meios coercivos depende do Direito local ([42]).

Por outro lado, quanto às formas de tutela específica de direitos de personalidade cuja violação se deva considerar abrangida pelo Regulamento Roma II apesar da exclusão estabelecida no art. 1.º/2/g ([43]), importa atender ao disposto no art. 15.º/d deste Regulamento que sujeita à lei reguladora da obrigação extracontratual "as medidas que um tribunal pode tomar para prevenir ou fazer cessar o dano", nos "limites dos poderes conferidos ao tribunal pelo seu direito processual". Parece, pois, que as formas de tutela específica dependerão neste caso da lei designada pelas normas de conflitos do Regulamento, com os limites decorrentes da competência da *lex fori* em matéria processual. Como adiante se assinalará, deve entender-se que o Regulamento Roma II não abrange a responsabilidade pela violação de direitos conferidos pelo RGPD aos titulares de dados pessoais.

Embora o princípio da personalidade aponte no sentido da competência da lei pessoal para determinar a atribuição dos direitos de personalidade e o seu conteúdo, a solução adotada pela maioria dos sistemas vai no sentido de estas questões serem submetidas à lei reguladora da responsabilidade extracontratual ([44]). Neste sentido invoca-se, designadamente, a vantagem de evitar o *dépeçage* entre a lei reguladora do direito de personalidade e a lei reguladora da responsabilidade pela sua violação; a eficácia *erga omnes* dos direitos de personalidade que reclama a utilização de elementos de conexão que sejam facilmente

41 - Ver Luís de LIMA PINHEIRO – *Direito Internacional Privado*, vol. II – *Direito de Conflitos - Parte Especial*, 4.ª ed., Coimbra, Almedina, 2015, § 52.
42 - Salvo tratado internacional em sentido diferente.
43 - Ver, sobre o ponto, LIMA PINHEIRO, *Direito Internacional Privado*, vol. II, *op. cit.*, 474-475, com mais referências.
44 - Ver, designadamente, *J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Einführungsgesetz zum Bürgerlichen Gesetzbuche, Art 38 – 42 EGBGB, Neubearbeitung 2001* /VON HOFFMANN, Berlim, Sellier- De Gruyter, Art. 40 EGBGB n.º 54; e *Münchener Kommentar zum Bürgerlichen Gesetzbuch*/JUNKER, vol. X, 6.ª ed., Munique, C. H. Beck, 2015, EGBGB Art. 40 n.º 83.

cognoscíveis por todos os interessados; e a possibilidade de a situação envolver um conflito de direitos entre o agente e o lesado que exige uma conexão neutra e previsível para ambas as partes.

Contra esta solução objeta-se que os direitos de personalidade não são relevantes apenas quando ocorre a sua violação, mas também em situações em que é apenas necessário determinar a sua existência, por exemplo, para saber se existe um direito de personalidade que seja passível de ser objecto de um negócio jurídico ([45]). Mas a esta objeção pode contrapor-se que independentemente de estar em causa uma violação, é, em princípio, possível consultar a lei do país em que se produziria o dano, caso o direito existisse e fosse violado. Trata-se de um raciocínio hipotético. Se essa lei atribuir o direito, todos os interessados sabem que a sua conduta deve respeitar esse direito, sob pena de responderem pelos danos causados pela sua violação ou de serem objecto de providências preventivas ou repressivas. Se essa lei não atribuir o direito, os interessados sabem que a sua conduta não é condicionada pelo mesmo.

Certo é que esta solução é de preferir a qualquer conexão cumulativa que faça depender a atribuição e conteúdo do direito simultaneamente da lei pessoal e da lei do foro ou da lei reguladora da responsabilidade extracontratual ([46]), que desfavoreceria a proteção dos bens de personalidade.

Dentro do âmbito de aplicação do RGPD, a atribuição dos direitos de proteção dos dados pessoais, o seu conteúdo e as restrições impostas ao seu exercício são, em princípio, regulados por este Regulamento, mesmo que a lei pessoal do titular dos dados seja a lei de um Estado terceiro, porque é diretamente aplicável a estes direitos. O que significa que *a norma de conflitos do art. 27.º/1 CC só pode desempenhar um papel relativamente à proteção de dados pessoais fora do âmbito de aplicação do RGPD ou, eventualmente, relativamente às questões que o RGPD remete para o Direito dos Estados-Membros sem definir o critério de conexão relevante*.

Relativamente a estas questões, vimos que coerência intrassistemática pode apontar para a competência do Direito do Estado a que está sujeito o responsável pelo tratamento ou o

45 - Ver ELSA DIAS OLIVEIRA – *Da Responsabilidade Civil Extracontratual por Violação de Direitos de Personalidade em Direito Internacional Privado*, Coimbra, Almedina, 2011, 292.

