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

CYBERLAW by CIJIC

EDIÇÃO N.º IX – MARÇO DE 2020

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

EDITOR: NUNO TEIXEIRA CASTRO

SUPORTE EDITORIAL: EUGÉNIO ALVES DA SILVA e AFONSO FREITAS DANTAS

PRESIDENTE DO CIJIC: EDUARDO VERA-CRUZ PINTO

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

NOTAS DO EDITOR:

Globalização. Tecnologia e Inteligência artificial. Mobilidade organizacional e individual. Manipulação. A pandemia de Coronavírus. Hoje. O futuro.

Vivemos tempos "*estranhos*". Acutilantes. Irresolutos. Contingentes. Exigentes. O "tema" que nos capta, quase em exclusivo, a atenção, desde o início do ano de 2020, é a pandemia de coronavírus. Aquela dinâmica, rotineira, até agora tida como "garantida" atravessa momentos de grande indeterminação. Hora a hora somos como que bombardeados com números esmagadores: de taxas mundiais galopantes de infectados, doentes em cuidados intensivos, de mortos. No passar deste tempo, diariamente, deambulámos entre um imoderado e célere na disseminação da infecção *versus* um vagaroso e fleumático passo na demonstração de resultados animadores no seu combate. O racional económico de «custo-benefício» geralmente revelaria a perigosidade associada à extrema cautela. Porém na questão, truncada, do coronavírus é diferente[1]. "*Achatar as curvas*", "*Proteger os mais idosos e os mais vulneráveis*", "*Suster a vaga de procura do SNS por forma a dar-lhe tempo para acudir às solicitações*", mesmo que o custo seja o parar da Economia. Global. Entretanto o tempo continua o seu passo. Assim como a epidemia há-de passar.

1 Cass Sunstein @ https://www.bloomberg.com/opinion/articles/2020-03-26/coronavirus-lockdowns-look-smart-under-cost-benefit-scrutiny

E, quando aí chegados, a questão resolutiva a colocar não deverá andar muito longe de um: "*Que mundo esperar do pós-covid19*"?

O avanço da tecnologia, combinando melhores recursos de *hardware* com inteligência artificial, aos quais o Homem socorre, permitiram sequenciar o genoma do COVID-19 em menos de um mês. A inteligência artificial, por exemplo, num contexto, global, de recursos exíguos tem sido testada para suprir lacunas críticas nos recursos de saúde, ajudando à racionalidade da decisão política, alavancando centros de inovação em inteligência artificial, robótica e automação em saúde. Na Ásia[2]. Por agora.

O mesmo avanço tecnológico, por sua vez, no actual cenário de "*guerra*" ao vírus, colocou a ponderação das liberdades fundamentais num estádio de confronto titânico. Recuperando o "*achatar a curva*", um pouco por todo o mundo, os governos, democráticos, colocaram os respectivos países em *lockdown*. Sem cautelas. Entre confinamentos e quarentenas obrigatórias, um recurso parece permitir - em face da falta de meios humanos para controlo efectivo de milhões de cidadãos - fiscalizar o cumprimento das directrizes estatais. A tentação executiva por esse controlo, universal, dos cidadãos preclude a fruição de múltiplas liberdades constitucionalmente consagradas. O racional da discussão que vinha sendo tido até agora[3], deslocou-se, por via do perigo abstracto que a pandemia comporta, da questão securitária *versus* liberdades fundamentais para "*saúde pública*" *versus* liberdades fundamentais.

Um pouco por todo o ocidente democrático, a tónica recursiva tem passado pelo uso da "*vigilância digital* estadual[4]". Tal como um pouco por todo o mundo, direitos humanos

2 Eficiência, especialidade, racionalidade, sistemas capacitativos e colaborativos público-privados. O trabalho dos dados ao serviço dos povos. https://www.technologyreview.com/s/614555/ai-in-health-care-capacity-capability-and-a-future-of-active-health-in-asia/

3 « Tribunal Constitucional chumba acesso das secretas a registos de comunicações», @ https://rr.sapo.pt/2019/09/19/politica/tribunal-constitucional-chumba-acesso-das-secretas-a-registos-de-comunicacoes/noticia/165164/

4 Por exemplo: https://www.wsj.com/articles/europe-tracks-residents-phones-for-coronavirus-research-11585301401

fundamentais[5] são colocados em teste face à imposição destas regras "excepcionais". O Estado de emergência tende a permitir, justificando múltiplas intrusões como *adequadas*[6], *necessárias e proporcionais*[7]. A questão, sendo excepcional e de carácter limitada no tempo, deveria ser pacificamente tolerada pelos cidadãos. Afinal, sob o manto de um fundamento como o "*interesse público*" [8] e salvaguarda da "*saúde pública*" até a limitação do escopo de protecção, desde logo, da privacidade de dados pessoais sensíveis claudica[9].

5 Por exemplo, no contexto da América do Sul, «Sociedade civil pede que tecnologias usadas devido à pandemia respeitem os Direitos Humanos», @ https://idec.org.br/noticia/sociedade-civil-pede-governos-da-america-latina-e-caribe-que-tecnologias-digitais-aplicadas

6 No parecer 32/2020, a CNPD, delimitando geograficamente a aplicação de videovigilância por drones ao concelho de Ovar, dada a excepcionalidade da cerca sanitária entretanto imposta, reitera que "(…)as restrições aos direitos fundamentais devem limitar-se ao estritamente necessário às finalidades visadas com este sistema de videovigilância ", recomendando, adicionalmente, "que se garanta que a captação de imagens assim realizada salvaguarde a privacidade daqueles que se encontrem nas respectivas habitações", e, "que se garanta o direito de acesso às imagens gravadas , nos termos legalmente previstos", bem como que se adoptem "medidas adequadas a garantir a integridade das imagens gravadas no processo de transferência dos registos(…) para o "contentor de informação encriptado"" . @ https://www.cnpd.pt/home/decisoes/Par/PAR_2020_32.pdf

7 Por exemplo, em Espanha, a AEPD: «(…)*Los fundamentos que legitiman/hacen posible dichos tratamientos son la necesidad de atender las misiones realizadas en interés público, así como la de garantizar los intereses vitales de los propios afectados o de terceras personas.* ***Las finalidades para las que pueden tratarse los datos son, únicamente, las relacionadas con el control de la epidemia****, entre ellas, las de ofrecer información sobre el uso de las aplicaciones de autoevaluación realizadas por las administraciones públicas o la obtención de estadísticas con datos de geolocalización agregados para ofrecer mapas que informen sobre áreas de mayor o menor riesgo.* ***Los datos que pueden obtenerse y utilizarse han de ser los que las autoridades públicas competentes consideren proporcionados/necesarios para cumplir con dichas finalidades.*** *Estos datos sólo podrán ser facilitados por quienes sean mayores de 16 años. En el caso de tratar datos de menores de 16 años, se requeriría de la autorización de sus padres o representantes legales.* ***Únicamente podrán tratar dichos datos las autoridades públicas competentes para actuar conforme a la declaración del estado de alarma****, es decir, el Ministerio de Sanidad y las Consejerías de Sanidad de las Comunidades Autónomas, que podrán cederse datos entre ellas, y a los profesionales sanitarios que traten a los pacientes o que intervengan en el control de la epidemia.****Las entidades privadas que colaboren con dichas autoridades sólo podrán utilizar los datos conforme a las instrucciones de estas y, en ningún caso, para fines distintos de los autorizados.*** **»** @ https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-apps-webs-autoevaluacion-coronavirus-privacidad

8 A limitação ao tratamento de dados sensíveis, por exemplo, de saúde sucumbe ante "*razões de interesse público nos domínios da saúde pública*", desde que «(…)***Tais atividades de tratamento de dados sobre a saúde autorizadas por motivos de interesse público não deverão ter por resultado que os dados sejam tratados para outros fins por terceiros, como os empregadores ou as companhias de seguros e entidades bancárias»*** (Considerando 54 in fine) .

Considerando *(54) « O tratamento de categorias especiais de dados pessoais pode ser necessário por razões de interesse público nos domínios da saúde pública, sem o consentimento do titular dos dados. Esse tratamento deverá ser objeto de medidas adequadas e específicas, a fim de defender os direitos e liberdades das pessoas singulares. Neste contexto, a noção de «saúde pública» deverá ser interpretada segundo a definição constante do Regulamento (CE) n.o 1338/2008 do Parlamento Europeu e do Conselho (11), ou seja, todos os elementos relacionados com a saúde, a saber, o estado de saúde, incluindo a morbilidade e a incapacidade, as determinantes desse estado de saúde, as necessidades de cuidados de saúde, os recursos atribuídos aos cuidados de saúde, a prestação de cuidados de saúde e o acesso universal aos mesmos, assim como as despesas e o financiamento dos cuidados de saúde, e as causas de mortalidade(…)* **».**

9 Confirmando o Considerando (54), ainda, da leitura conjunta **das alíneas g) e i) do Art.o 9, n.º2, RGPD**: «**G)** *Se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados*;», e**, i)** « *Se o tratamento for* ***necessário por motivos de interesse público no***

Mas há um "*senão*". O receio de que a excepcionalidade vire regra é real[10]. Com efeito, é inegável que, neste momento, os receios de Yuval Harari [11], criador de *Homo Deus*, sejam partilhados por muitos de nós. Tal como as considerações de Joel P. Trachtman, quanto aos benefícios de um mundo global[12]: benéfico se mais cooperativo, com capacidades regulatórias internacionais reforçadas ao nível da saúde, cibersegurança, proteção ambiental e crises financeiras.

Ambos convergem na necessidade de compromisso, de partilha, cooperação e solidariedade global. O que se conclui espontaneamente dos apontamentos citados, através de um silogismo categórico: ameaça sobre todos os países, ameaça global, logo, resposta de todos os países, global. Não obstante, será que hoje temos líderes políticos mundiais à altura dos desafios[13] pungentes que se nos colocam nestes termos?

E no futuro?

---

domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde *ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional*;». @ https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

10 Yuval Harari:«(…) *Many short-term emergency measures will become a fixture of life. That is the nature of emergencies. They fast-forward historical processes. Decisions that in normal times could take years of deliberation are passed in a matter of hours. Immature and even dangerous technologies are pressed into service, because the risks of doing nothing are bigger.", @* https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

11 Harari: «(…) *In this moment of crisis, the crucial struggle takes place within humanity itself. If this epidemic results in greater disunity and mistrust among humans, it will be the virus's greatest victory. When humans squabble – viruses double. In contrast, if the epidemic results in closer global cooperation, it will be a victory not only against the coronavirus, but against all future pathogens*.», @ https://time.com/5803225/yuval-noah-harari-coronavirus-humanity-leadership/

12 Joel P. Trachtman, «(…) *Not all global problems result from globalization. For those that do, globalization itself can ameliorate them to some extent. Furthermore, we can establish international laws and institutions to minimize those problems that do arise from globalization: globalized governance to respond to globalization-induced problems. This is smart globalization, and once we do it this way, it is likely that globalization should be retained because, on net, it will make us better off*.", @ https://www.bostonglobe.com/2020/03/30/opinion/not-all-global-problems-result-globalization/

13 Ainda Harari: «(…)*Today humanity faces an acute crisis not only due to the coronavirus, but also due to the lack of trust between humans. To defeat an epidemic, people need to trust scientific experts, citizens need to trust public authorities, and countries need to trust each other. Over the last few years, irresponsible politicians have deliberately undermined trust in science, in public authorities and in international cooperation. As a result, we are now facing this crisis bereft of global leaders that can inspire, organize and finance a coordinated global response*.», *idem*.

Gerd Leonhard, num exercício curioso reproduzido no Diário de Notícias, destaca dois aspectos cruciais. Circunscrevendo-nos à tecnologia, esta *"tornou-se a nova religião"*. "*Estamos a entrar num novo Renascimento*". *O próximo passo será regulamentá-la de forma mais apertada com o objetivo de que humanos e o próprio planeta beneficiem do progresso tecnológico.* Não obstante, esta relação acabará seduzir-se ante uma *vigilância estatal por meios tecnológicos* (que) *irá tornar-se o novo normal após as medidas extraordinárias que foram tomadas para controlar esta pandemia*[14].

E como já vai longo, para concluir, convocamos, novamente, a questão fundamental: "*Que mundo esperar do pós-covid19*"?

A provocação desconcertante e acutilante que se impõe, inclusive politicamente, não poderia ser outra: «*Of course, even if we disappear, it will not be the end of the world. Something will survive us. Perhaps the rats will eventually take over and rebuild civilization. Perhaps, then, the rats will learn from our mistakes. But I very much hope we can rely on the leaders assembled here, and not on the rats.*» [15]

Nesta nova edição da «Cyberlaw by CIJIC», procuramos sustentar o crescimento paralelo que o Mestrado de Segurança da Informação e Direito do Ciberespaço[16] vai granjeando. É pois, com orgulho, que passaremos a destacar produção deste, com maior regularidade. Afinal, este é um desígnio da própria criação da revista. Provavelmente, num futuro não muito distante, estará na calha a edição em papel de futuras edições. Se há questão que se nos colocou com o teletrabalho foi: qual a redundância digital? *Ie*, sem acesso à internet, ou sem eletricidade/bateria, como é que seria possível aceder a conteúdos para efeitos de estudo? Como ler(aceder) nestas circunstâncias? Como mitigar a "info-exclusão" quando o sistema não é propriamente redundante na acessibilidade[17]?

14 «Não haverá normal: futuristas preveem mudanças permanentes pós-coronavírus», @ https://www.dn.pt/dinheiro/nao-havera-normal-futuristas-preveem-mudancas-permanentes-pos-coronavirus-11987179.html

15 Yuval Harari: «Yuval Harari's blistering warning to Davos», @ https://www.weforum.org/agenda/2020/01/yuval-hararis-warning-davos-speech-future-predications/

16 Mais informações @ : https://fenix.tecnico.ulisboa.pt/cursos/msidc

17 Por exemplo, «Ministro Siza Vieira admite aulas por canais "estilo youtube" ou TV por cabo.», @ https://observador.pt/2020/03/29/ministro-siza-vieira-admite-aulas-por-canais-estilo-youtube-ou-tv-por-cabo/

Reavendo, nesta edição, incorporando conteúdo em inglês escrito, por força de deveres de participação, cooperação e colaboração internacional[18] que muito nos orgulha, procuramos revisitar temas como cibersegurança em contexto marítimo, dados pessoais e dados não pessoais, monitorização de trabalhadores em contexto laboral, a regulação jurídica do ciberespaço - mutação do paradigma à luz do acórdão James Elliot, *Phishing*, redes sociais e manipulação da opinião pública, o problema da mobilidade em contexto organizacional, e, os desafios da cibersegurança forense de *smartphones* no continente africano. Os temas são oportunos. São, igualmente, desafiantes. São, finalmente, abertos a colaboração múltipla, participada.

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

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

Boas leituras.

Lisboa, FDUL, 29 de Março de 2020

Nuno Teixeira Castro

Mas, sem acesso internet, ou sem cabo – até porque a cobertura não é de 100%, há, pelo menos, cerca de 20% de famílias sem acesso ao Cabo – como é que as crianças e adolescentes que se encontrem nesta situação se integram? Como é que se combate esta exclusão digital?

18 Um trabalho colaborativo ímpar. @ https://networkofcenters.net/center/cyberlaw-research-centre-university-lisbon-school-law-cijic

CYBERLAW by CIJIC

CIBERSEGURANÇA NO SETOR MARÍTIMO

A. GAMEIRO MARQUES *

* Diretor-Geral do Gabinete Nacional de Segurança e Autoridade Nacional de Segurança, Oficial da Marinha Portuguesa.

RESUMO

No âmbito da Conferência realizada em Dezembro de 2019 na Faculdade de Direito da Universidade de Lisboa, sobre Cibersegurança no Setor Marítimo, partilhamos algumas considerações sobre um tema que nos é especialmente grato. Neste conspecto, consideramos pertinente adiantar desde logo o repto seguinte: "Ao longo dos tempos a história tem-nos mostrado que sem segurança não há desenvolvimento sustentado. A segurança, incluindo a cibersegurança, é uma responsabilidade coletiva onde todos os atores, sejam públicos ou privados, devem cooperar para que juntos, possamos estar mais preparados para as ameaças que conhecemos e sobretudo para as que desconhecemos. Tal como noutros setores da sociedade, também no setor marítimo cada vez mais dependemos da tecnologia para viver como vivemos.»