46 - Cp. ELSA DIAS OLIVEIRA, *Da Responsabilidade Civil Extracontratual*…, *op. cit.*, 295 e segs., defendendo que o art. 27.º CC, entendido à luz do "princípio da tutela da confiança", dever ser interpretado no sentido de a restrição contida no n.º 2 se referir não apenas às formas de tutela mas também aos direitos tutelados, quando exista um contacto entre a situação e a ordem jurídica portuguesa.

subcontratante (II), enquanto o principal objetivo do RGPD, que é o de tutelar os titulares de dados pessoais, oferece um argumento no sentido da aplicação da lei do Estado que tem a ligação mais estreita com titular dos dados.

Parece inevitável uma diferenciação, designadamente consoante estão em causa interesses públicos ou a constituição, funcionamento e atividade das autoridades de controlo, ou interesses privados.

Quando estiverem diretamente em causa interesses públicos é de esperar que os Estados-Membros que prosseguem esses interesses delimitem por meio de normas de conflitos unilaterais o âmbito de aplicação das normas que os tutelam.

As questões relativas à constituição, funcionamento e atividades das autoridades de controlo deverão, em princípio, estar submetidas ao Direito do Estado-Membro a que pertence a autoridade.

Nos outros casos, parece-me que, em princípio, é de preferir, em conformidade com o princípio da personalidade, a aplicação da lei de um Estado que tenha uma ligação estreita com o titular dos dados. Excetuam-se os casos em que estejam em causa interesses privados que não interfiram diretamente com interesses do titular dos dados, designadamente do responsável pelo tratamento e/ou do subcontratante.

Na determinação dessa lei importa também atender à conveniência de aplicar a mesma lei que rege a responsabilidade extracontratual pela violação dos direitos do titular dos dados e de uma convergência entre a lei aplicável e o foro competente.

Perante o art. 5.º/3 do Regulamento Bruxelas I (competência internacional em matéria extracontratual), o TUE entendeu no caso *eDate Advertising* (2011) ([47]) que o critério do lugar do dano causado a um direito de personalidade suscita dificuldades quando a violação resulta de um conteúdo introduzido na internet, visto que este é acessível universalmente, e, por isso, carece de adaptações. Nesta base, o tribunal entendeu que a competência se pode fundamentar na localização do centro de interesses do lesado, que corresponde, em princípio, à sua residência habitual ([48]).

O TUE acrescentou que uma pessoa pode ter o centro dos seus interesses igualmente num Estado-Membro onde não reside habitualmente, na medida em que outros indícios, como o

47 - 25/10/2011 [*in www.curia.europa.eu*].
48 - N.ºs 47-49.

exercício de uma atividade profissional, podem estabelecer a existência de um nexo particularmente estreito com esse Estado ([49]).

Já tive ocasião de defender anteriormente que embora não se deva fazer uma transposição mecânica desta solução para a determinação do Direito aplicável à responsabilidade extracontratual por danos causados a direitos de personalidade através da internet, é concebível que uma solução adequada nesta matéria atenda igualmente à residência habitual do lesado ou, mais amplamente, ao seu centro de interesses ([50]).

Acrescente-se que o art. 79.º/2 do RGPD determina que os titulares de dados podem optar entre propor a ação contra o responsável pelo tratamento ou o subcontratante nos tribunais do Estado-Membro em que o responsável pelo tratamento ou o subcontratante tenham estabelecimento ou nos tribunais do Estado-Membro em que o titular dos dados tenha a sua residência habitual ([51]).

Estas considerações levam-me a concluir que é *o Direito do Estado em que o titular dos dados pessoais tem o centro dos seus interesses que está em melhor posição para reger os seus direitos no contexto da internet*.

Fora do âmbito de aplicação do RGPD esta solução só parece defensável *de iure condendo*.

Dentro do âmbito de aplicação deste RGPD, mas relativamente às questões que remete para o Direito dos Estados-Membros sem definir o critério de conexão relevante, a necessidade de evitar um excessivo fracionamento das situações, mediante a aplicação do regime do RGPD, da lei pessoal do titular dos dados e da lei reguladora da responsabilidade extracontratual, parece justificar uma redução teleológica do art. 27.º/1 CC, e a integração da lacuna daí resultante com esta solução.

Quanto às questões que o RGPD não regula, a lei reguladora dos contratos obrigacionais, definida nos termos do Regulamento Roma I, tem um papel a desempenhar relativamente a

---

49 - N.º 49.

50 - Ver propostas convergentes em ELSA DIAS OLIVEIRA – "Algumas considerações sobre a responsabilidade civil extracontratual por violação de direitos de personalidade em Direito Internacional Privado", *Cuadernos de Derecho Transnacional* 5 (2013) 139-162, 147-148 ns. 34 e 35 e, para a posição diversa desta autora, loc. cit., 160 e segs.

51 - Ver também Considerando n.º 145 e art. 82.º/6. O foro da residência habitual do titular dados é, porém, excluído, se o responsável pelo tratamento ou o subcontratante for uma autoridade de um Estado-Membro no exercício dos seus poderes públicos (n.º 2 *in fine*).

compromissos livremente assumidos pelo responsável pelo tratamento ou pelo subcontratante perante o titular dos dados ([52]).