***Palavras-Chave**: Cibersegurança, tecnologia; Setor Marítimo; Valor estratégico; "security by design"; "safety"*

1. INTRODUÇÃO

Começo por agradecer o gentil convite que me foi dirigido pelo Sr. Professor Eduardo Vera Cruz, para proferir esta comunicação subordinada ao tema "Cibersegurança no Setor Marítimo", que congrega duas áreas que muito me dizem: a cibersegurança, por ser aquela em relação à qual detenho a responsabilidade de Direção superior da entidade do Estado onde funciona o Centro Nacional de Cibersegurança, a quem incube a coordenação da resposta a incidentes de cibersegurança, incluindo a capacitação da sociedade para os desafios que o mundo digital no aporta; e o mar, por ser, desde há algumas dezenas de anos Oficial da Marinha Portuguesa, e em relação ao qual mantenho um incessante fascínio, interesse e gosto por tudo o que com ele se relaciona e por ele estar, efetivamente, na base da nossa identidade enquanto Estado Nação e ainda por constituir um recurso fundamental para o nosso desenvolvimento económico. Assim, é com redobrado gosto que me encontro nesta prestigiada entidade para partilhar algumas reflexões sobre o tema.

Agradeço, ainda, a todos os presentes. O estarem aqui é para mim um claro sinal do interesse que estes assuntos vos suscitam, uma vez que, sendo tão atuais, são cada vez mais condicionadores da forma como vivemos, incluindo o modo como as democracias e assim os direitos liberdades e garantias dos cidadãos se exercem. E este assunto, que poderia ser tema para um outro debate, é cada vez mais relevante e potencialmente determinante quanto à forma como cada vez mais os poderes detidos, quer por Estados quer por grandes empresas transnacionais, se irão exercer ao nível geoestratégico.

No início deste ano tive o grato prazer de ouvir, com muito interesse e atenção, na Academia de Marinha uma alocução proferida pelo Sr. Professor Dr. António Barreto intitulada "O Mar como património". Reli a sua comunicação e retive algumas ideias que gostaria de trazer à colação: o Sr. Professor afirmou que, para a sua definição de identidade, contava com "a natureza, a geografia, o património e a história". Na sua alocução referiu ainda que "a singularidade de Portugal (e de qualquer outro país) reside na combinação única da sua natureza com a geografia e a história. A geografia mais o património de um

país são, em grande parte, a sua identidade. O património … é toda a criação cultural, técnica, artística e ideológica de um povo." A questão que aqui coloco para reflexão é a seguinte: será que poderemos reforçar a nossa singularidade e o nosso património identitário através do Mar, no contexto da rápida evolução que o digital constantemente nos aporta, mais concretamente no âmbito do tema desta conferência? Se sim, como poderemos fazer isso?

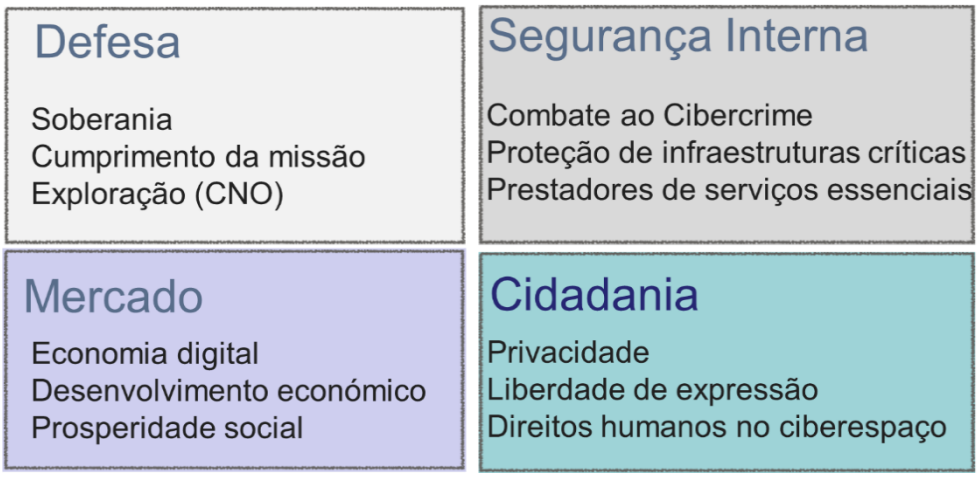
2. ENQUADRAMENTO CONCEPTUAL

Do ponto de vista doutrinário, o Mar possui cinco dimensões estratégicas, a saber: a ambiental, a política, a económica, a social e a securitária. A **dimensão ambiental** contempla as características intrínsecas do Oceano inerentes ao facto de 70% da terra ser coberta com água, ser um natural sumidouro de Dióxido de Carbono, constituir uma cada vez mais vital fonte de Oxigénio, um determinante regulador do clima, para além de ser uma preciosa fonte de biodiversidade. A **dimensão geopolítica** por constituir um espaço de afirmação e de disputa de poder, que povos, ao longo da história da humanidade (como foi o nosso caso nos séculos XV e XVI), foram conquistando para afirmação planetária da sua influência geoestratégica. A **dimensão económica**, uma vez que 90% do comércio mundial se faz pelo mar, as comunicações que materializam 97 % da Internet tal como hoje a conhecemos estão baseadas em milhares de Km de cabos submarinos (em que Portugal representa um local particularmente de destaque por ser o único País da União Europeia ligado por este meio à maioria dos continentes), para além de ser uma enorme fonte de energia e de recursos naturais da mais diversa índole. A **dimensão social** porque um terço da população mundial vive em zonas costeiras, 80% das mega cidades estão implantadas ao longo das zonas ribeirinhas e cerca de 30% dos empregos existentes estão direta ou indiretamente ligados à economia do Mar. Finalmente, a **dimensão securitária**, que contempla atividades desde as que endereçam situações de "safety", de baixo espetro de intensidade e normalmente não intencionais, até às de Defesa Naval, numa lógica multidimensional, eventualmente suscetíveis de ser enquadradas no conceito de "ameaças híbridas", atualmente consagrado quer na doutrina da OTAN quer na da EU.

Por outro lado, o ciberespaço é um domínio que hoje em dia é utilizado quer por Estados quer por organizações supranacionais, para afirmação do seu poder geoestratégico. E é neste contexto que conceptualmente podemos afirmar que a cibersegurança possui 4 dimensões: a de Defesa, como espaço ou domínio de exercício da soberania e da proteção dos interesses de um Estado no ciberespaço, designadamente através do planeamento e condução de *Computer Network Operations*; uma segunda, no âmbito da "segurança interna" que contempla o combate ao cibercrime, a proteção de infraestruturas críticas e prestadores de serviços essenciais ao saudável funcionamento da sociedade; uma terceira, a dimensão económica, como acelerador e facilitador da economia digital, uma vez que bem

sabemos que não existe desenvolvimento económico sustentável sem segurança, e finamente a dimensão de cidadania, com enfoque na privacidade do cidadão, nos seus direitos liberdades e garantias, incluindo a liberdade de expressão. Esta é, talvez hoje, a dimensão mais ameaçada, na medida em que existem reiteradas evidências de Estados (ou entidades por si patrocinadas), que cada vez mais usam o ciberespaço para controlo e limitação da liberdade dos seus cidadãos.

As dimensões da cibersegurança



Vejamos, de seguida, como é que as duas se relacionam, i.e., como é que as dimensões da visão estratégica do mar se ligam com as dimensões da cibersegurança:

Valor estratégico do Mar vs Cibersegurança

		CIBERSEGURANÇA			
	Dimensões	**Defesa**	**Seg. Interna**	**Economia**	**Cidadania**
VALOR EST. DO MAR	**Ambiental**				
	Geopolítica				
	Económica				
	Social				
	Securitária				

Ainda que sem a profundidade de uma análise científica, julgo que fica claro que as dimensões do valor estratégico do Mar têm uma profunda relação com as dimensões da cibersegurança, o que indicia que, quaisquer iniciativas enquadrados no primeiro, devem ser acompanhadas dos mecanismos adequados nas componentes da cibersegurança, para que o uso do mar não fique quartado de todo o seu potencial, sobretudo quando cada vez mais as atividades neste importante setor dependem do digital e assim do ciberespaço.

3. CARACTERIZAÇÃO DO SETOR MARÍTIMO E OS CIBERATAQUES NESTE SETOR

Quando neste contexto falamos do Mar referimo-nos concretamente a três componentes do setor marítimo: (i) as infraestruturas portuárias e de vigilância costeira incluindo as respetivas autoridades; (ii) os navios em geral, em particular os que possuem guarnições multinacionais, cujos armadores são muitas vezes proprietários de embarcações que arvoram bandeiras de conveniência; (iii) e as cadeias logísticas que são responsáveis não só pelo abastecimento dos próprios navios, como pela garantia que as mercadorias são transportadas da sua origem ao cliente de forma segura e determinística.

As infraestruturas portuárias são complexas e têm a sua atividade ancorada em sistemas de IT bastante elaborados, que, sendo fundamentais para as atividades dos portos, não foram concebidos, de uma forma geral, com o princípio da "security by design". O mesmo acontece com os sistemas de vigilância marítima, desde os costeiros aos portuários.

Os navios são cada vez mais concentrados de tecnologia da mais diversa índole e origem, como forma de incrementar os respetivos automatismos e assim diminuir a necessidade de guarnições numerosas, incrementando, desta forma, a rentabilidade da atividade económica. Como é consabido, já existem experiências de operações com navios de dimensões assinaláveis sem qualquer ser humano a bordo para respetiva operação.

Para aumentar a sua eficiência, a cadeia logística recorre a vários tipos de sistemas de informação e comunicação, desde os que permitem efetuar o rastreamento dos contentores na zona portuária propriamente dita até aos que, como a Janela Única Logística (JUL), permitem efetuar o processamento do navio e respetiva carga de forma desmaterializada, envolvendo as diversas entidades necessárias ao respetivo tratamento ao longo de todo o processo.

Se a este complexo contexto adicionarmos a baixa sensibilidade da comunidade marítima para a importância da cibersegurança no setor; a falta de um sólido corpo de recomendações e standards que se encontra em desenvolvimento, mas ainda não é exaustivo; a fragmentação da governação dos assuntos relacionados com este setor; a falta

de uma abordagem transversal aos ciber riscos, que são dilatados pela diversidade dos atores em jogo; e finalmente a inexistência de incentivos económicos à implementação de boas práticas de cibersegurança no setor marítimo, temos o que é necessário para que as coisas possam não correr satisfatoriamente.

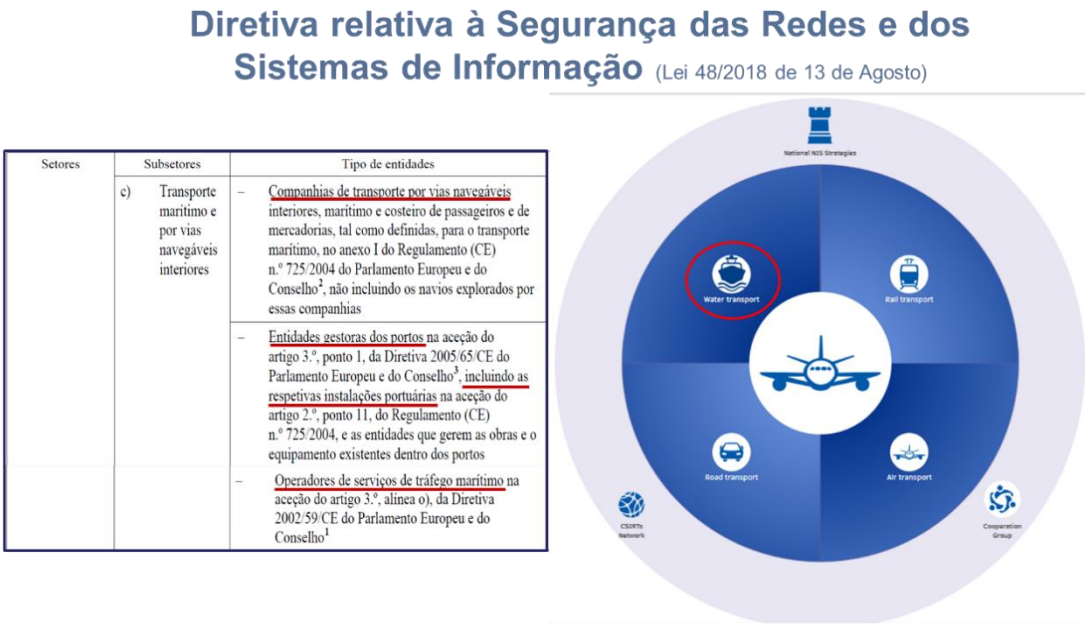
Os factos são demonstrativos disto mesmo (mostrar com os tipos de ataques mais comuns no setor e os mais recentes e significativos – 3 slides). O que mais nos deve preocupar é que, para além do grave impacto económico e reputacional que tal pode trazer a um armador, a um porto, enfim a um País, um incidente de cibersegurança perpetrado numa grande instalação portuária ou num navio pode provocar um problema ainda maior de "safety", com danos ambientais e mesmo perda de vidas humanas. Por outras palavras, estamos convencidos que negligenciar estes assuntos poderá impactar negativamente o valor estratégico do mar em todas as suas dimensões. É, por isso, necessário agir de forma sistemática, estruturada e perseverante.

Consciente deste facto, a Agência da União Europeia para a segurança das redes e da informação (ENISA) publicou em dezembro de 2011 um relatório que aferiu o "estado da arte" na união no que à cibersegurança no setor marítimo diz respeito. Já naquela altura o documento mostrava evidências de que o setor sofria de problemas de diversa índole, que o tornavam muito vulnerável a ataques perpetrados por pessoas ou organizações mal-intencionadas.

Desde então, várias iniciativas da parte da UE ocorreram, visando mitigar os riscos de segurança (que incluía a cibersegurança), das quais destacaria a publicação, em 24 de Junho de 2014 da EU Maritime Security Strategy[1], cujo plano de ação foi divulgado em 16 de Dezembro desse mesmo ano[2]. Posteriormente, foram desenvolvidos dois relatórios relativos ao seu estado de execução, em 22 de Junho de 2016[3], e 14 de Junho de 2017[4] respetivamente. Já em 26 de junho de 2018 foi publicado uma revisão do plano de ação original bem como as conclusões do Conselho sobre esse documento[5].

1 https://ec.europa.eu/maritimeaffairs/policy/maritime-security_en
2 https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf
3 https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/swd-2016-217_en.pdf
4 https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/swd-2017-238_en.pdf
5 https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/2018-06-26-eumss-revised-action-plan_en.pdf

Da leitura deste conjunto de documentos pode-se apurar que o tema da cibersegurança se encontra contemplado, estando relacionado, quer com a *EU Cybersecurity Framework*, anunciada pelo Presidente da Comissão Europeia em setembro de 2017 quer, mais importante ainda, com a Diretiva sobre a Segurança das Redes e dos Sistemas de Informação (Diretiva SRI) adotada pelo Parlamento Europeu em 6 de julho de 2016[67]. Esta é a primeira legislação da União Europeia sobre segurança do ciberespaço, que estabelece um conjunto de medidas para capacitar os Estados-Membros para proteger, prevenir, reagir e combater incidentes desta natureza. Entre outros objetivos, visa aumentar a cooperação na União nesta matéria e criar uma sólida cultura de segurança em sectores essenciais para a sociedade que dependam fortemente do domínio digital.



https://www.enisa.europa.eu/news/enisa-news/enisa-releases-online-nis-directive-tool-showing-per-sector-the-national-authorities-for-operators-of-essential-services-and-digital-service-providers

O Anexo II da Diretiva (e também no anexo à Lei 46/2018 de 13 de agosto que a transpõe para a legislação nacional) elenca os serviços designados como "essenciais" para a sociedade, que incluem os transportes em geral e o transporte marítimo em particular. Todavia não contempla um dos mais importantes e também um dos mais difíceis componentes: os navios. Nem tão pouco fornece orientações específicas quanto à melhor forma de mitigar a governação fragmentada que se observa neste setor, o que já era um problema identificado no relatório da ENISA de dezembro de 2011.

6 https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L1148&from=PT
7 Transposta para a legislação nacional através da já mencionada Lei 46/2018 de 13 de agosto

Com a insistência de alguns estados membros, entre os quais Portugal, a ENISA voltou a debruçar-se sobre o estado da cibersegurança no setor marítimo, optando por uma abordagem segmentada: acabou de publicar e apresentar a 26 de novembro em Lisboa num workshop sobre cibersegurança no setor marítimo um relatório sobre a cibersegurança no subsetor portuário em 2019. Este relatório[8] identifica de forma concreta as maiores ameaças que o setor enfrenta no ciberespaço e caracteriza os vários cenários mais plausíveis de ocorrerem no contexto portuário, incluindo as técnicas e os procedimentos para lhes fazer face.

Relativamente aos navios, diversas entidades internacionais ligadas ao setor marítimo, das quais destacaria a *International Maritime Organiza*tion (IMO), o *Oil Companies International Marine Forum* (OCIMF), e a *International Maritime Contractors Association* (IMCA), desenvolveram e atualizaram documentação já existente sobre a segurança (security) a bordo dos navios, incluindo a cibersegurança ainda que sejam "orientações" e não regras a cumprir.

Por seu lado, a Comissão Europeia definiu que a cibersegurança no setor marítimo é uma prioridade estratégica[9]. Através do *NIS Cooperation Group*, no qual Portugal é representado pelo CNCS, aquela entidade lidera os trabalhos que esperemos venham dar origem a planos de ação concretos para tornar este setor, que tanto depende do digital, mais resiliente a ataques cibernéticos.

8https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector

9 Svetlana Schuster, Dr. Nineta Polemi, Comissão Europeia, Reunião do Cooperation Group da CE, 4SET19

4. SITUAÇÃO EM PORTUGAL

A Lei 46/2018 de 13 de agosto efetuou a transposição da Diretiva SRI já mencionada. Esta legislação estabelece que o CNCS é o ponto focal para os assuntos de cibersegurança nos setores que prestam serviços essenciais à sociedade, entre os quais se encontra o setor dos transportes marítimos.

Neste âmbito, o Centro tem trabalhado com os reguladores de todas as áreas previstas naquela Lei na identificação dos respetivos operadores de serviços essenciais e do modelo que deverá enquadrar a respetiva regulação, a qual já se encontra em curso. Assim, foram identificadas e notificadas mais de um milhar de entidades das quais 11 pertencem ao setor dos transportes marítimos.

Uma vez que, de uma forma global, a atuação do CNCS se alicerça no princípio da subsidiariedade, estamos a trabalhar, em estreita colaboração com os reguladores do setor (AMT e DGRM), que o preconizado naquela diretiva e transposto na legislação nacional, seja cumprido e devidamente acompanhado. Neste enquadramento, iremos recomendar a aplicação de um modelo que já foi utilizado noutras áreas e que consiste na criação de um *Information Sharing and Analysis Center* (ISAC)[10] específico, desejavelmente endossado e apoiado pelo nível político, como por exemplo a Comissão Interministerial para os Assuntos do Mar (CIAM). O CNCS tem documentação produzida e experiência na ajuda à criação destes mecanismos em Portugal, e pode ser um facilitador da construção de algo congénere no nosso País. Todavia, considero que o nível de ambição deve ser maior. De facto, julgo que se deveria desenvolver um modelo de prestação de serviços colaborativo na comunidade marítima, mais concretamente com os portos nacionais, de modo a tornar as políticas e os procedimentos de segurança de informação coerentes e interoperáveis, incrementar a capacidade de recurso a fundos da UE (CEF-TELECOM) e otimizar o emprego de recursos humanos e financeiros (CAPEX e OPEX) na edificação e manutenção da capacidade de cibersegurança portuária.

10 https://www.cncs.gov.pt/cooperacao/isac/

Paralelamente, e como nação cuja identidade e singularidade está indelevelmente ligada ao Mar, julgo que nos fóruns internacionais, designadamente ao nível das instâncias europeias, Portugal deverá continuar a trazer e a perseguir os assuntos da cibersegurança no setor marítimo para agenda, pois assim estará a pugnar pelos seus interesses e a honrar a sua identidade e singularidade.

5. CONCLUSÕES

Ao longo dos tempos a história tem-nos mostrado que sem segurança não há desenvolvimento sustentado. A segurança, incluindo a cibersegurança, é uma responsabilidade coletiva onde todos os atores, sejam públicos ou privados, devem cooperar para que juntos, possamos estar mais preparados para as ameaças que conhecemos e sobretudo para as que desconhecemos. Tal como noutros setores da sociedade, também no setor marítimo cada vez mais dependemos da tecnologia para viver como vivemos. Mas julgo que não podemos deixar que seja a tecnologia a determinar como vivemos. São, sem dúvida, as pessoas que devem continuar a contar. E também devem ser as pessoas que devem determinar e marcar a diferença e o caminho.

Regressando ao ponto de partida desta reflexão, voltaria a citar o Professor Dr. António Barreto no âmbito da conferência a que me referi: *O mar é natureza. Por definição, não faz parte do património de um país, entendendo este como essencialmente cultural e técnico. O património é obra humana e resulta da história e da cultura. Mas há realidades naturais que se transformam, pela história, pela cultura e pela técnica, em obras de património. Assim é com o mar para os Portugueses. O mar da pesca, da marinha, das viagens, dos transportes, das praias, do desporto, dos recursos económicos, da fonte de energia, dos civis e dos militares é património. O mar do poema, da literatura, da mitologia, do sonho, dos descobrimentos, da expansão, do império, da Europa e da economia é património e identidade. Há um mar igual ao dos outros, há um mar que é português.* Fim de citação.

Estou convicto de que o valor estratégico do Mar, magnificamente retratado pelo Sr. Professor nestas suas palavras, poderá ser engrandecido através do ciberespaço, se a respetiva segurança estiver sempre presente de forma pragmática e consequente, através de Portugal, na agenda nacional e internacional. Desta forma, enquanto portugueses, estaremos também a reforçar a nosso património e assim a nossa identidade.

NA BORDA: DADOS PESSOAIS E NÃO PESSOAIS NOS DOIS REGULAMENTOS DA UNIÃO EUROPEIA[1]-[2]

MANUEL DAVID MASSENO [3]

1 Versão em Língua Portuguesa da Comunicação apresentada no *IV Congreso Interactivo Virtual - Humanos Máquinas Derecho ¿amigos ou inimigos?*, sediado na *Universidad Nacional de Lanús*, (Argentina), a 20 de novembro de 2019, antes exposta como "On the Waterfront: 'Personal' and 'Non-Personal' Data at Both EU Regulations", na *Nordic Conference on Legal Informatics 2019 - Digital Rights, Digital Lawyers, Digital Courts*, realizada na *Lapin yliopisto* (Universidade da Lapónia, Finlândia) dia 14 de novembro de 2019. Esta versão está em publicação nas *Actas* do referido *Congreso*, pela *Editorial Astrea*, de Buenos Aires.

2 Atendendo à circunstância de se tratar de uma publicação em formato digital, sobretudo destinada à América Latina, apenas serão indicadas referências bibliográficas disponíveis na Internet e em Acesso Aberto, assumindo as consequências resultantes de não o fazer com outras, mais marcantes, apenas publicadas em papel ou sujeitas a pagamento.

3 Professor Adjunto do IPBeja - Instituto Politécnico de Beja, onde também integra as Coordenações do Laboratório UbiNET – Segurança Informática e Cibercrime e do MESI – Mestrado em Engenharia de Segurança Informática, sendo ainda o seu Encarregado da Proteção de Dados. Pertence à EDEN – Rede de Especialistas em Proteção de Dados da Europol – Agência Europeia de Polícia e ao Grupo de Missão "Privacidade e

Segurança" da APDSI – Associação para a Promoção e Desenvolvimento da Sociedade da Informação, em Portugal, ao Grupo de Estudos de Direito Digital e *Compliance* da FIESP – Federação das Indústrias do Estado de São Paulo, à Comissão Estadual de Direito Digital da Ordem dos Advogados do Brasil, Seção de Santa Catarina e à Comissão de Direito Digital da Subseção de Campinas da OAB.

RESUMO

No contexto regulatório da sua Economia dos Dados, a União Europeia dispõe de regras distintas para os tratamentos de dados pessoais e de dados não pessoais, embora com níveis de densidade diferentes. Porém, a evolução das técnicas de anonimização e de personalização dos dados tornaram instáveis os limites entre aos âmbitos de aplicação material de cada um dos regimes jurídicos, o que acabou por ser assumido pelo Legislador. Assim, este texto explora os critérios normativos subjacentes a tais fronteiras, em especial no que se refere à personalização potencial de dados anónimos ou anonimizados e procura identificar os riscos inerentes, assim como os instrumentos técnicos e normativos disponíveis para os minimizar, desde as avaliações de impacto em proteção de dados até às certificações previstas, incluído as relativas à cibersegurança.

Palavras-Chave: Anonimização, Certificação, Dados, Risco, União Europeia.

RESUMÉN

En el marco de la regulación de la Economía de los Datos, la Unión Europea dispone de reglas distintas para los tratamientos de datos personales y de datos no personales, aún que con niveles de densidad diferentes. Sin embargo, la evolución de las técnicas de anonimización y de personalización volvieron instables los límites entre los ámbitos de aplicación material de cada uno de los regímenes jurídicos. Por consiguiente, este texto explora los criterios normativos subyacentes a tales confines, en especial en que concierne a la personalización potencial de datos anónimos o anonimizados y busca identificar los riegos inherentes, además de los instrumentos técnicos y normativos disponibles para minimizarlos, desde las evaluaciones de impacto relativas a la protección de datos hasta las certificaciones previstas, incluso las que tienen que ver con la ciberseguridad.

Palabras Clave: Anonimización, Certificación, Datos, Riesgo, Unión Europea.

"Assistimos a uma nova revolução industrial induzida pelos dados digitais, a informática e a automatização. As atividades humanas, os processos industriais e a investigação conduzem, todos eles, à recolha e ao tratamento de dados numa escala sem precedentes, favorecendo o surgimento de novos produtos e serviços, assim como de novos processos empresariais e metodologias científicas [e] Desde que as regras relativas à proteção dos dados pessoais, quando aplicáveis, sejam cumpridas, os dados, uma vez registados, podem ser reutilizados muitas vezes sem perda de fidelidade. Esta geração de valor agregado está no cerne do conceito de cadeia de valor dos dados. [tendo sempre presente que] O direito fundamental à proteção dos dados pessoais aplica-se aos grandes volumes de dados no caso de se tratar de dados pessoais: o seu tratamento tem de respeitar todas as regras aplicáveis em matéria de proteção de dados." (COM/2014/0442 final, de 2 de julho).

1. *as referências*

Antes de mais, é necessário ter presente que, uma vez operada a *constitucionalização* da Proteção de Dados operada em 2009 com a entrada em vigor do *Tratado de Lisboa*, com a inclusão da mesma no *Tratado sobre o Funcionamento da União Europeia* (Art.º 16.º) e com a receção da *Carta dos Direitos Fundamentais* (Art.º 8.º) no Direito Primário da União (*Ex vi*, Art.º 6.º do *Tratado da União Europeia*), o respetivo microssistema ficou consolidado, ainda que não completo, com a adoção do 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 e que revoga a Diretiva 95/46/C (*Regulamento Geral sobre a Proteção de Dados*) – o *RGPD*[1].

1 Os estudo sobre o RGPD são hoje multidão. Mas, sempre podemos referir os estudos de Angelina TEIXEIRA (2016), de Alfonso ORTEGA JIMÉNEZ e Juan José Gonzalo DOMENECH (2018) e ainda de Chris HOOFNAGLE, Bart van der SLOOT e Fredrik ZUIDERVEEN BORGESIUS (2019).

Ao mesmo tempo e enquanto ainda decorria o processo legislativo correspondente ao *RGPD*, a *Comissão* [presidida por Jean-Claude] *Juncker* avançou com a "Estratégia para o Mercado Único Digital na Europa" (COM/2015/192 final, de 6 de maio), dando continuidade a orientações que vinham da *Comissão* [presidida por José Manuel Durão] *Barroso* e constavam da Comunicação "Para uma economia dos dados próspera" (COM/2014/0442 final, de 2 de julho)[2].

O que foi explicitado através de uma sua nova Comunicação, "Construir uma Economia Europeia dos Dados" (COM/2017/9 final, de 10 de janeiro), agora centrada na necessidade de avançar com disciplinas para os "dados em bruto", com um especial ênfase na sua portabilidade em todo o Mercado Interno da União[3]. Daí que a Comissão tenha avançado com a *Proposta* (COM/2017/0495 final, de 13 de setembro) do que veio a ser o Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho de 14 de novembro de 2018 relativo a um regime para o livre fluxo de dados não pessoais na União Europeia – o *Regulamento LFD*[4].

No entanto e entre outras, voltou a ser colocada questão a necessitar de respostas jurídicas tão robustas quanto possível, a de existir uma borda, mutável de acordo com a evolução das tecnologias, entre os âmbitos de aplicação material de ambos os Regulamentos, isto é, entre os dados pessoais e os dados não pessoais. A determinação dessa borda, e um breve esboço do que fazer, constitui o objeto desta intervenção.

---

2 Aliás, na sua "Estratégia para o Mercado Único Digital na Europa" a Comissão acentua que "As empresas e os consumidores continuam a não se sentirem suficientemente confiantes para adotar serviços de computação em nuvem transfronteiras para fins de armazenamento ou processamento de dados, devido a preocupações relacionadas com a segurança, o respeito dos direitos fundamentais e a proteção de dados em termos mais gerais. A adoção do Pacote Reforma da Proteção de Dados assegurará que o tratamento de dados pessoais seja regido por regras atualizadas e uniformes em toda a União. No entanto, frequentemente os contratos excluem, ou limitam de forma significativa, a responsabilidade contratual do prestador de serviços de computação em nuvem caso os dados deixem de estar disponíveis ou fiquem inutilizáveis, ou dificultam a rescisão do contrato. Isso significa que não existe, de facto, uma portabilidade dos dados. No domínio da proteção de dados, tanto o atual como o futuro quadro legislativo impede as restrições à livre circulação de dados pessoais na União. As restrições à livre circulação de dados por outros motivos não são abordadas. [Pelo que] A Comissão irá propor em 2016 a Iniciativa Europeia «Livre Circulação de Dados» que aborda a questão das restrições à livre circulação de dados por motivos não relacionados com a proteção de dados pessoais na UE e das restrições injustificadas sobre a localização de dados para fins de armazenamento ou de tratamento. A iniciativa abordará as questões emergentes de propriedade, interoperabilidade, utilizabilidade e acesso aos dados nomeadamente em situações entre empresas, entre empresas e consumidores e dados gerados por máquinas e máquina-a-máquina. Incentivará o acesso aos dados públicos a fim de contribuir para dinamizar a inovação."

3 Sobre estes Documentos e em termos gerais sobre o Mercado Único Digital e por todo, é de atender à exposição de Fernanda Ferreira DIAS (2016).

4 Para uma perspetiva geral do *Regulamento LFD*, embora tratando essencialmente de outras questões, Pedro DE MIGUEL ASENSIO (2019).

2. *até mesmo nos limites*

Para começar, temos que o *RGPD* "aplica-se ao tratamento de dados pessoais" (Art.º 2.º n.º 1), não só a uma "pessoa singular [física] identificada", mas também a uma que venha a ser "identificável", em termos potenciais e através de meios técnicos, incluindo os indiretos[5]-[6].

Consequentemente, do *RGPD* resulta que: "[…] Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação." (*Considerando* 26 *in fine*)

Por sua vez, o *Regulamento LFD* veio esclarecer que o mesmo "aplica-se ao tratamento de dados eletrónicos que não sejam dados pessoais" (Art.º 2.º n.º 1), entendendo estes "na aceção do artigo 4.º, ponto 1, do Regulamento (UE) 2016/679 [o *RGPD*]" (Art.º 3.º n.º 1)[7].