Observe-se que quando o contrato for regido pela lei de um terceiro Estado nos termos do Regulamento Roma I, o regime do RGPD sobrepor-se-á, dentro do seu âmbito de aplicação, à lei reguladora do contrato por força própria, e não nos termos do art. 9.º/2 do Regulamento Roma I ([53]).

Na prática, porém, a questão mais importante é a da *responsabilidade extracontratual pela violação de direitos à proteção de dados pessoais* ([54]).

O art. 82.º contém algumas regras sobre a responsabilidade civil do responsável pelo tratamento ou do subcontratante perante qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do RGPD.

Estas regras:

- reconhecem a qualquer pessoa que tenha sofrido danos o direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos;

- limitam a responsabilidade dos subcontratantes aos casos de incumprimento das obrigações decorrentes do RGPD que lhes são dirigidas especificamente ou de não observância das instruções lícitas do responsável pelo tratamento;

- exoneram o responsável pelo tratamento ou o subcontratante de responsabilidade se provar que não é de modo algum responsável pelo evento que deu origem aos danos;

- estabelecem a responsabilidade solidária dos responsáveis pelo tratamento ou subcontratantes que estejam envolvidos no mesmo tratamento e sejam responsáveis por eventuais danos.

O Considerando n.º 146 fornece indicações importantes para a interpretação desta disposição.

---

52 - Ver também KOHLER, "Conflict of Law Issues…, *loc. cit.*, 671. Colocando este ponto em dúvida, com referência à supracit. decisão TUE no caso *Verein für Konsumenteninformation*, Sabine CORNELOUP – "De la loi applicable aux activités des entreprises de commerce électronique", *R. crit.* (2017) 112-122, 121-122.

53 - Neste sentido, porém, KOHLER, "Conflict of Law Issues…, *loc. cit.*, 661, e MIGUEL ASENSIO, "Competencia y Derecho aplicable…", *loc. cit.*, 104. Relativamente à Dir. 95/46/CE, ver BRKAN, "Data Protection…", *loc. cit.*, 26 e segs.

54 - MIGUEL ASENSIO, "Competencia y Derecho aplicable…", *loc. cit.*, 105-106, chama a atenção para a possibilidade de delicados problemas de delimitação entre o regime do RGPD, que depende de uma conexão autónoma, e a lei aplicável às obrigações extracontratuais, quando esteja em causa a responsabilidade por violação de regras do RGPD.

Primeiro, o conceito de dano deverá ser interpretado em sentido lato à luz da jurisprudência do Tribunal de Justiça, de uma forma que reflita plenamente os objetivos do RGPD.

Segundo, a disposição não prejudica os pedidos de indemnização por danos provocados pela violação de outras regras do Direito da União ou dos Estados-Membros.

Terceiro, os tratamentos que violem o RGPD abrangem igualmente os que violem os atos delegados e de execução adotados nos termos do RGPD e o Direito dos Estados-Membros que dê execução a regras do RGPD.

Quarto, os titulares dos dados deverão ser integral e efetivamente indemnizados pelos danos que tenham sofrido.

Por último, apesar de cada um dos responsáveis pelo tratamento ou os subcontratantes envolvidos no mesmo tratamento responder pela totalidade dos danos causados, se os processos forem associados a um mesmo processo judicial, em conformidade com o Direito dos Estados-Membros, a indemnização poderá ser repartida em função da responsabilidade que caiba a cada responsável pelo tratamento ou subcontratante pelos danos causados em virtude do tratamento efetuado, na condição de ficar assegurada a indemnização integral e efetiva do titular dos dados pelos danos que tenha sofrido.

Os outros aspetos da responsabilidade extracontratual do responsável pelo tratamento e do subcontratante, como a culpa, as causas de justificação, o nexo de causalidade e, em princípio, o cálculo da indemnização são regidos pela lei aplicável a essa responsabilidade.

Sobre a lei aplicável à responsabilidade extracontratual vigora na ordem jurídica portuguesa o *Regulamento Roma II*, mas o art. 1.º/2/g exclui do seu âmbito de aplicação as obrigações extracontratuais que decorram da violação da vida privada e dos direitos de personalidade. Embora esta exclusão dos direitos de personalidade deva ser interpretada restritivamente, parece de entender que dado o relacionamento da proteção de dados pessoais com a privacidade está excluída a responsabilidade por violação de direitos à proteção de dados pessoais ([55]).

---

55 - Bem como a violação de normas de proteção de dados pessoais que não confiram direitos subjetivos.
Cf. KOHLER , "Conflict of Law Issues…, *loc. cit.*, 673-674, e MIGUEL ASENSIO, "Competencia y Derecho aplicable…", *loc. cit.*, 105-106. Em sentido diferente, BRKAN, "Data Protection…", *loc. cit.*, 26 e segs., com mais referências. MIGUEL ASCENSIO [*loc. cit.*] defende que os interesses em presença apontam no sentido da competência da lei do lugar onde ocorre a lesão dos bens ou direitos do prejudicado, tipicamente a sua residência habitual "ou centro de interesses". Ver, com mais desenvolvimento, Id. – *Derecho Privado de Internet*, 5.ª ed., Cizur Menor (Navarra), Civitas e Thomson Reuters, 2015, 217-218. O autor invoca o paralelismo com a regra de

Importa, por isso, recorrer ao *Direito de Conflitos de fonte interna* contido no art. 45.º CC.