---

5 Ou seja "[…] que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;" (Art.º 4.º 1). O que incluí os quase-identificadores e os metadados, ao ser certo que, "As pessoas singulares podem ser associadas a identificadores por via eletrónica […] tais como endereços IP (protocolo internet) ou testemunhos de conexão (*cookie*) ou outros identificadores como as etiquetas de identificação por radiofrequência." (*Considerando* 30). Diversamente, a propósito da reindentificação de dados pseudonimizados, o *RGPD* acrescenta que "[…] importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica." (*Considerando* 26).

6 Neste particular, há ainda que atender ao conteúdo do Parecer 4/2007 sobre o conceito de dados pessoais, de 20 de junho de 2007, do *Grupo de Trabalho do 29.º* [o qual antecedeu o CEPD – Comité Europeu para a Proteção de Dados], assim como à Jurisprudência do Tribunal de Justiça da União Europeia, a qual culminou no Acórdão proferido no Processo C‑582/14, *Patrick Breyer*, de 19 de outubro de 2016. Quanto a estas referências, são de atender os estudos, complementares entre si, de Rossana DUCATO (2016), de Nadezhda PURTOVA (2018), de A. Barreto MENEZES CORDEIRO (2018) e ainda de Lorenzo dalla CORTE (2019), inclusive quanto a referências bibliográficas adicionais.

7 Isto, porque "A internet das coisas, a inteligência artificial e a aprendizagem automática, que estão em expansão, representam grandes fontes de dados não pessoais, por exemplo, em consequência da sua utilização em processos automatizados de produção industrial. Exemplos concretos de dados não pessoais incluem conjuntos de dados agregados e anonimizados utilizados para a análise de grandes volumes de dados, os dados relativos à agricultura de precisão que podem ajudar a controlar e a otimizar a utilização de pesticidas e de água ou ainda dados sobre as necessidades de manutenção de máquinas industriais." (*Considerando* 9).

Assim, ao *Regulamento Geral sobre Proteção de Dados* é conferida uma *vis atractiva*, sempre que não seja possível identificar os dados em presença como, exclusivamente, não pessoais. Pelo que, "No caso de um conjunto de dados compostos por dados pessoais e não pessoais, o presente regulamento aplica-se aos dados não pessoais do conjunto de dados. Caso os dados pessoais e não pessoais de um conjunto de dados estejam indissociavelmente ligados, o presente regulamento não prejudica a aplicação do Regulamento (UE) 2016/679" (Art.º 2.º n.º 2 do *Regulamento LFD*).

3. *mas, afinal nada é para sempre*

No que concerne a distinção que nos ocupa, temos que a Diretiva 95/46/CE, que precedeu o *Regulamento sobre Proteção de Dados*, assentara numa *fictio iuris*, ao abstrair-se da evolução da técnica, ainda que previsível. Daí, na mesma constar que "[…] os princípios da proteção não se aplicam a dados tornados anónimos de modo tal que a pessoa já não possa ser identificável [os quais são, também] conservados sob uma forma que já não permita a identificação da pessoa em causa." (*Considerando* 26).

O que já não ocorre com o *RGPD*, ao ser assumido que "As pessoas singulares podem ser associadas a identificadores por via eletrónica, fornecidos pelos respetivos aparelhos, aplicações, ferramentas e protocolos [e também que] Estes identificadores podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares." (*Considerando* 30).

Por sua vez, o *Regulamento LFD* é transparente, ao explicitar que "Se os progressos tecnológicos permitirem transformar dados anonimizados em dados pessoais, esses dados devem ser tratados como dados pessoais, e o Regulamento (UE) 2016/679 deve ser aplicado em conformidade" (*Considerando* 9 *in fine*), o mesmo valendo para os dados originariamente anónimos, por identidade de razão.

Porém, é necessário ter presente que não estamos face a algo verdadeiramente novo. Aliás, as Instituições da União Europeia foram ficando cientes desta realidade, como mostram os Pareceres do *Grupo de Trabalho do Art.º 29.º*.

Assim e num primeiro momento, tal ocorreu a propósito dos riscos para a proteção dos dados dos administrados que poderiam advir da transposição da Diretiva 2003/98/CE do Parlamento Europeu e do Conselho, de 17 de Novembro de 2003, relativa à reutilização de informações do sector público, designadamente, o Parecer n.º 7/2003 sobre a reutilização de informações do setor público e a proteção dos dados pessoais, de 12 de dezembro. A que se seguiu o Parecer n.º 6/2013 sobre dados abertos e reutilização de informações do setor público (ISP), de 5 de junho, suscitado pela adoção da Diretiva 2013/37/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, que altera a Diretiva 2003/98/CE relativa à reutilização de informações do setor público[8].

Mas, uma análise detalhada desta questões, tanto desde o ponto de vista técnico quanto numa perspetiva jurídica, constituiu o objeto do Parecer n.º 5/2014 sobre técnicas de anonimização, de 10 de abril[9].

Por isso mesmo, algumas autoridades nacionais avançaram com orientações destinadas a mostrar padrões aos respetivos responsáveis pelo tratamento de dados, como no Reino Unido com a ICO - *Information Commissioner's Office*, que aprovou o *Anonymisation: managing data protection risk code of practice*, em novembro de 2012, ou com a *Agencia Española de Protección de Datos*, com as suas *Orientaciones y garantías en los procedimientos de anonimización de datos personales*, de outubro de 2016.

8 Sobre esta tensão entre as políticas de dados abertos e a proteção de dados, criticamente, temos também o artigo de Katleen JANSSEN e Sara HUGELIER (2013).

9 No qual é afirmado, precisamente, que "A anonimização de dados pessoais pode ser uma boa estratégia para manter os benefícios e atenuar os riscos. Quando um conjunto de dados se encontra verdadeiramente anonimizado e as pessoas deixam de ser identificáveis, a legislação europeia de proteção de dados deixa de ser aplicável.
No entanto, estudos de casos e publicações de investigação evidenciam que criar um conjunto de dados verdadeiramente anónimo a partir de um conjunto substancial de dados pessoais mantendo, simultaneamente, as informações subjacentes exigidas para a tarefa não é um desafio simples. Por exemplo, um conjunto de dados considerado anónimo pode ser combinado com outro conjunto de dados de modo a que uma ou mais pessoas sejam passíveis de ser identificadas."

Entretanto e a propósito da entrada em vigor do *Regulamento LFD*, a Comissão Europeia publicou as suas "Orientações sobre o regulamento relativo a um quadro para o livre fluxo de dados não pessoais na União Europeia" (COM/2019/250 final, de 29 de maio), com referências específicas e desenvolvidas quanto a esta questão[10], concluindo que "[…] se determinados dados não pessoais puderem ser associados a uma pessoa de qualquer forma, tornando-os direta ou indiretamente identificáveis, devem ser considerados dados pessoais. [e, do mesmo modo] Aplicam-se as mesmas regras [as relativas ao tratamento de dados pessoais] quando a evolução da tecnologia e da análise de dados torna possível a conversão de dados anonimizados em dados pessoais."

Acrescente-se que preocupações idênticas, em especial motivadas pela disponibilização de informações do Setor Público destinadas à sua reutilização por privados num contexto tecnológico de acesso generalizado às analíticas de *Big Data*, enformaram o Anexo II do Relatório de 24 de novembro de 2016 (A/HRC/31/64) do Relator Especial para a Privacidade do Conselho dos Direitos Humanos das Nações Unidas, Joseph A. Cannataci.

Adicionalmente e como resulta também dos Documentos antes referidos, diversos estudos académicos foram mostrando as dificuldades de manter distinções claras, consistentes e, mais ainda, irreversíveis entre dados pessoais e dados não pessoais. O que se concretiza na explicitação dos limites das técnicas de anonimização disponíveis em cada momento, assim como nas possibilidades de personalização de dados anónimos ou anonimizados.

10 "Todos os dados que não sejam «dados pessoais», na aceção do Regulamento Geral sobre a Proteção de Dados, são dados não pessoais. Os dados não pessoais podem ser classificados segundo a origem:
· Desde o início - dados originalmente não relacionados com uma pessoa singular identificada ou identificável, tais como dados sobre as condições meteorológicas gerados por sensores instalados em turbinas eólicas ou dados sobre as necessidades de manutenção de máquinas industriais.
· Em segunda fase - dados inicialmente pessoais, mas posteriormente anonimizados. A «anonimização» de dados pessoais é diferente da pseudonimização (ver supra), uma vez que os dados devidamente anonimizados não podem ser atribuídos a uma determinada pessoa, nem sequer pela utilização de dados adicionais, pelo que se tratam de dados não pessoais.
Aferir da correta anonimização dos dados depende de circunstâncias específicas e únicas de cada caso. Os vários exemplos detetados de reidentificação de conjuntos de dados supostamente anonimizados demonstraram que essa avaliação pode ser exigente. Para determinar se uma pessoa é identificável, é necessário ter em conta todos os meios suscetíveis de serem razoavelmente utilizados por um responsável pelo tratamento ou qualquer outra pessoa para identificar uma pessoa direta ou indiretamente.
No entanto, se determinados dados não pessoais puderem ser associados a uma pessoa de qualquer forma, tornando-os direta ou indiretamente identificáveis, devem ser considerados dados pessoais."

A título exemplificativo, logo em 2010 e desde uma perspetiva jurídica, Paul OHM expôs as insuficiências das técnicas então disponíveis. Entretanto, em julho último, seguindo uma metodologia de natureza matemática, Luc ROCHER, Julien M. HENDRICKX e Yves-Alexandre de MONTJOYE demonstraram como a reidentificação de dados anónimos ou anonimizados pode ser alcançada, com níveis muito altos de eficácia e uma relativa facilidade técnica[11]-[12].

4. *e, "que fazer?"…antes do tratamento de dados, pessoais e não pessoais*

Atendendo a este contexto técnico e regulatório, também resultante do Princípio da responsabilidade proativa (*Accountability*)[13] e por força da aplicação dos Princípios e regras constantes do *RGPD*, o Responsável pelo Tratamento deverá promover a realização de análises de risco, previamente à anonimização de dados pessoais ou ao tratamento de dados não pessoais[14]. O que o afastará de incorrer em qualquer uma das responsabilidades previstas

11 Depois das conclusões de Paul OHM, a questão continuou a sem debatida na Doutrina de ambas margens do Atlântico, procurando uma compatibilização, porventura impossível, entre uma tecnologia crescentemente mais poderosa no sentido de viabilizar a repersonalização de dados anonimizados e as regras pressupondo a correspondente irreversibilidade, sobretudo durante o processo legislativo que culminou na adoção do *Regulamento Geral sobre Proteção de Dados*, ou logo após, como ocorreu com Paul SCHWARTZ e Daniel SOLOVE (2011) e (2014), Samson Y. ESAYAS (2015) ou ainda com Sophie STALLA-BOURDILLON e Alison KNIGHT (2017).

12 Quanto à utilização de analíticas de *Big Data* para a "definição de perfis" (isto é, uma "qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações", Art.º 4.º 4) do *RGPD*) e para a personalização, também a partir de dados anónimos ou anonimizados, são de referir os estudos de Benjamin HABEGGER *et al*. (2014), de Alessandro MANTELERO (2016) e de Elena GIL (2016, *maxime* pp. 86-110) ou, desde uma perspetiva técnica de, Nils GRUSCHKA *et al*. (2018) e ainda o meu trabalho e de Cristiana Teixeira SANTOS (2019), tal como as reflexões críticas de Lorenzo COTINO HUESO (2017).

13 Havendo sido objeto do Parecer 3/2010 sobre o princípio da responsabilidade, adotado em 13 de julho de 2010 pelo *Grupo de Trabalho do Art.º 29*, o mesmo ficou explicitado n.º 2 do Art.º 5.º do *RGPD*, em cujos termos, "O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 [, isto é, pelo cumprimento dos "Princípios relativos ao tratamento de dados pessoais] e tem de poder comprová-lo", sobre o mesmo, além das considerações de Teresa Vale LOPES (2018) e de Emanuele LUCCHINI GUASTALLA (2018), tem muito interesse o recente estudo de Lachlan URQUHART, Tom LODGE e Andy CRABTREE (2019).

14 Isto, porque "Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica." (*Considerando* 26 do *RGPD*). A propósito das análises de risco neste contexto, em termos gerais, são de referir os estudos de Niels van DIJK, Raphaël GELLERT e Kjetil ROMMETVEIT (2016), de Alessandro MANTELERO (2017), assim como as considerações de Teresa Vale LOPES (2018).

nas tipologias constantes do *RGPD* em resultado da personalização de dados, mesmo se apenas potencial ou realizada por terceiros[15].

Aliás, embora se nos afigure evidente, deve ficar claro que a anonimização de dados pessoais pressupõe a presença dos inerentes requisitos no que respeita à "Licitude do tratamento" (Art.ºs 6.º a 11.º), assim como a observância dos "Princípios relativos ao tratamento de dados pessoais" (Art.º 5.º). O mesmo valendo para a personalização, ou a repersonalização, de dados anónimos ou anonimizados.

Especificamente, deverão ser seguidos os critérios indicados no *RGPD* a propósito tanto da "Proteção de dados desde a conceção e por defeito [omissão…]" (Art.º 25), em particular no que se refere à "Segurança do tratamento" (Art.º 32.º), ou seja, "Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas […]."[16].

E ainda, se isso resultar da análise de risco ou for necessário por a mesma ser obrigatória para tratamentos de dados pessoais análogos aos pretendidos (Art.º 35.º n.º 3)[17], deverá também ser efetuada uma "Avaliação de impacto sobre a proteção de dados", com especial

15 Como ocorre com o "direito de indemnização e responsabilidade", objetiva e solidária (Art.º 82.º), com as "coimas" [sanções administrativas], que podem atingir montantes muito elevados (Art.ºs 58.º n.º 1 i) e 83.º), e, sendo o caso, com outras "sanções", designadamente de ordem penal (Art.º 84.º). Para uma melhor compreensão destes preceito e por todos, atente-se no estudo Brendan Van ALSENOY, (2017) e na síntese de Pedro Miguel FREITAS (2018).

16 Quanto ao conteúdo e ao sentido destas previsões, são sobretudo os estudos encomendados pela ENISA – agora, Agência da União Europeia para a Cibersegurança, antes da adopção do *RGPD*, a George DANESIS *et a*l. (2014) e a Giuseppe D'ACQUISTO *et al*. (2015), e, depois, a Marit HANSEN e Konstantinos LIMNIOTIS (2018), sendo ainda de considerar os contributos de Simone CALZOLAIO (2017), de Lee A. BYGRAVE (2017), de Irene KAMARA (2017), este centrado na definição e aplicação de normas técnicas neste domínio, assim como de Teresa Vale LOPES (2018).

17 Especificamente, "a) Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar; b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.º, n.º 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.º; ou c) Controlo sistemático de zonas acessíveis ao público em grande escala."

ênfase no acompanhamento da evolução das técnicas de personalização ou de repersonalização de dados anónimos ou anonimizados, isto é, "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 […]." (Art.º 35.º n.º 1)[18].

Por outras palavras, essas Avaliações devem realizar-se periodicamente ou sempre que se verifique a emergência de novas técnicas neste domínio, não apenas para a anonimização mas também para a personalização[19].

Adicionalmente, o enquadramento de tais tratamentos de dados no âmbito de "um procedimento de certificação aprovado nos termos do artigo 42.º" (tal como referido no Art.º 25.º n.º 3 a propósito da "proteção de dados desde a conceção e por defeito" e no Art.º 32.º n.º 2 no que se refere à "segurança do tratamento") poderá assumir uma grande importância para evitar males maiores no que se refere às várias responsabilidades nas quais os responsáveis pelos tratamentos podem incorrer, embora não as afastem, pelo menos por inteiro[20].

Neste mesmo sentido, a aprovação de "critérios de certificação", contendo parâmetros objetivos e detalhados quanto às técnicas de anonimização mais robustas, pelo Comité Europeu para a Proteção de Dados, conduzindo a um "Selo Europeu de Proteção de Dados", reveste-se da maior relevância (Art.ºs 42.º n.º 5 e 70.º n.º 1 p)[21].

18 A este propósito e em geral, são de assinalar as referências breves de Luís PICA (2018) e as considerações de Teresa Vale LOPES (2018), bem como e sobretudo os estudos de Niels van DIJK, Raphaël GELLERT e Kjetil ROMMETVEIT (2016) e de Bruno PEREIRA e João ORVALHO (2019)

19 Para tanto, cumprirá seguir as 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 (Revistas e adotadas pela última vez em 4 de outubro de 2017), do Comité Europeu para a Proteção de Dados.

20 No que se refere a este regime, atente-se nos estudos de Giovanni Maria RICCIO e Federica PEZZA, (2018) e de Jorge A. VIGURI CORDERO (2018), assim como nos apontamentos de Luís PICA (2018) e de Teresa Vale LOPES (2018).

21 Aliás, essa mesma preocupação já consta, ainda que como referências muitos sintéticas, das Orientações 1/2018 relativas à certificação e à definição de critérios de certificação de acordo com os artigos 42.º e 43.º do Regulamento (Versão 3.0, de 4 de junho de 2019), adotadas pelo CEPD.

Sempre a propósito da certificação das técnicas de anonimização e do tratamento de dados anónimos ou anonimizados, ferramentas complementares poderiam resultar do novel "sistema europeu de certificação da cibersegurança", tal como previsto no Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho de 17 abril de 2019 relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (*Regulamento Cibersegurança*)[22]. O que teria consequências, pelo menos no que se refere à segurança no tratamento dos dados, sobretudo perante uma "violação de dados pessoais"[23], com implicações quanto à presença e conteúdo do dever de notificação da mesma aos titulares dos dados (Art.º 34.º do *RGPD*).

Em especial, estaria em causa uma certificação facultando um 'nível de garantia' 'substancial'[24] ou, até mesmo, um 'alto'[25] (Art.º 52), relativamente a ameaças por parte de terceiros, no sentido de afastar no tempo os riscos resultantes da evolução das tecnologias e da redução dos respetivos custos, pelo menos.

22 A propósito destas questões, em termos gerais, é de atender aos estudos de Helena CARRAPIÇO e André BARRINHA (2017), na expetativa de uma próxima publicação de trabalhos específicos, embora estas questões não sejam novas, como mostra o estudo de Roksana MOORE (2013), por exemplo.

23 Por "«Violação de dados pessoais», [entende-se] uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento;" (Art.º 4.º 12) do *RGPD*). No que se refere a esta matéria, é de atender ao conteúdo do muito recente artigo de Stephanie von MALTZAN (2019).

24 "6. Um certificado europeu de cibersegurança que ateste um nível de garantia «substancial» dá garantia de que os produtos, serviços e processos de TIC objeto desse certificado cumprem os requisitos de segurança correspondentes, incluindo as funcionalidades de segurança, e de que foram avaliados a um nível que visa a redução ao mínimo dos riscos conhecidos para a cibersegurança e do risco de incidentes e ciberataques levados a cabo por autores com competências e recursos limitados. As atividades de avaliação a realizar compreendem, pelo menos, o seguinte: uma análise para demonstrar a inexistência de vulnerabilidades que sejam do conhecimento público e a realização de ensaios para demonstrar que os produtos, serviços ou processos de TIC aplicam corretamente as funcionalidades de segurança necessárias."

25 "7. Um certificado europeu de cibersegurança que ateste um nível de garantia «elevado» dá garantia de que os produtos, serviços e processos de TIC objeto desse certificado cumprem os requisitos de segurança correspondentes, incluindo as funcionalidades de segurança, e de que foram avaliados a um nível que visa a redução ao mínimo dos riscos de ciberataques sofisticados levados a cabo por autores com competências e recursos significativos. As atividades de avaliação a realizar compreendem, pelo menos, o seguinte: uma análise para demonstrar a inexistência de vulnerabilidades que sejam do conhecimento público, a realização de ensaios para demonstrar que os produtos, serviços ou processos de TIC aplicam corretamente as funcionalidades de segurança necessárias, ao nível tecnológico mais avançado, e uma avaliação da sua resistência a atacantes competentes através de ensaios de penetração. […]"

5. *e para prevenir responsabilidades, pelo menos em parte*

Como acabámos de ver, a minimização dos riscos de incumprimento do *RGPD* resultantes de personalizações futura de dados anónimos ou anonimizados, de forma a manter até aos limites do possível a liberdade de tratamento dos mesmo, incluindo a respetiva negociação, implica acompanhar de perto a evolução do estado da técnica, assim como da ações das autoridades, de proteção de dados ou de cibersegurança, no que se refere às certificações de ferramentas ou de procedimentos. Porém, os riscos de incumprimento estarão sempre presentes, apenas podendo ser contidos.

No entanto, o procedimento mais eficaz para afastar tais riscos, ainda que inviável em muitos casos, pela própria *natureza das coisas*, passaria pela aplicação da disciplina constante do *RGPD* a todos os tratamentos de dados, pessoais e não pessoais, pelo menos quando fossem empregues tecnologias como as inerentes à "internet das coisas, a inteligência artificial e a aprendizagem automática" (*Considerando* 9 do *Regulamento LFD*)[26]. Designadamente e pelo menos, com a cifragem de tais massas de dados, de modo a prevenir as consequências e responsabilidades resultantes de eventuais "violações de dados"[27].

26 Em síntese, trata-se de observar os "Princípios relativos ao tratamento de dados pessoais" - em especial no que se refere à "limitação das finalidades", à "minimização dos dados" e à sua "integridade e confidencialidade" (Art.º 5.º n.º 1 b) e c) e n.º 2), de acatar os requisitos de licitude que couberem (Art.ºs 6.º a 11.º), de respeitar pelos "direitos dos titulares dos dados" (Art.ºs 12.º a 22.º), bem como cumprir as obrigações impostas aos responsáveis pelo tratamento (Art.ºs 24.º a 39.º), em especial formulando e seguindo políticas de privacidade (Art.º 24.º n.º 2), metodicamente. A este propósito, vejam-se as considerações breves de Lurdes Alves DIAS (2018), os artigos de Dag Wiese SCHARTUM (2017) e de Filippo A. RASO (2018), os estudos temáticos realizados por mim e por Cristiana Teixeira SANTOS (2018) e (2019), e ainda as reflexões críticas de Miguel MORENO MÚNÕZ (2017).
27 No que se refere à utilização desta técnica no âmbito do *RGPD*, é de referir o trabalho de Gerald SPINDLER e Philipp SCHMECHEL (2016), sendo ainda de muito interesse as reflexões contextuais de Samson Y. ESAYAS (2015).

BIBLIOGRAFIA

(*Todas as hiperligações foram verificadas no dia 30 de novembro de 2019*)

ALSENOY, Brendan Van (2017), "Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation", *JIPITEC - Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol. n. 7;

BYGRAVE, Lee A. (2017), "Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements", *Oslo Law Review*, Vol 4. n. 2, pp. 105-120;

CALZOLAIO, Simone (2017), "*Privacy by design*. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679", *Federalismi.it – Rivista di diritto pubblico italiano, comparator e europeo*, n. 24, pp. 2-21;

CARRAPIÇO, Helena; BARRINHA, André (2018), "European Union cyber security as an emerging research and policy field", *European Politics and Society*, Vol. 19, n. 3, pp. 299-303;

CORTE, Lorenzo dalla (2019), "Scoping personal data: Towards a nuanced interpretation of the material scope of EU data protection law", *European Journal of Law and Technology*, Vol. 10 n. 1;

COTINO HUESO, Lorenzo (2017), "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", *Dilemata – Revista internacional de éticas aplicadas*, n. 24, pp. 131-150;

DANESIS, George *et al*. (2014). *Privacy and Data Protection by Design – from policy to engineering*, ENISA - Agência da União Europeia para a Cibersegurança;

D'ACQUISTO, Giuseppe *et al*. (2015). *Privacy by design in big data - An overview of privacy enhancing technologies in the era of big data analytics*, ENISA - Agência da União Europeia para a Cibersegurança;

DE MIGUEL ASENSIO, Pedro A. (2019), "Servicios de almacenamiento y tratamiento de datos: el Reglamento (UE) 2018/1807 sobre libre circulación de datos no personales", *La Ley Unión Europea*, n. 66, pp. 1-6;

DIAS, Lurdes Alves (2018), "RPGD: Principais Dificuldades e Dúvidas das Organizações e dos Titulares de Dados Pessoais na Adaptação ao Atual Regime", *Cyberlaw by CIJIC*, n. 6;

DIAS, Fernanda Ferreira (2016), "O Mercado Único Digital Europeu", *Análise Europeia - Revista da Associação Portuguesa de Estudos Europeus*, n. 2, pp. 17-41;

DIJK, Niels van; GELLERT, Raphaël; ROMMETVEIT, Kjetil (2016), "A risk to a right? Beyond data protection risk assessments", *Computer Law & Security Review*, Vol. 32 n. 2, pp. 286-306;

DUCATO, Rossana (2016), "La crisi della definizione di dato personale nell'era del web 3.0", *Quaderni della Facoltà di Giusrisprudenza dell'Università di Trento*, n. 26, pp. 143-178;

ESAYAS, Samson Yoseph (2015), "The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing' approach", *European Journal of Law and Technology*, Vol. 6 n. 2;

FREITAS, Pedro Miguel (2018), "The General Data Protection Regulation: an overview of the penalties' provisions from a Portuguese standpoint". *UNIO - EU Law Review*, Vol. 4 n. 2;

GIL, Elena (2016), *Big data, privacidad y protección de datos*. Madrid: Agencia Española de Protección de Datos / Boletín Oficial del Estado;

GRUSCHKA, Nils *et al*. (2018), "Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR", *Proceedings of the 2018 IEEE International Conference on Big Data*, Seattle;

HABEGGER, Benjamin *et al*. (2014), "Personalization vs. Privacy in Big Data Analysis", *International Journal of Big Data*, n. 1, pp. 25-35;

HANSEN, Marit; LIMNIOTIS, Konstantinos (2018), *Recommendations on shaping technology according to GDPR provisions - Exploring the notion of data protection by default*, ENISA – Agência da União Europeia para a Cibersegurança;

HOOFNAGLE, Chris J.; SLOOT, Bart van der; ZUIDERVEEN BORGESIUS, Frederik (2019), "The European Union general data protection regulation: what it is and what it means", *Information & Communications Technology Law*, Vol. 28 n. 1, pp. 65-98;

JANSSEN, Katleen; HUGELIER, Sara (2013), "Open data as the standard for Europe? A critical analysis of the European Commission's proposal to amend the PSI Directive", *European Journal of Law and Technology*, Vol. 4 n. 3;

KAMARA, Irene (2017), "Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'". *European Journal of Law and Technology*, Vol. 8 n. 1;

LOPES, Teresa Vale (2018), "Responsabilidade e governação das empresas no âmbito do novo Regulamento sobre a Proteção de Dados", *Anuário da Proteção de Dados 2018*, pp. 45-69;

LUCCHINI GUASTALLA, Emanuele (2018), "Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori", *Contratto e Impresa*, n. 1, pp. 106-125;

MALTZAN, Stephanie von (2019), "No Contradiction Between Cyber-Security and Data Protection? Designing a Data Protection Compliant Incident Response System", *European Journal of Law and Technology*, Vol. 10 n. 1;

MANTELERO, Alessandro (2016), "Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection", *Computer Law & Security Review*, Vol. 22 n. 2, pp. 238-255;

IDEM (2017), "Responsabilità e rischio nel Reg. UE 2016/679", *Le nuove leggi civili commentate*, Vol. XL n. 1, pp. 144-164;

MASSENO, Manuel David; SANTOS, Cristiana Teixeira (2018), "Assuring Privacy and Data Protection within the Framework of Smart Tourism Destinations", *MediaLaws – Rivista di diritto dei media*, n. 2, pp. 251-266;

IDEM (2019), "Personalization and profiling of tourists in smart tourism destinations - a data protection perspective", *International Journal of Information Systems and Tourism*, Vol. 4 n. 2, pp. 7-23;

MENEZES CORDEIRO. A. Barreto (2018), "Dados pessoais: conceito, extensão e limites", *Revista de Direito Civil*, A. 3 n. 2, pp. 297-321;

MORENO MUÑOZ, Miguel (2017), "Privacidad y procesado automático de datos personales mediante aplicaciones y bots", *Dilemata – Revista internacional de éticas aplicadas*, n. 24, pp. 1-23;

MOORE, Roksana (2013), "The Case for Regulating Quality within Computer Security Applications". *European Journal of Law and Technology*, Vol. 4 n. 3;

ORTEGA JÍMENEZ, Alfonso; GONZALO DOMENECH, Juan José (2018), "Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea", *Revista de la Faculdad de Derecho de la Universidad de la República*, n. 44;

PEREIRA, Bruno; ORVALHO, João (2019), "Avaliação de Impacto sobre a Protecção de Dados", *Cyberlaw by CIJIC*, n.º 7;

PICA, Luís (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*, n.º 5;

PURTOVA, Nadezhda (2018), "The law of everything. Broad concept of personal data and future of EU data protection law", *Law, Innovation and Technology*, Vol. 10 n. 1, pp. 40-81;

RASO, Filippo A. (2018), "Innovating in Uncertainty: Effective Compliance and the GDPR", *Harvard Journal of Law & Technology Digest*;

RICCIO, Giovanni Maria; PEZZA, Federica (2018), "Certification Mechanism as a Tool for the Unification of the Data Protection European Law", *MediaLaws – Rivista di diritto dei media*, n.º 1, pp. 249-260;

SCHARTUM, Dag Wiese (2017), "Intelligible Data Protection Legislation: A Procedural Approach", *Oslo Law Review*, Vol 4. n. 1, pp. 48-59;

SCHWARTZ, Paul; SOLOVE, Daniel (2011), "The PII Problem: Privacy and a New Concept of Personally Identifiable Information", *New York University Law Review*, Vol. 86, pp. 1814-1894;

IDEM (2014), "Reconciling Personal Information in the United States and European Union", *California Law Review*, Vol. 102, pp. 877-916;

SPINDLER, Gerald; SCHMECHEL, Philipp (2016), "Personal Data and Encryption in the European General Data Protection Regulation", *JIPITEC - Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol. 7;

STALLA-BOURDILLON, Sophie; KNIGHT, Alison (2017), "Anonymous Data v. Personal Data - A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data", *Wisconsin International Law Journal*, Vol. 34 n. 2, pp. 285-322;

TEIXEIRA, Angelina (2016), "A Chave para a Regulamentação da Protecção de Dados (Das pessoas singulares)", *Data Venia - Revista Jurídica Digital*, n.º 6, pp. 6-32;

URQUHART, Lachlan; LODGE, Tom; CRABTREE, Andy (2019), "Demonstrably doing accountability in the Internet of Things", *International Journal of Law and Information Technology*, Vol. 27 n. 1, pp. 1-27;

VIGURI CORDERO, Jorge A. (2018), "La Certificación en el Nuevo Reglamento Europeo de Protección de Datos y Anteproyecto de Ley Orgánica de Protección de Datos", *El Tiempo de los Derechos*, n. 11.

CYBERLAW
by CIJIC

PODEM AS EMPRESAS REALIZAR A MONITORIZAÇÃO DE SEUS TRABALHADORES ATRAVÉS DE FERRAMENTAS DE SEGURANÇA DA INFORMAÇÃO, SEM VIOLAR O RGPD?

MÁRCIO COTS [1]

e

ANDRESA CRUZ [2]

1 Advogado português, especializado em Cyberlaw e Direito dos Negócios Digitais, sendo também membro do escritório norte-americano CyberlawStudio PLLC.Professor universitário.Mestre em Direito pela FADISP, especialista em Cyberlaw pela Harvard Law School – EUA, com extensão universitária em Direito da Tecnologia da Informação, pela FGV/EPGE.Membro do Harvard Faculty Club.Advogados.

2 Formada em Direito, atuando como advogada no Brasil e em Portugal em parceria com a COTS Advogados. Éspecialista em Direito Informático, presta consultoria em Proteção de Dados, privacidade e adequação jurídica para as novas tecnologias, além da área contenciosa.Co-autora de obra "O Legítimo Interesse e a LGPDP"

Participante de diversos congressos e eventos com foco em Privacidade, Proteção de Dados, Inteligência Artificial e o Direito 4.0.

RESUMO

Uma das preocupações das empresas na era da informação é a possibilidade do vazamento dos dados, portanto, o investimento em segurança da informação torna-se necessário.