O n.º 1 do art. 45.º CC submete a responsabilidade extracontratual fundada quer em ato ilícito quer no risco ou em qualquer conduta lícita "à lei do Estado onde decorreu a principal atividade causadora do prejuízo; em caso de responsabilidade por omissão, é aplicável a lei do lugar onde o responsável deveria ter agido" ([56]).

No entanto, por força do n.º 2 aplica-se a lei do Estado onde se produziu o efeito lesivo quando esta considerar responsável o agente, mas não o considerar como tal a lei do país onde decorreu a sua atividade, desde que o agente devesse prever a produção de um dano, naquele país, como consequência do seu ato ou omissão.

Nos casos de violação da proteção de dados pessoais no contexto da internet *qual é o lugar da atividade causadora do prejuízo*?

Creio que tanto o lugar onde são tratados os dados pessoais como o lugar em que o responsável pelo tratamento ou subcontratante acede à rede ([57]) poderiam ser relevantes como lugar da atividade causadora de prejuízo. Normalmente coincidem. Se esta coincidência não se verificar, deve relevar, como lugar da atividade principal, aquele em que os dados foram tratados.

A determinação dos lugares onde os dados são tratados e onde o agente acede à rede pode suscitar grandes dificuldades. Este lugar pode não ser cognoscível pelos titulares de dados ou só o ser com custos proibitivos ([58]). Como solução de recurso pode interpretar-se o art. 45.º no sentido de o Direito do lugar do efeito lesivo ser aplicável quando não for possível determinar o lugar da atividade.

---

competência internacional do art. 79.º/2 RGPD, mas este paralelismo apontaria mais no sentido de uma aplicação alternativa da lei do Estado de estabelecimento do responsável pelo tratamento de dados (em princípio, a lei do lugar da atividade) e da lei da residência habitual do titular dos dados

56 - Ver também o art. 16.º da Convenção de Bruxelas Relativa ao Auxílio Mútuo em Matéria Penal entre os Estados-Membros da União Europeia (2000), com respeito à responsabilidade civil dos agentes de um Estado-Membro que se encontrem em missão noutro Estado-Membro.

57 - Cf. Peter MANKOWSKI – "Das Internet im Internationalen Vertrags- und Deliktsrecht", *RabelsZ.* 63 (1999) 203-294, 257. Cp. James FAWCETT e Paul TORREMANS – *Intellectual Property and Private International Law*, 2.ª ed., Oxford, Oxford University Press, 2011, n.º 16.104, entendendo que a ofensa ao bom nome e reputação é perpetrada em todos os Estados em que a informação é "descarregada" recebida, e *Dicey, Morris and Collins on the Conflict of Laws* – 15.ª ed. por LORD COLLINS OF MAPESBURY (ed. geral), Adrian BRIGGS, Andrew DICKINSON, Jonathan HARRIS, J. McCLEAN, Peter McELEAVY, Campbell McLACHLAN e C. MORSE, Londres, Sweet & Maxwell e Thompson Reuters, 2012, n.º 35-119, entendendo como lugar do delito o lugar em que a informação é "descarregada" ou acedida, pelo menos se o lesado sofre uma ofensa à sua reputação nesse lugar.

58 - Ver propostas de solução deste problema em MANKOWSKI, "Das Internet…", *loc. cit.*, 258 e segs.

Além disso, no caso de delitos cometidos através de radiodifusão, transmissão por satélite e rede informática, o risco de manipulação do elemento de conexão lugar da atividade é especialmente elevado. O operador pode facilmente deslocar o lugar da sua atuação para um Estado especialmente permissivo. A possibilidade de aplicar o Direito do lugar do efeito lesivo quando o Direito de o lugar da atividade não considerar o agente responsável não anula este risco, porque o Direito do lugar da atividade pode submeter o agente a um regime de responsabilidade menos severo que o Direito do lugar do efeito lesivo.

Este risco agravado de fraude à lei poderia ser prevenido mediante uma disposição especial segundo a qual em caso de delito cometido por estes meios o lesado pode optar entre a aplicação do Direito do lugar da atividade e a aplicação do Direito da residência habitual ou sede da administração do agente.

Em sentido próximo, o art. 139.º/1 da Lei suíça de Direito Internacional Privado confere ao lesado, com respeito às pretensões fundadas em violação de direitos de personalidade através de meios públicos de comunicação, uma escolha entre o Direito do Estado da residência habitual do lesado, contanto que o agente pudesse contar com a produção do resultado neste Estado, o Direito do Estado do estabelecimento ou residência habitual do agente e o Direito do Estado onde se produz o resultado da violação, contanto que o agente pudesse contar com a produção do resultado neste Estado.

Um segundo problema, é *o da determinação do lugar em que se produz o efeito lesivo*.

Na violação de direitos de personalidade através da colocação de um conteúdo na internet o efeito lesivo pode-se produzir em todos os lugares em que é facultado o acesso dos utilizadores à rede ([59]). Embora esta multiplicação dos lugares do efeito lesivo possa ser restringida, em certos casos, em função do conteúdo do direito de personalidade em causa ([60]), implica sempre potencialmente um fracionamento do Direito aplicável que pode levar a dificuldades dificilmente superáveis e não atende ao princípio geral da conexão mais estreita ([61]). Estas considerações justificam uma adaptação da solução conflitual, que, nos termos anteriormente referidos, se pode *até certo ponto* inspirar na jurisprudência do TUE perante o

59 - Cf. MANKOWSKI, "Das Internet…", *loc. cit.*, 269, com algumas exceções.
60 - Assim, a lesão do bom nome e reputação produz-se apenas nos Estados em que o lesado é conhecido. Com efeito, o bom nome e reputação só pode ser lesado pela afirmação ou divulgação de factos num meio social em que a pessoa atingida seja conhecida. Por razão afim, o tipo de responsabilidade extracontratual contido no art. 484.º CC português (ofensa do crédito ou do bom nome) só está preenchido quando um facto é afirmado ou divulgado no meio social em que a pessoa atingida viva ou exerça a sua atividade – cf. ANTUNES VARELA – *Das Obrigações em geral*, 10.ª ed., Coimbra, 2004, 549.
61 - Ver também MIGUEL ASENSIO, "Competencia y Derecho aplicable…", *loc. cit.*, 217-218.

art. 5.º/3 do Regulamento Bruxelas I (competência internacional em matéria extracontratual) ([62]) e no art. 79.º/2 RGPD (competência internacional para a ação de responsabilidade pela violação dos direitos conferidos pelo RGPD ao titular dos dados) ([63]).

Nesta ordem de ideias, será de considerar como lugar do efeito lesivo aquele em que o titular dos dados tenha a sua residência habitual ou, mais amplamente, o seu centro de interesses.

Em sentido convergente com o art. 4.º/3 do Regulamento Roma II, creio que se justificaria um outro desvio por aplicação da ideia do respeito da interdependência de complexos normativos, à semelhança do disposto no art. 133.º/3 da Lei suíça e no art. 41.º/2/1 da Lei de Introdução do Código Civil alemão, com a redação dada em 1999 ([64]). Segundo este desvio, se entre o agente e o lesado preexiste uma relação jurídica, será a lei aplicável a esta relação que, em princípio, regerá a responsabilidade extracontratual.

Também entendo que o Direito de Conflitos de fonte interna deveria convergir com o Regulamento Roma II quanto à admissibilidade da escolha pelas partes do Direito aplicável às obrigações não voluntárias ([65]).

---

62 - No já referido caso *eDate Advertising* (TUE 25/10/2011 [in http://curia.europa.eu], n.º 52), o TUE entendeu que em caso de alegada violação dos direitos de personalidade através de conteúdos colocados em linha num sítio na Internet, a pessoa que se considerar lesada tem a faculdade de intentar uma ação fundada em responsabilidade pela totalidade dos danos causados, quer nos órgãos jurisdicionais do Estado-Membro do lugar de estabelecimento da pessoa que emitiu esses conteúdos quer nos órgãos jurisdicionais do Estado-Membro onde se encontra o centro dos seus interesses. Esta pessoa pode igualmente, em vez de uma ação fundada em responsabilidade pela totalidade dos danos causados, interpor a sua ação nos órgãos jurisdicionais de cada Estado-Membro em cujo território esteja ou tenha estado acessível um conteúdo em linha. Estes são competentes para conhecer apenas do dano causado no território do Estado-Membro do órgão jurisdicional em que a ação foi intentada.

63 - Os titulares de dados podem optar entre propor a ação nos tribunais do Estado-Membro em que o responsável pelo tratamento ou o subcontratante tenham estabelecimento ou nos tribunais do Estado-Membro em que o titular dos dados tenha a sua residência habitual. Ver também Considerando n.º 145.

64 - O preceito da lei alemã insere esta solução numa cláusula de exceção e alarga-a à existência de uma relação de facto entre os interessados. Ver ainda Jan KROPHOLLER – *Internationales Privatrecht*, 6.ª ed., Tubinga, Mohr Siebeck, 2006, 530 e seg.; as considerações convergentes de António FERRER CORREIA – *Direito Internacional Privado. Alguns problemas*, Coimbra, Almedina, 1981, 105 e segs.; e ANABELA DE SOUSA GONÇALVES – *Da Responsabilidade Extracontratual em Direito Internacional Privado. A Mudança de Paradigma*, Coimbra, Almedina, 2013, 410-411; e as obras indicadas por Rui MOURA RAMOS – *Da Lei Aplicável ao Contrato de Trabalho Internacional*, Coimbra, Almedina, 1991, 378 n. 19. Ver ainda Dário MOURA VICENTE – *Da Responsabilidade Pré-Contratual em Direito Internacional Privado*, Coimbra, Almedina, 2001, 498 e segs., com desenvolvidas referências doutrinais e comparativas, que admite limitadamente este desvio mesmo *de iure constituto*, seguido por ELSA DIAS OLIVEIRA, *Da Responsabilidade Civil Extracontratual*…, *op. cit.*, 523-524.