Neste contexto, há como realizar a monitorização de seus trabalhadores a fim de evitar tais vazamentos sem que o direito à reserva da intimidade da vida privada, direito consagrado na Constituição da República Portuguesa, em seu artigo 26º, seja violado? E, ainda, manter os dados pessoais de seus trabalhadores protegidos?

Palavras-chave: Proteção de dados pessoais; Regulamento Geral Proteção Dados; empregador e trabalhador; tecnologia; monitorização.

> *"Interpretar as normas constitucionais significa (como toda a interpretação de normas jurídicas) compreender, investigar e mediatizar o conteúdo semântico dos enunciados linguísticos que formam o texto constitucional. A interpretação jurídica constitucional reconduz-se, pois, à atribuição de um significado a um ou vários símbolos linguísticos escritos na constituição".*
>
> ***(CANOTILHO, J. J. Gomes)***

Uma das preocupações das empresas na era da informação é a possibilidade do vazamento dos dados, portanto, o investimento em segurança da informação torna-se necessário.

Neste contexto, há como realizar a monitorização de seus trabalhadores a fim de evitar tais vazamentos sem que o direito à reserva da intimidade da vida privada, direito consagrado na Constituição da República Portuguesa, em seu artigo 26º, seja violado? E, ainda, manter os dados pessoais de seus trabalhadores protegidos?

O artigo 20º, nº1 do Código do trabalho, prescreve que:

> "*O empregador não pode utilizar meios de vigilância a distância no local de trabalho, mediante o emprego de equipamento tecnológico, com a finalidade de controlar o desempenho profissional do trabalhador*".

Já no nº2 do mesmo artigo:

> "*A utilização de equipamento referido no número anterior é lícita sempre que tenha por finalidade a protecção e segurança*

de pessoas e bens ou quando particulares exigências inerentes à natureza da actividade o justifiquem".

Ou seja, há sim formas válidas de monitorização dos funcionários, a questão em si é, quais serão as finalidades e limites para o fazê-lo.

> *"Apesar de o artº 20º, nº 1 do Código do Trabalho proibir a utilização de meios de vigilância distância para controlar de forma dedicada e permanente o desempenho profissional do trabalhador,* ***esta utilização é lícita se cumprir os requisitos de fim e publicidade previstos*** *nos nºs 2 e 3 do mesmo artº 20º e* conforme manifestado pela *Comissão Nacional de Protecção de Dados.* ***Neste último caso, os dados obtidos podem servir de meio de prova em procedimento disciplinar e no controlo jurisdicional da licitude da decisão disciplinar****."*[1]

Publicado pelo grupo de trabalho do artigo 29 para Proteção de Dados, em seu parecer 2/2017[2] sobre o tratamento de dados no local de trabalho, e que reafirma também a posição e as conclusões do Parecer 8/2001[3], bem como do documento de trabalho GT55[4], aquando do tratamento dos dados pessoais dos empregados:

- os empregadores devem ter sempre em conta os princípios fundamentais da proteção de dados, independentemente da tecnologia utilizada;

- o conteúdo das comunicações eletrónicas feitas a partir de um estabelecimento comercial goza da mesma proteção dos direitos fundamentais que a das comunicações análogas;

1 *Ac. TRC, de 02.06.2016*
2 Parecer 2/2017 sobre o tratamento de dados no local de trabalho
3 GT 29, Parecer 8/2001 sobre o tratamento de dados pessoais no contexto laboral, GT 48, 13 de setembro de 2001, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf
4 GT 29, documento de trabalho sobre a vigilância das comunicações eletrónicas no local de trabalho, GT 55, 29 de maio de 2002, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55_pt.pdf

- é muito improvável que o consentimento possa constituir uma base jurídica para o tratamento de dados no local de trabalho, a menos que os empregados possam recusar, sem consequências adversas;

- a execução de um contrato e o interesse legítimo podem, por vezes, ser invocados, desde que o tratamento seja estritamente necessário para uma finalidade legítima e respeite os princípios da proporcionalidade e da subsidiariedade;

- **os empregados devem receber informações eficazes sobre a realização da monitorização**; e

- qualquer transferência internacional de dados dos empregados apenas deve ser realizada nos casos em que seja garantido um nível de proteção adequado.

Pela própria natureza das atividades relacionadas a monitorização de dados pessoais, ressalta-se a obrigatoriedade de uma Avaliação de Impacto sobre a Proteção de Dados - AIPD, sendo este um dos requisitos obrigatórios ao responsável pelo tratamento de dados, e com previsão no RGPD em seu artigo 35º, devendo ser sempre executado quando um certo tipo de tecnologia, principalmente as "novas tecnologias", impliquem num elevado risco para os direitos e liberdades das pessoas singulares, como por exemplo a temática deste artigo, a monitorização de emails, mensagens eletrónicas, e controlos pertinentes do universo corporativo.

Para tal, e em conformidade com o RGPD artigo 88º, nº 2, para que a monitorização seja resguardada e adequada ao regulamento, o exercício de monitorização, deve ser sustentada com medidas adequadas e específicas de segurança, de forma a salvaguardar a dignidade, os interesses legítimos e os direitos fundamentais do titular dos dados, avaliando se:

- a transferência de dados pessoais é realizada num grupo empresarial ou num grupo de empresas envolvidas numa atividade económica conjunta?;

- a atividade de tratamento e monitorização é necessária?

- a proposta do tratamento de dados pessoais e monitorização é equitativa para os empregados?;

- a atividade de monitorização é proporcional às preocupações suscitadas?; e
- existe transparência do tratamento de dados e sistemas de controlo no local de trabalho, para com os empregados?

Alguns exemplos onde a monitorização e tratamento de dados pode ser considerado legítima por parte do empregador:

- Deteção e prevenção de perda ou vazamento de dados pessoais;
- Deteção e prevenção de perda ou roubo de propriedade intelectual ou física de negócios;
- Finalidades estatísticas;
- Controlos de qualidade.

É importante reconhecer que, embora a melhoria da produtividade e desempenho dos funcionários seja um interesse legítimo do empregador, este não pode colocar em causa os direitos fundamentais e a privacidade dos funcionários.

Para além dos direitos dos trabalhadores, deve-se levar em conta os direitos das entidades patronais, a quem se reservam o "**direito de propriedade privada**"[5], bem como o "**poder de direção**"[6], onde compete ao empregador estipular os termos do contrato de trabalho, nos limites das normas que os regem, e, a partir da elaboração do "**regulamento interno**"[7] estipular as regras de comunicação da empresa, as formas de controlo a serem realizadas e as condições dos tratamentos dos dados. "*Mas a escolha dos meios de controlo por parte do empregador tem de obedecer aos princípios da necessidade, da proporcionalidade e da boa-fé, devendo este demonstrar que escolheu as formas de controlo com menor impacto sobre os direitos fundamentais dos trabalhadores*[8]."

5 Constituição da República Portuguesa, artigo 62º.
6 Código do Trabalho, artigo 97º.
7 Código do Trabalho, artigo 99º.
8 Deliberação n.º 1638/2013 CNPD.

Também parte obrigatória do Regulamento Interno, a monitorização através de ferramentas e aplicativos conhecidos popularmente pelo termo "Redes Sociais", só é permitido quando:

- O perfil na rede social está diretamente relacionada a fins profissionais;
- Em processo de recrutamento e seleção, o perfil do candidato possuir informações sobre habilidades ou características altamente relevantes para o trabalho oferecido.

A título exemplificativo de uma monitorização em "redes sociais, o Tribunal de Matosinhos, declara justa causa em despedimento por ofensas dirigidas ao empregador no Facebook.

Aquando do controlo do correio eletronico, as empresas podem realizar a monitorização dos mesmos, desde que tenham regras bem delineadas e publicitadas (artigo 99º, nº3, Código do Trabalho).

Em alusão ao tema supra mencionado há uma referência histórica onde o "Tribunal dos Direitos do Homem, dá razão a juiz português[9] sobre a privacidade no trabalho em ação que remonta a 10 anos, onde este teve seu voto vencido. Afinal, e ao contrário do que tinha sido decidido anteriormente, as empresas só podem aceder aos e-mails dos seus trabalhadores depois de os avisarem. Trata-se de um marco importante na evolução do direito sobre privacidade no trabalho. O caso diz respeito à Bogdan Barbulescu[10], um engenheiro informático romeno que foi despedido em 2007 por ter usado para comunicações privadas o seu Yahoo!Messenger da empresa. Esta aplicava uma política estrita na matéria, proibindo formalmente os empregados de se servirem do Messenger para quaisquer fins que não fossem profissionais. Barbulescu infringiu a política ao trocar mensagens com o seu irmão e a sua noiva."[11]

9 Juiz Paulo Pinto de Albuquerque
10 O Tribunal Europeu dos Direitos do Homem (TEDH) - http://hudoc.echr.coe.int/eng-press?i=003-5825428-7419362
11 Luís M Faria

Segundo o magistrado português, «uma abordagem ao uso da Internet no local de trabalho centrada nos direitos humanos», com regras claras e transparentes e notificação pessoal da prática da entidade patronal com consentimento explícito dos seus profissionais.

Em Portugal, **os trabalhadores gozam de direito à personalidade, isto é, proteção "contra qualquer ofensa ilícita à sua pessoa física ou moral**", prescrito no Artigo 70.º do Código Civil. Isto posto, a autoridade recorre ao Código do Trabalho e a uma deliberação da Comissão Nacional de Proteção de Dados de forma a estabelecer um enquadramento legal que cubra este direito em contexto de monitorização das comunicações.

Em acordo com o Código do Trabalho no artigo 22.º, **o trabalhador tem direito à reserva e à confidencialidade no que toca a mensagens de cariz pessoal e ao acesso a informação de caráter não profissional via email**. Adverte a ACT, "**tal não prejudica o poder de o empregador estabelecer regras e políticas de utilização dos meios de comunicação na empresa**".

A **Comissão Nacional de Proteção de Dados** emitiu, a 16 de julho de 2013, uma deliberação[12] que **estabelece os limites** dentro dos quais as entidades empregadoras podem proceder a tal vigilância.

> "*Sejam quais forem as regras definidas pela empresa para a utilização do correio eletrónico para fins privados, o empregador não tem o direito de abrir, automaticamente, o correio eletrónico dirigido ao trabalhador*."

As mensagens não perdem o cunho pessoal ou confidencial por ficarem gravadas num servidor detido pela entidade patronal. A deliberação, contudo, **adverte que devem ser criadas pastas próprias dos trabalhadores, devidamente identificadas.**

12 DELIBERAÇÃO n.º 16 D38/2013 - https://www.cnpd.pt/bin/orientacoes/Delib_controlo_comunic.pdf

De fora da monitorização patronal ficam as mensagens relacionadas com segredo e sigilo profissionais:

> "***Também no que diz respeito ao correio eletrónico, o segredo profissional específico que impende sobre o empregado (v.g., sigilo médico, sigilo profissional de advogado, ou segredo das fontes) tem de ser preservado, não devendo o conteúdo das suas mensagens ser acedido em circunstância alguma nem os dados de tráfego reveladores dos remetentes ou destinatários exteriores ser objeto de tratamento para fins de controlo***."

Em caso de **preservação de segredo comercial, a empresa pode proceder a eventuais ações de controlo**. No entanto, estas só podem incidir sobre as pessoas que têm acesso a tais informações sigilosas e quando existe fundamento de possíveis fugas de informações. Neste contexto específico, o acesso ao e-mail deve ser "o último recurso a utilizar pela entidade empregadora", e deve ser feito na presença do trabalhador em questão e, preferencialmente, de um representante da comissão de trabalhadores ou alguém indicado pelo mesmo empregado.

> "*O referido acesso deve limitar-se à visualização dos endereços dos destinatários, o assunto, a data e hora do envio, podendo o trabalhador – se for o caso – especificar a existência de algumas mensagens de natureza privada e que não pretende que sejam lidas pela entidade empregadora."*

Assim, como diz o antigo provérbio "mais vale prevenir, que remediar", cabe a entidade empregadora definir e, muito bem as regras a serem seguidas na empresa, da forma como os ditames legais especificam, publicitá-las e a partir disto monitorizar seus trabalhadores de forma coerente, a fim de resguardar os dados da empresa e os dados pessoais de seus trabalhadores.

O fato é que a privacidade não é o único direito envolvido na questão da relação entre empresas e colaboradores na monitorização dos computadores. Vale ressaltar que, as empresas têm a propriedade da estação de trabalho, do acesso à Internet e do domínio corporativo.

Quem fornece os meios para se trabalhar, também tem seus direitos. Desta feita, é assegurado às empresas o direito à propriedade, pelo artigo 62.º - Direito de propriedade privada - ***1. A todos é garantido o direito à propriedade privada e à sua transmissão em vida ou por morte, nos termos da Constituição***.

No mundo corporativo, a Internet e outros meios eletrónicos de comunicação tornaram-se mais uma ferramenta de trabalho, fornecidas, em certos casos, pela empresa aos seus empregados, que possibilitam agilidade na comunicação.

Sendo esta ferramenta mal utilizada, compromete-se a imagem e segurança da empresa.

No meio jurídico, quando existem questões desta natureza, em que há um conflito de premissas constitucionais a serem aplicadas em um mesmo caso, tenta-se utilizar a proporcionalidade e a razoabilidade, para evitar que um direito constitucional se sobreponha a outro.

Outro ponto polémico é a questão da ***Culpa in eligendo*** (Direito Civil), onde *"há* culpa *in eligendo se dá quando alguém escolhe, para realizar um qualquer acto ou actividade, uma pessoa que não tem as necessárias qualidades ou qualificações, quando podia e deveria ter escolhido pessoas diferente. Quando o devedor de uma obrigação faz intervir no cumprimento desta um terceiro que, por falta de aptidões ou de preparação, desencadeia um não cumprimento, é o devedor responsável pelos danos resultantes,*

fundando-se tal responsabilidade no acto próprio da culposa escolha do substituto ou auxiliar. (...)".[13]

Desta feita, se a empresa tem responsabilidade quanto aos actos praticados por seus funcionários, certamente esta pode, dentro dos parâmetros legais, monitorizar seus actos.

Além do mais, as empresas têm o direito de cuidarem de sua imagem ou marca na internet.

Portanto, caso a empresa, face aos seus direitos constitucionais de propriedade, de imagem e diante de sua responsabilidade ao eleger determinados funcionários para actos de suas responsabilidade, queira monitorizá-los, com ferramentas de segurança da informação, deverá previamente informá-lo de tal monitorização, afim de retirá-lhe a expectativa de privacidade no meio virtual laboral.

13 PRATA, Ana, com colab. CARVALHO, Jorge (2014), Dicionário Jurídico, Vol. I, reimp. da 5ª ed. de jan 2008, Coimbra, Almedina, p. 413.

A Regulação Jurídica do Ciberespaço – Mutação do paradigma à luz do Acórdão James Elliot do TJUE

VALTER FREITAS [1]

1 Mestrando de Segurança da Informação e Direito do Ciberespaço do Instituto Superior Técnico e mestrando de Direito e Segurança da Faculdade de Direito da Universidade Nova de Lisboa. Atualmente desempenha a função de Consultor de Segurança de Informação/IT Security Officer. Contacto: valter.dione@campus.ul.pt

RESUMO

Com o advento da tecnologia, as funções primordiais do Estado tendem a migrar para o mundo do ciberespaço, incumbindo-o na salvaguarda de direitos fundamentais tecnológicos assentes na pessoa digital. Conjuntamente, certas funções clássicas atribuídas aos Estado paulatinamente migram para a esfera supranacional, bem como para o tecido privado, em particular para os organismos de normalização. Estes colaboram na produção de normas soft law concorrentes à produção legislativa, carecendo da legitimidade democrática. Neste panorama, cumpre refletir a partir da análise do Acórdão James Elliot à luz da regulação do ciberespaço.

Palavras-Chave: Legitimidade democrática, norma harmonizada, regulação, sector privado.

ABSTRACT

With the advent of technology, the primary functions of the State tend to migrate to the Cyberspace, entrusting with safeguarding fundamental IT rights based on the digital person. Together, certain classic functions attributed to the State gradually migrate to the supranational sphere, as well as to the private fabric, in particular the standardization bodies. These bodies collaborate in the production of soft law norms with legislative production, lacking democratic legitimacy. In this context, it is necessary to reflect with analysis of the James Elliot Judgment in the light of cyberspace regulation.

Keywords: Democratic legitimacy, harmonized standard, regulation, private sector

NÓTULA METODOLÓGICA

Este estudo focará numa análise singela do processo de normalização, conjugando os atores intervenientes neste processo à escala internacional e à escala europeia, sem prejuízo da breve menção do enquadramento nacional português para compreensão de certas destrinças concetuais. Em pormenor, com a menção da Diretiva da Nova Abordagem da União Europeia, bem como a casuística, *máxime* o Acórdão Elliot de 2016.

A pertinência do presente estudo no âmago da unidade curricular de Direito Constitucional e Informática, parte da evolução da regulação jurídica constatada, por um lado, com incremento de direitos conexos com as tecnologias de informação e comunicação e, por outro lado, o acompanhamento das funções do Estado com a evolução tecnológica, reconhecendo o aparato legislativo algo burocrático, lento e, por vezes ineficaz. Desta feita, carece de uma resposta eficaz, rápida e especializada, em especial, através dos Organismos de Normalização.

Compreendendo a dificuldade da elaboração da dissertação de mestrado, torna-se imperativo enquadrar este estudo com o projeto final, visando a eficiência da investigação e prossecução da investigação nesta área de profundo interesse. Partiremos da investigação qualitativo, recorrendo ao método indutivo, acompanhado da recolha de dados provenientes da análise documental, em especial, a análise do Acórdão.

Para o efeito do presente estudo, pretenderemos responder à seguinte questão de partida, tomaremos as indagações de Erica Palmerini (2012), em matéria de regulação do ciberespaço, tomando em consideração a seguinte questão:

(Q1) Será que o Acórdão confere um modelo póstumo de regulação do ciberespaço?

Partindo desta questão, elaboramos as seguintes hipóteses:

(H1) Este acórdão confere um modelo de regulação do ciberespaço;

(H2) Este acórdão não confere um modelo de regulação do ciberespaço.

1. NÓTULA INTRODUTÓRIA JURÍDICO-POLÍTICA

> *"Combining formal law and technical standards, as a feasible approach to techno-regulation, requires the private sector to be included in the legal order and raises problems of democratic control and legitimacy."*
>
> Erica Palmerini, The Interplay between Law and Technology

Nas sociedades hodiernas, o Estado tem progressivamente externalizado parte das suas funções, recorrendo à privatização[1] em setores considerados vitais para a prossecução do interesse público, tomando como ilustrativo a Segurança[2], assumindo uma função complementar à Segurança Pública, e a resolução alternativa de litígios[3], em oposição à justiça pública, não menosprezando os inúmeros setores da atividade do Estado[4] privatizados. De facto, este movimento deve-se às limitações legais e orçamentais.

Deste modo, cumpre questionar se a função legislativa, tal como a função administrativa do Estado, é passível de tornar-se privatizado? E se é passível de privatizar, poderemos depreender um modelo de regulação do Ciberespaço? Esta tendência da *New*

1 Para o entendimento de privatização, poderemos considerar a privatização plena com a passagem das funções asseguradas previamente para o Estado, passando para a gestão pelos privados, na esteira da doutrina, em especial os juristas Nuno Sá Gomes, Maria Eduarda Azevedo. Sem prejuízo desta posição doutrinal, parece sensato apoiar na definição do termo privatização por Gomes Canotilho e Vital Moreira: *"o termo privatização é hoje um termo polissémico na literatura jurídica e económica, designando um variado conjunto de políticas públicas (transferência de propriedade de empresas ou de serviços públicos para entidades privadas ou concessão da responsabilidade da gestão em entidades privadas, abertura à iniciativa privada de sectores ou serviços (...) explorados pelo sector público em regime de exclusivo, contratação a entidades privadas de serviços anteriormente assegurados pelos próprios serviços públicos, "desregulamentação" do controlo da produção ou distribuição de um bem ou serviço, submissão dos serviços ou empresas públicas e regras de natureza privada."* [sublinhado nosso] Cfr. Gomes Canotilho, J., J., e Moreira, V., *Constituição da República Portuguesa Anotada*, p. 415 e ss. *apud* Vilhena de Freitas, L., *Direito Administrativo das Privatizações, in Tratado de Direito Administrativo Especial, Vol. VII*, pp. 269-355

2 Verificamos um aumento exponencial de vigilantes promotores da Segurança Privada, enfraquecendo o *Ius imperii* do Estado, reduzindo o número agentes, em prol do incremento da atividade suplementar à Segurança Pública. Cfr. Poiares, N., *Uma policialização da segurança privada*, pp. 1-11

3 Aliás, como nos aponta Catarina Frade: "O Estado contemporâneo perdeu o monopólio da função de julgar, repartindo-a com os privados e a sociedade civil e entrando em parceria ou mesmo em concorrência com eles." Cfr. Frade, C., *A Resolução Alternativa de Litígios e o acesso à justiça*, pp. 107-128

4 A nossa Constituição da República Portuguesa, recorrendo ao emanado do n.º 3 do artigo 86.º da Constituição, habilita o legislador a vedar a a atividade pro empresas privadas em setores básicos para a sociedade.

Public Management, encontra-se explanada no manual de Direito Administrativo de José Carlos Vieira de Andrade (2017), passando a citar os elementos caraterizadores desta nova gestão da administração pública:

a) privatização (material, formal, instrumental e funcional) de sectores significativos da atividade administrativa, e o consequente (e disseminado) uso misto do direito público e do direito privado;

b) europeização e internacionalização do direito administrativo, seja pela imposição normativa e reguladora (substancial e procedimental) do direito transnacional, prevalecente em áreas cada vez mais vastas, amplificada e efectivada pelo activismo judicial dos tribunais europeus (TJUE, TEDH), seja pelo desenvolvimento da organização administrativa europeia, seja ainda pela eficácia transnacional de decisões administrativas, num contexto internacional de progressiva globalização do direito administrativo, especialmente notória ao nível organizativo, procedimental e processual;

c) economicização do direito administrativo, através da aplicação dos princípios da eficiência e da sustentabilidade, que, designadamente a partir de uma análise económica do direito, propõem uma nova organização e gestão administrativa (New Public Management), caracterizada por novos métodos de interpretação e de avaliação das normas jurídicas, orientados para os resultados (optimização dos efeitos desejados e evitação dos efeitos indesejados);

d) cooperação coordenada (local, regional, nacional e europeia) baseada numa conectividade multi-nível das actuações das diversas entidades administrativas, horizontal (em rede) ou vertical (em degraus);

e) desmaterialização ou digitalização dos procedimentos, da informação e da comunicação, nas relações com os particulares e no relacionamento interadministrativo, incluindo as administrações europeias e internacionais (electronic government);

f) deslegalização e rarefacção jurídica dos padrões normativos substanciais da actividade administrativa, num quadro de policentralidade normativa ("interconstitucionalidade" e "internormatividade") e de centrifugação organizativa e social, que visa a definição de políticas públicas nacionais e a co-implementação ou execução de políticas europeias, designadamente no campo económico e social, associada a ideias de bom governo ou de "governança" *(New Public Government Governance*)."

Nestas tendências, subentende-se a digitalização e a instrumentalização do ciberespaço para a prossecução do interesse público[5], conjugando com a tendência da privatização da função administrativa. Aliás, nunca a administração teve tão informatizada como no quotidiano, perfazendo um novo panorama da regulação jurídica, em especial, no Ciberespaço. Neste sentido, as *Multistakeholders*[6], atuam numa ótica apartada das fronteiras políticas, as quais, por sua vez, confinam a atuação do Estado. Padece de instrumentos que sustentem a função legislativa fase à constante desatualização[7] no mundo cibernético. Torna-se imperativo a abordagem flexível interpretativa[8], a introdução de técnicas regulatórias que antecipem os riscos futuros da, focando nas questões da legitimidade democrática e do escrutínio público.

Destarte, não se verifica somente a privatização da função administrativa, como, em certos casos, a delegação de atribuições ao privado para a elaboração normativa com teor técnico-jurídica, designados por normas *standard*[9]. Cumpre realizar a destrinça deste tipo de norma, com a norma jurídica, partindo do teórico Karl Engisch, esta última como "uma norma de determinação, fruto da vontade imperativa do legislador, e não como uma norma de valoração que exprime uma ordenação objetiva da vida"[10]. Já as normas técnicas, em

5 Assim, os acessos às plataformas configuram uma profunda alteração na prestação dos serviços ao público, substituindo o papel ou complementando com o meio virtual, ingressando por um uso de aparelhos eletrónicos de comunicação, constituindo o *E-Government*. Este, por sua vez, promove a desburocratização, a maior aproximação dos serviços às populações e assegura a participação dos interessados, possibilitando o direito à informação sobre o andamento dos processos, o direito de acesso aos arquivos e registos administrativos.

6 Para exemplificar, tomamos como ilustrativo as RFC da IETF, os domínios consignados à ICANN, entre outras organizações com o papel primordial na regulação do Ciberespaço, numa ótica de *Soft Law*. Para o aprofundamento das caraterísticas destas *multistakeholders*, sugerimos, Cfr. Waz, J., e Weiser, P., *Internet Governance: The Role Of Multistakeholder Organizations*, pp. 333-350; Cfr. B. Svantesson, D., J., *Internet & Jurisdiction, The Global Status Report*, pp. 1-181

7 Reforçando esta constante do mundo das tecnologias: "*Law-making is a slow process, while technology changes rapidly. This distance between technological innovation and legal change may affect legal certainty and cause people to act in an ambiguous environment where rights and responsibilities cannot be clearly acknowledged or predicted."* Cfr. Palmerini, E., *The Interplay between Law and Technology,* pp. 7-25.

8 Partindo da necessidade de uma nova leitura constitucional, como apela a doutrina, particularmente a Drª Profª Raquel Brizida Castro, tendo em vista a interpretação constitucional tecnologicamente neutra, emanada dos ensinamento de Lawrence Tribe, reconhecemos a essencialidade esta *meta-interpretação,* numa ótica hermenêutica flexível, ajustado, não apenas no texto constitucional, como também na legislação derivada, colmatando os riscos futuros de desadequação da norma, Cfr. Brízida Castro, R., *Constituição e Ciberespaço: Argumentos Para um "Direito Constitucional Do Inimigo"?,* pp. 1-42*;* Cfr. Palmerini, E., *The interplay between Law and Technology*, pp. 7-25

9 Parafraseando Vieira de Andrade, estes *standards*, "por vezes de origem privada, europeia e internacional, que, a vários títulos e em diversos níveis, adquirem força vinculativa e regulam a actividade administrativa – ou seja, de normas que constituem programas finais (e não condicionais), com prejuízo para a intensidade da vinculação administrativa", constituindo um dos aspetos para a criase da legalidade estrita apontada por este autor. Cfr. Vieira de Andrade, J., C., *Lições de Direito Administrativo*, pp. 52 e ss.

10 Cfr. *apud* Nogueira de Brito, M., *Introdução ao Estudo do Direito,* pp.401-454

contraponto às normas jurídicas, são um documento com caráter não vinculativo com conteúdo técnico aprofundado, pautado pela flexibilidade por não revestir a formalidade burocrática do aparato legislativo, visando, essencialmente, a padronização de um determinado produto/serviço, através das boas práticas internacionais.

Concomitantemente, estas normas pertencem materialmente à categoria de *Soft Law*, a qual a doutrina não é unânime quanto à sua definição, sem prejuízo de atender a um conteúdo flexível, os instrumentos jurídicos tipicamente não são vinculantes, são tipicamente menos custosos e mais rápido, comparativamente à *Hard Law*[11]. Evidentemente, compreendemos a sua essencialidade no Direito Internacional, em especial, o exemplo do Acordo sobre as Barreiras Técnicas ao Comércio (doravante TBT)[12], tal como o exemplo do Regulamento da Nova Abordagem n.º 1025/2012 de 25 de outubro, no seio da União Europeia, norteando a política de normas *standard* através dos princípios emanados da Organização Mundial do Comércio (OMC), podendo confrontar o considerando n.º 2 do mesmo Regulamento.

11 Cfr. Schaffer, G., C., & Pollack, M., A., *Hard vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance*, pp. 707-723; Cf. Palmerini, E., *The Interplay between Law and Technology*, pp. 7-25

12 Entendido como parte integrante do Acordo Marraquexe criador da Organização Mundial de Comércio em 1994, caso observemos o n.º 4 do artigo 2.º do TBT, este dispõe destas normas *standard* para remover os obstáculos ao comércio, privilegiando da presunção de conformidade ao não obstaculizar, partindo do n.º 2 do artigo 2.º do TBT, sendo relevante este instrumento para a promoção da liberdade de circulação de mercadorias.

2- NÓTULA SOBRE A REGULAÇÃO DO CIBERESPAÇO

Nesta esteira, reconhece-se imperatividade desta regulação à luz da produção das normas técnicas, enquadrando estas na intitulada *Self-Regulation*[13], tomando a essencialidade dos fóruns internacionais, regulando aspetos essenciais no Ciberespaço, retomando o caso do ICANN e o sistema de domínios. Entre nós, este modelo aproxima-se da *Lex informatica*[14], regulando o ciberespaço através da fonte do conhecimento informático, partindo da configuração do sistema, com capacidade de decorrer decisões automatizadas. Indubitavelmente, este aponta para o incremento das tecnologias emergentes e disruptivas no seio da Nova Administração Pública e, em parte, têm a sua concretização nos princípios de segurança por defeito e à conceção, tomando o caso da assinatura digital.

Concomitantemente, privilegia-se modelos de governança assentes na cooperação do privado para com o público, intitulado por Co-regulação, modelo este evidente no contexto da normalização europeia, principalmente as normas harmonizadas, as quais são requeridas pela Comissão. Por fim, cumpre retomar a regulação pública com a formalidade no processo legislativo, na ótica da *Hard Law* e, por outro lado, fomentar comunicações e recomendações, previstas na ótica da *Soft Law.*[15] Nesta esteira, para a compreensão dos modelos de regulação, deveremos enunciar o objeto desta mesma regulação*: "As such, digital law must essentially concern itself with three things (although here we are interested only in the first and the last): firstly, the regulation of the code or the architecture of the Internet, understood as the standards and protocols that configure it; secondly, the regulation of the physical network; and finally, the regulation of the content and the activities that are carried out across the Internet."* [16]

13 Cf. Portalier, P., *Myths and realities of the presumption of conformity*, pp. 1-10

14 Para o entendimento aprofundado sobre a *Lex Informatica*, recomendamos a leitura: Cfr. Stemler, A., *Regulation 2.0, The Marriage of New Governance and Lex Informatica*, pp. 87-133

15 Citando Palmerini, E., *"On a different track, in order for regulation to evolve with technology and in consideration of the constraints of a 'hard law' approach, legal systems are steered towards adopting "prospective and homeostatic" instruments, capable of adapting themselves to a changing landscape, […] 'Soft law' alternatives seem the most suitable governance approach, as they have looser procedures and are compatible with the process of internal adjustment through technical delegation to independent bodies which are enabled to register variations, assess the need for amendments and implement those amendments"* Cfr. *The Interplay between Law and Technology*, pp. 7-25

16 Cfr. Teruel Lozano, G., M., *Fundamental Rights in the Digital Society: Towards a constitution for the cyberspace*, pp. 301-315

Visa-se aqui uma proteção dos direitos fundamentais da nova geração, ponderando o equilíbrio constitucional dos bens jurídicos refletido nas relações intersubjectivas, tomando o Direito Constitucional[17] como o garante destes direitos. Indubitavelmente, a regulação do ciberespaço deve ser ponderado as multinacionais, centralizando o domínio de certos serviços da Internet, não sendo este o equilíbrio constitucional, mas sim, a colaboração do público com o privado e, como nos explana Lessig, os direitos fundamentais no Ciberespaço, *máxime* a liberdade, só poderá ser alcançado com a absorção do Estado das novas tecnologias e instrumentaliza-as na prossecução do Estado de Direito democrático e Social (Lessig, 2009, *apud* Teruel Lozano, 2019).