65 - Ver também o art. 42.º da Lei de Introdução do Código Civil Alemão, com a redação dada em 1999. Já tenho por indefensável a admissibilidade da escolha da lei aplicável perante o Direito constituído, como sustenta NUNO PISSARRA – *O Dano Transnacional em Direito Internacional Privado. Alguns Problemas* (Diss. de Mestrado policopiada), Lisboa, 2004, 153 e segs. O legislador optou inequivocamente, no art. 45.º CC, por elementos de conexão objetivos, pelo que seria manifestamente contrário à intenção legislativa admitir a autonomia conflitual nesta matéria.

O regime que se acaba de referir é também aplicável à responsabilidade extracontratual de prestadores de serviços em linha, visto que o DL n.º 7/2004, de 7/1, interpretado em conformidade com a *Diretiva sobre Comércio Eletrónico*, não afasta a regra de conflitos do art. 45.º CC ([66]). No entanto, decorre do entendimento adotado pelo TUE, no já referido caso *eDate Advertising* (2011), que a lei designada pelo art. 45.º CC não pode estabelecer, para os prestadores de serviços estabelecidos num Estado-Membro, um regime mais rigoroso que o da lei deste Estado-Membro ([67]).

66 - Ver LIMA PINHEIRO, *Direito Internacional Privado*, vol. II, *op. cit.*, § 65 D *in fine* e 68 *B in fine*. Sobre o problema, antes da decisão do TUE no caso *eDate Advertising*, ver LIMA PINHEIRO – "Direito aplicável à responsabilidade extracontratual na *Internet*", *RFDUL* 42 (2001) 825-834, 833 e seg., e – "O Direito de Conflitos e as liberdades comunitárias de estabelecimento e de prestação de serviços", *in Seminário sobre a Comunitarização do Direito Internacional Privado*, 79-109, Coimbra, Almedina, 2005 (=*in Estudos de Direito Internacional Privado*, 357-387, Coimbra, Almedina, 2006) 102 e segs., com mais referências.
67 - N.º 67.

IV. CONSIDERAÇÕES FINAIS

Não cabendo examinar neste estudo a controvérsia suscitada por certas soluções materiais, pode afirmar-se que a vasta uniformização do Direito material aplicável à proteção de dados pessoais na UE é, em princípio, justificada. No entanto, o âmbito espacial de aplicação do RGPD parece demasiado amplo, não assegurando que existe sempre uma ligação significativa com a União Europeia.

O art. 50.º prevê a adoção das medidas necessárias para a cooperação internacional com países terceiros e organizações internacionais que são de grande importância:

- estabelecer regras internacionais de cooperação destinadas a facilitar a aplicação efetiva da legislação em matéria de proteção de dados pessoais;

- prestar assistência mútua a nível internacional no domínio da aplicação da legislação relativa à proteção de dados pessoais, nomeadamente através da notificação, comunicação de reclamações, e assistência na investigação e intercâmbio de informações, sob reserva das garantias adequadas de proteção dos dados pessoais e de outros direitos e liberdades fundamentais;

- associar as partes interessadas aos debates e atividades que visem intensificar a cooperação internacional no âmbito da aplicação da legislação relativa à proteção de dados pessoais; e

- promover o intercâmbio e a documentação da legislação e das práticas em matéria de proteção de dados pessoais, nomeadamente no que diz respeito a conflitos jurisdicionais com países terceiros.

A importância desta cooperação internacional é ilustrada por algumas decisões muito discutidas não só relativamente à proteção internacional de dados pessoais, mas também relativamente à investigação penal transfronteiriça ([68]).

A internet, como realidade global, carece de uma regulação global, que em boa parte pode ser proporcionada por organizações privadas representativas da comunidade dos participantes na internet, mas também carece, em diversos domínios, como é o caso da

68 - Ver, designadamente, CHRISTAKIS, "Data, Extraterritoriality and International Solutions…", *loc. cit.*, 35 e segs.

proteção de dados pessoais, de uma regulação por Convenções internacionais de âmbito universal ([69]).

Já se deram alguns passos no sentido da unificação internacional do regime aplicável à proteção de dados pessoais, mas com significado limitado.

Assim, o Conselho de Europa adotou em 1981 a Convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (Convenção 108), de que são partes todos os Estados-Membros do Conselho, mas que só obteve um acolhimento muito limitado de outros Estados. Em 2001, foi aberto à assinatura um Protocolo Adicional à Convenção Respeitante às Autoridades de Controlo e aos Fluxos Transfronteiriços de Dados, de que são partes 36 dos 47 Estados-Membros do Conselho de Europa, incluindo Portugal, e que também só obteve um acolhimento muito limitado de outros Estados. Com vista a modernizar a Convenção 108, designadamente perante o crescente uso de novas tecnologias de informação e comunicação, o Conselho de Europa adotou muito recentemente um novo Protocolo de modificação da Convenção 108. O texto consolidado daí resultante é designado Convenção Modernizada para a Proteção das Pessoas Relativamente ao Processamento de Dados Pessoais (Convenção 108+).

Para além da limitação geográfica, estes instrumentos não estabelecem um regime uniforme, antes obrigam os Estados Contratantes a conformar o seu Direito interno com as disposições convencionais e a assegurar a sua efetividade.

No âmbito da União Europeia, o RGPD opera uma ampla uniformização, mas este RGPD remete muitas questões para o Direito dos Estados-Membros, sendo necessária desenvolvida legislação nacional de execução do RGPD, que tem de oferecer soluções adequadas de Direito material, de Direito Internacional Privado e de Direito Público Internacional para essas questões.

---

69 - Ver Rolf WEBER – *Shaping Internet Governance: Regulatory Challenges*, em colaboração com Mirina Grosz e Romana Weber, Zurique, Basileia e Genebra, Springer, 2009, 16-17; e Luís de LIMA PINHEIRO – "Reflexões sobre a governação e a regulação da internet, com especial consideração da ICANN", *in Estudos de Direito Intelectual em Homenagem ao Prof. Doutor José de Oliveira Ascensão*, 363-385, Coimbra, Almedina, 2015, 371-372. Considerando que a viabilidade política desta unificação internacional é altamente questionável, BRKAN, "Data Protection…", *loc. cit.*, 36-37. Menos adequada, porém, se afigura uma unificação internacional dos regimes da competência internacional e da determinação do Direito aplicável limitada à proteção de dados pessoais, aventada pelo autor.

BIBLIOGRAFIA

BRKAN, Maja – "Data Protection and European Private International Law", *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal, Vol. 2 No. 43, 07/28/2015* (acessível em SSRN)

CALSTER, eert van – "Regulating the Internet. Prescriptive and Jurisdictional Boundaries to the EU's 'Right to Be Forgotten', *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal, Vol. 2 No. 64, 11/12/2015* (acessível em SSRN)

CHRISTAKIS, Theodore – "Data, Extraterritoriality and International Solutions to Transatlantic Problems of Access to Digital Evidence. Legal Opinion on the Microsoft Ireland Case (Supreme Court of the United States)", *LSN Cyberspace Law eJournal, Vol. 23 No. 2, 01/10/2018* (acessível em SSRN)

CORNELOUP, Sabine – "De la loi applicable aux activités des entreprises de commerce électronique", *R. crit.* (2017) 112-122

CORREIA, António FERRER – *Direito Internacional Privado. Alguns problemas*, Coimbra, Almedina, 1981

Dicey, Morris and Collins on the Conflict of Laws – 15.ª ed. por LORD COLLINS OF MAPESBURY (ed. geral), Adrian BRIGGS, Andrew DICKINSON, Jonathan HARRIS, J. McCLEAN, Peter McELEAVY, Campbell McLACHLAN e C. MORSE, Londres, Sweet & Maxwell e Thompson Reuters, 2012

ERDOS, David – "European Union Data Protection Law and Media Expression: Fundamentally Off Balance", *Int. Comp. L. Q.* 65 (2016) 139-184

FAWCETT, James e Paul TORREMANS – *Intellectual Property and Private International Law*, 2.ª ed., Oxford, Oxford University Press, 2011

GONÇALVES, ANABELA DE SOUSA – *Da Responsabilidade Extracontratual em Direito Internacional Privado. A Mudança de Paradigma*, Coimbra, Almedina, 2013

J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Einführungsgesetz zum Bürgerlichen Gesetzbuche, Art 38 – 42 EGBGB, Neubearbeitung 2001 /VON HOFFMANN, Berlim, Sellier- De Gruyter, 2001

KELLER, Daphne – "The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation", *LSN Cyberspace Law eJournal, Vol. 22 No. 19, 03/15/2017* (acessível em SSRN)

KOHLER, Christian – "Conflict of Law Issues in the 2016 Data protection Regulation of the European Union", *RDIPP* (2016) 653-675

KROPHOLLER, Jan – *Internationales Privatrecht*, 6.ª ed., Tubinga, Mohr Siebeck, 2006

KULK, Stefan e Frederik Borgesius – "Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe", *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal, Vol. 4 No. 13, 03/09/2017* (acessível em SSRN).

MACHADO, J. BAPTISTA – *Lições de Direito Internacional Privado*, (apontamentos das aulas teóricas do ano letivo de 1971/1972 na Faculdade de Direito de Coimbra), 2.ª ed., Coimbra, Almedina, 1982.

MANKOWSKI, Peter – "Das Internet im Internationalen Vertrags- und Deliktsrecht", *RabelsZ.* 63 (1999) 203-294

MIGUEL ASENSIO, Pedro – *Derecho Privado de Internet*, 5.ª ed., Cizur Menor (Navarra), Civitas e Thomson Reuters, 2015

Id. – "Competencia y Derecho aplicable en el reglamento general sobre protección de datos de la Unión Europea", *Rev. Española de Derecho Internacional* 69 (2017) 75-108.

MIRANDA, JORGE – *Direitos Fundamentais*, 2.ª ed., Coimbra, Almedina, 2017

Münchener Kommentar zum Bürgerlichen Gesetzbuch/JUNKER, vol. X, 6.ª ed., Munique, C. H. Beck, 2015.

NADEEM, Danial – "Territorial Limits to the European Union's Right to be Forgotten: How the CNIL Ignores Jurisdictional Basics in Its March 10, 2016 Decision Against Google", *Creighton Int'l & Comp. L.J.* 8 (2017) 182-199

NUNZIATO, Dawn – "The Fourth Year of Forgetting: The Troubling Expansion of the Right to Be Forgotten", *LSN Cyberspace Law eJournal, Vol. 23 No. 49, 07/16/2018* (acessível em SSRN)

OLIVEIRA, ELSA DIAS – *Da Responsabilidade Civil Extracontratual por Violação de Direitos de Personalidade em Direito Internacional Privado*, Coimbra, Almedina, 2011

Id. – "Algumas considerações sobre a responsabilidade civil extracontratual por violação de direitos de personalidade em Direito Internacional Privado", *Cuadernos de Derecho Transnacional* 5 (2013) 139-162

Id. – "A relevância do *right of publicity* no âmbito da propriedade intelectual", *in Est. de Direito Intelectual/José de Oliveira Ascensão*, 209-232, Coimbra, Almedina, 2015.

PINHEIRO, Luís de LIMA– "Direito aplicável à responsabilidade extracontratual na *Internet*", *RFDUL* 42 (2001) 825-834

Id. – "O Direito de Conflitos e as liberdades comunitárias de estabelecimento e de prestação de serviços", *in Seminário sobre a Comunitarização do Direito Internacional Privado*, 79-109, Coimbra, Almedina, 2005 (=*in Estudos de Direito Internacional Privado*, 357-387, Coimbra,

Almedina, 2006)
Id. – *Direito Internacional Privado*, vol. I – *Introdução e Direito de Conflitos – Parte Geral*, 3.ª ed., Coimbra, Almedina, 2014
Id. – *Direito Internacional Privado*, vol. II – *Direito de Conflitos-Parte Especial*, 4.ª ed., Coimbra, Almedina, 2015
Id. – "Reflexões sobre a governação e a regulação da internet, com especial consideração da ICANN", *in Estudos de Direito Intelectual em Homenagem ao Prof. Doutor José de Oliveira Ascensão*, 363-385, Coimbra, Almedina, 2015
PISSARRA, NUNO – *O Dano Transnacional em Direito Internacional Privado. Alguns Problemas* (Diss. de Mestrado policopiada), Lisboa, 2004
RAMOS, Rui MOURA – *Da Lei Aplicável ao Contrato de Trabalho Internacional*, Coimbra, Almedina, 1991
RIVERO, Fomperosa – "Right to Be Forgotten in the European Court of Justice Google Spain Case: The Right Balance of Privacy Rights, Procedure, and Extraterritoriality", *LSN Cyberspace Law eJournal, Vol. 22 No. 19, 03/15/2017* (acessível em SSRN).
SANTOS, António MARQUES DOS – *Direito Internacional Privado. Sumários*, 2.ª ed., Lisboa, AAFDL, 1987
SCHWARTZ, Paul e Karl-Nicolaus PEIFER – "Transatlantic Data Privacy", *LSN Cyberspace Law eJournal, Vol. 22 No. 85, 11/22/2017* (acessível em SSRN)
SOUSA, Rabindranath CAPELO DE – *O Direito Geral de Personalidade*, Coimbra, Coimbra Editora, 1995.
Tallinn Manual 2.0 International Group of Experts and Other Participants, General Editor Michael Schmitt, Cambridge, Cambridge University Press, 2017
VARELA, ANTUNES – *Das Obrigações em geral*, 10.ª ed., Coimbra, Almedina, 2004
VICENTE, Dário MOURA – *Da Responsabilidade Pré-Contratual em Direito Internacional Privado*, Coimbra, Almedina, 2001
WATTS, Sean e Theodore RICHARD – "Baseline Territorial Sovereignty and Cyberspass", *LSN Public International Law: Foreign Relations & Policy Law eJournal, Vol. 5 No. 18, 03/30/2018* e *LSN Cyberspace Law eJournal, Vol. 23 No. 33, 04/05/2018* (acessível em SSRN),
WEBER, Rolf – *Shaping Internet Governance: Regulatory Challenges*, em colaboração com Mirina Grosz e Romana Weber, Zurique, Basileia e Genebra, Springer, 2009
WOODS, Keane – "Against Data Exceptionalism", *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal, Vol. 3 No. 16, 03/24/2016* (acessível em SSRN).