17 São inúmeros os direitos previstos no texto constitucional, os quais carecem da interpretação constitucionalmente neutra e flexível, erguida pela Dr.ª Raquel Brízida Castro, consagrando o legislador ordinário a liberdade de opinião, a liberdade de imprensa, a liberdade de manifestação, entre outros, os quais deverão ser enquadrados no âmago do Ciberespaço, adequando essa proteção por esta interpretação e não a mera interpretação através do elemento temporal, o elemento teleológico, o elemento histórico e o elemento literal, tipicamente ensinados nas Universidades. Cfr. Bacelar Gouveia, J., *A Democracia na Teoria do Direito Constitucional*, pp. 492-527

3- NÓTULA SOBRE O FENÓMENO DA NORMALIZAÇÃO

A produção destas normas *standard* são provenientes de diversos organismos, os quais densificaremos no próximo subcapítulo. Com efeito, estas normas assumem o propósito de *compliance*, através do processo de certificação (Cf. figura 1) tipicamente por privados acreditados[18] para o efeito, visando evadir a responsabilidade pelas consequências lesivas decorrentes da atividade, concretizando no caso de exfiltração de dados, a certificação apoiará na demonstração da conformidade com o Regulamento Geral da Proteção de Dados (doravante RGPD), passando por um processo de avaliação dessa conformidade.

Figura 1 - Normalização, Acreditação, Certificação, no caso Português

Fonte: Autor

Simultaneamente, estas normas poderão atrair a procura do determinado produto/serviço pela qualidade atribuída pela certificação[19], conferindo confiança nos consumidores daquele determinado bem, diminuindo os erros e os custos. Por conseguinte, no espetro da segurança da informação, é imprescindível o papel das normas ISO (do inglês *International Organization for Standardization*), em especial a série 27001, tomando como ilustrativa a ISO/IEC 27701:2019, reconhecendo uma extensão dos controlos da ISO

18 A Acreditação, no ordenamento jurídico europeu, rege-se nos termos do Regulamento (CE) nº 765/2008
19 Neste sentido, a regulação da certificação poderá ser compreendida em quatro dimensões, repartidas em regras Cfr. Daskalova, V., I., e Heldeweg, M., A., *Challenges for Responsible Certification in Institutional Context: The Case of Competion Law Enforcement in Markets with Certification* pp. 24-71

27001:2013, com a preocupação na privacidade erguida em sede do Regulamento Geral da Proteção de Dados n.º 2016/679, de 27 de abril.

Partindo das especificidades destas normas, neste âmago, estas aglutinam informações práticas para a implementação de um determinado controlo, bem como as melhores práticas, estando à venda no próprio sítio *web*. Subsequentemente, após a compra e, no caso da ISO/IEC 27701:2019, e, posteriormente neste caso concreto, a implementação de um Sistema Gestão da Privacidade da Informação, juntamente com os controlos exigidos, é realizada a auditoria pela entidade acreditada para o efeito, habilitando ou não com o título de certificação. Conjugando com as normas ISO, neste Regulamento, nomeadamente nos artigos 42.º e 43.º, prevê-se o modelo de normalização, recaindo a acreditação de aprovação das autoridades de controlo, habilitador da certificação das organizações que visam a obtenção desta certificação [20].

3.1 sobre os organismos de normalização

Reconhecemos a essencialidade dos inúmeros *stakeholders*, focando, para o presente estudo nos organismos de normalização. No espetro internacional, existe a ISO, criada em 1946, a *International Electrotechnical Commission* (IEC), fundada em 1906, a *International Telecommunications Union* (ITU)[21], criada em 1865 com a Convenção Internacional do Telégrafo, tendo sido revista com a designação atual em 1989, criando a Constituição e Convenção da ITU. Estes organismos encontram-se sediados na Suíça, no cantão de Genebra. Já no espetro europeu, os organismos europeus de normalização (doravante OEN) são o Comité Europeu de Normalização (doravante o CEN), criada em 1961, juntamente com o Comité Europeu de Normalização Electrotécnica (doravante o CENELEC), originada em 1973 e, por fim, a *European Telecommunications Standards Institute* (doravante o ETSI),

20 Também é essneical as normas *standard* promotoras da segurança da informação na Diretiva da Segurança das Redes Informáticas (UE) n.º 2016/1148, de 6 de julho. Em especial, no considerando 43.º, para fins de cooperação internacional, no considerando 66.º, entendido enquanto impulsionador do mercado ao garantir o elevado nível de segurança, remetendo para o Regulamento (UE), n.º 1025/2012, o qual densificaremos posteriormente. Já na alínea e) do n.º 1 do artigo 16.º da Diretiva, revela estas normas enquanto medidas para salvaguarda da segurança das redes informáticas, no artigo 19.º, o papel dos Estados e a ENISA promover o uso de normas internacionalmente reconhecidas e aceites, entre outras disposições.
21 Pese embora não tenha a designação de Organismo de Normalização, deverá ser equipara como tal.

criada em 1988. Estes organismos europeus encontram-se sediados em Bruxelas, excetuando este último, encontrando-se em Sophie-Antipolis, em Valbonne na França.

Em contraste, a maioria destes organismos operam com um mandato delegado pela administração estatal para regular nas matérias incumbidas, com maior enfoque nos requisitos legais e formais[22]. Excetua-se o ETSI, dependendo da atividade a desempenhar, torna-se eclético nas suas atribuições, podendo assumir recomendações com valor acrescentado, entendido como vantagem competitiva, como também poderá desempenhar a sua função partindo de um mandato. Seguidamente, estes organismos publicam normas *standards* baseadas no consenso alargado dos seus membros, em especial, a IEC na componente de produtos de eletrónica, sistemas e serviços, como também fomenta a compreensão internacional, e, por fim, fornece avaliação de conformidade[23]. Incorpora os Comités Nacionais enquanto instâncias representantes de cada Estado reconhecido pelas Nações Unidas, entre nós o Instituto Português da Qualidade (IPQ), como também na ISO e na ITU. Este têm vindo a entrosar a cooperação com os restantes organismos internacionais, em especial com a ISO, orientando os procedimentos técnicos pelas diretivas, em especial a ISO/IEC DIR 1:2019. Simultaneamente, a ISO[24] promove a padronização visando a facilitação das trocas comerciais, incrementando os processos de negócio, desenvolvendo cooperação na esfera intelectual, científica, tecnológica e económica. Por fim, a ITU[25], com o intuito da promoção da paz e o desenvolvimento económico e social, funcionado como agente facilitar e cooperador de meios eficientes para as telecomunicações.

Concomitantemente, nos organismos europeus de normalização, o CEN[26] visa, segundo os seus estatutos, a harmonização internacional e europeia das normas *standard*, cooperando

22 Cfr. Baron, J., *et al*, *Making the Rules – The Governance of Standard Development*, pp. 1-58

23 Cfr. artigo 1 e 2 dos Estatutos e Regras de Procedimentos da IEC. Para a compreensão da estrutura orgânica da IEC, bem como o processo decisório, as regras de procedimento e os estatutos subjacentes a cada estrutura, Cfr. IEC, *Statutes and Rules of Procedure*, pp.1-33, consultado a 04 de janeiro, URL.: https://www.iec.ch/members_experts/refdocs/iec/stat_2001-2018e.pdf

24 Para a compreensão da estrutura orgânica da ISO, o seu processo decisório e as regras de procedimentos, deverá-se consultar o estatutos da ISO, com a última versão de 2017, Cfr. ISO Statutes, pp. 1-80, consultado a 04 de janeiro, , URL.: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/statutes.pdf

25 Na mesma linha do intuito anterior, recomendamos a leitura da Constituição da ITU, bem como a Convenção da ITU, Cfr. ITU, *Collection of the basic textsadopted by the Plenipotentiary Conference*, pp. 1-963, consultado a 04 de janeiro, URL.: https://www.itu.int/en/history/Pages/ConstitutionAndConvention.aspx

26 Cfr. CEN, *The Statues of CEN, Approved by the Extraordinary General Assembly of 2018-07-04*, pp. 1-16 ,consultado a 04 de janeiro, URL.: https://www.cen.eu/about/GovStructure/GeneralAssembly/Pages/default.aspx

com a ISO, sempre que possível, promovendo a remoção das barreiras comerciais, operando nos termos do Regulamento (UE) n.º 1025/2012, tal como o CENELEC[27], excetuando o objeto desta última, pois visa principalmente a harmonização no âmago dos *standards* eletrotécnicos. Ambos são representados pela lógica dos organismos internacionais, com o âmbito de aplicação reduzido à União Europeia e à EFTA. Por fim, a ETSI[28], compreendendo o seu estatuto, tem por objeto a padronização e a elaboração de normas *standard*, podendo desempenhar o papel de agente facilitador.

3.2 sobre a "Nova Abordagem"

Para compreendermos este Regulamento, é essencial depreendermos a importância de padronizar determinadas condutas, sistemas e comportamentos para o desenvolvimento civilizacional, tomando o exemplo da linguagem, como também para a facilitação do contacto entre civilizações, tomemos o exemplo da essencialidade da criação do sistema de unidades de medida de comprimento, isto na Civilização do Vale do Indo à volta de 2600 a.c., sendo imprescindível para o quotidiano.(Almacinha, 2013)[29]

Desta feita, este regulamento orienta-se pelos princípios da OMC, em especial o princípio do saber, a abertura, o consenso, a aplicação voluntária, a independência em relação a interesses especiais e eficiência, tomando como os princípios basilares. Visando a destrinça concetual das tipologias de norma do presente regulamento, previsto no n.º 1 do artigo 2.º:

"1) «Norma», uma especificação técnica, aprovada por um organismo de normalização reconhecido, para aplicação repetida ou continuada, cuja observância não é obrigatória, que assume uma das seguintes formas:

> *a) «Norma internacional», uma norma aprovada por um organismo internacional de normalização;*

27 Cfr. CENELEC, *The Articles of Association of CENELEC, Approved by the General Assembly of 2015-06-05*, pp. 1-15, consultado a 04 de janeiro, URL.: https://www.cenelec.eu/membersandexperts/referencematerial/index.html

28 Cfr. ETSI, *ETSI directives, version 38*, pp. 1-228, consultado a 04 de janeiro, URL.: https://portal.etsi.org/directives/38_directives_feb_2018.pdf

29 Para a compreensão histórica do uso da normalização, as vantagens deste mesmo uso, bem como o exemplo ilucidado, recomendamos a leitura de José António Almacinha, Cfr. Almacinha, J., A., *Introdução ao Conceito de Normalização em Geral e sua Importância na Engenharia*, pp. 1-21

b) «Norma europeia», uma norma aprovada por uma organização europeia de normalização;

c) «Norma harmonizada»[30], uma norma europeia aprovada com base num pedido apresentado pela Comissão[31] tendo em vista a aplicação de legislação da União em matéria de harmonização;

d) «Norma nacional», uma norma aprovada por um organismo nacional de normalização;"

Compreendendo o alcance da definição presente na alínea a) e b) do n.º 1 do artigo 2.º do Regulamento, cumpre explanar na alínea c) este pedido endorsa o ato de delegação, previsto no artigo 290.º do Tratado sobre o Funcionamento da União Europeia (doravante TFUE), forçando o respeito pelo preceituado no mesmo artigo, com possibilidade de revogação pelas instituições europeias com maior legitimidade democrática[32], tomando o Parlamento Europeu e o Conselho da União Europeia. Estes pedidos devem orientar pelos trâmites procedimentais do artigo 10.º conjugado com o n.º 3 do artigo 22.º do Regulamento (UE) n.º 1025/2012:

I. Pedido – Contempla o prazo estabelecido no pedido, o prazo para aprovação, exigindo uma confirmação da aceitação do pedido. Deverá prosseguir o interesse público, encontrando-se assistido do Comité como mecanismos de controlo dos Estados-Membros, consignado no Regulamento (UE) n.º 182/2011, de 16 de fevereiro. Assenta numa base consensual e verificar se corresponde aos objetivos políticos e de conteúdo enunciados no pedido da Comissão[33].

30 Como tal, inúmeras normas harmonizadas têm sido desenvolvidas no seio europeu, em particular as acessibilidades dos sítios web e aplicações do setor público (Diretiva n.º 2016/2102/UE); Substâncias químicas REACH (Regulamento n.º 7907/2006/CE); Equipamento de rádio (Diretiva n.º 2014/53/UE) entre outras presentes no seguinte link: https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards_pt

31 Cumpre referir que, nos termos do n.º 2 do artigo 17.º do Tratado da União Europeia, a Comissão congrega o monopólio da iniciativa legislativa

32 Para a compreensão da legitimidade democrática e a sua evolução no enquadramento democrático, recomendamos esta leitura, Cfr. Baptista, A., *Democracia e representação democrática*, pp. 491-514

33 Esta intervenção robusta da Comissão é essencial, caso contrário ocorreria ampla discricionariedade, produzindo normas técnicas de baixa qualidade, prejudicando o consumidor. Para uma compreensão de casos concretos: Cfr. ECOS, *The Use of Standards In Legislation and Policies*, pp. 1-18 Nesta situação, cumpre indagar sobre a responsabilidade, se a mesma deverá incidir na organização que publica, podendo recorrer ao processo C-219/15 da TÜV Rheinland como ilustrativo da falta de inspeção promotora do escândalo dos implantes mamários, ou então a responsabilidade das agências de Rating, em inúmeros casos, forjavam classificações especulativas, não correspondendo à realidade. Cfr. Rott, P., *Certification – Trust, Accountability, Liability*, vol. 16, pp. 1-250

II. Consulta - Consulta às organizações europeias interessadas, às OEN e ao Comité e, caso haja especialistas do setor. Caso as OEN careçam de financiamento para a elaboração do documento, poderão pedir à Comissão um pedido de financiamento e, esta, poderá conceder uma subvenção para a elaboração de uma norma europeia ou de um produto de normalização europeu. As OEN informam a Comissão sobre as atividades, para a elaboração dos documentos, e, conjuntamente com a Comissão, avalia a conformidade dos documentos com o pedido inicial da Comissão

III. Publicação – Caso satisfaça os requisitos previstos no pedido, deverá ser publicado no Jornal Oficial da União Europeia, podendo inclusive dispor de outros meios.

Posto os trâmites processuais, cumpre referir os efeitos jurídicos desta norma harmonizada, conferindo a presunção de conformidade[34], instrumento este originado na "Velha Abordagem" nos anos 80. Esta presunção não é, tipicamente, obrigatória para os operadores económicos, pelo contrário, é perspetivado como um benefício, expelindo a perceção da exigência desta presunção para afastar a responsabilidade.[35] Poderá contribuir para conferir segurança jurídica ao conformar a atuação com estas normas, mas deverá ser perspetivado como um indicador chave, não como prova[36], passível de ser contestada pelas autoridades públicas, conforme verificamos no n.º 1 do artigo 11.º do Regulamento. Deverá observar os requisitos essenciais e as referências terão sido publicadas no Jornal Oficial, aprovadas na qualidade de comunicações na série C do Jornal, para a produção dos efeitos mencionados. (Portalier, 2017)

34 "*The presumption of conformity is the legal consequence that derives from a known fact – the claim that the product conforms with the harmonised standards cited in the OJEU – to establish the unknown fact that the product conforms with the essential requirements of the EU law.*"

35 Tomemos o caso da perceção do caráter vinculativo normas harmonizadas previstas no seio do Regulamento dos Produtos de Construção n.º 305/2011, ilustrado no seguinte artigo. Cfr. Portalier, P., *Myths and realities of the presumption of conformity*, pp. 1-10

36 Cfr. Idem, pp. 1-10

4 - NÓTULA CASUÍSTICA

Teceremos uma análise abrangente da casuística envolvente, focando principalmente no Acórdão James Elliot de 2016 (Processo C-613/14). Este caso remonta ao fornecimento de agregados de rocha do tipo «*Clause 804 hardcore*», por parte da empresa *Irish Asphalt Limited* à construtora *James Elliot Construction Limited*, designadamente para os pavimentos interiores do edifício. Por sua vez, começou a "surgir fendas nos pavimentos e nos tetos, tornando o edifício inutilizável". Após ter assumido a responsabilidade da reparação, com o custo de 1,5 milhões de euros, procedeu a uma ação de indemnização contra a *Irish Asphalt*, tendo concluído que os agregados não estavam conformes às exigências de qualidade previstas na norma harmonizada europeia EN 13242:2002. Erguiam-se inúmeras questões no âmbito do Direito da União Europeia submetidas ao Tribunal de Justiça da União Europeia a título prejudicial, através do reenvio prejudicial do *Supreme Court*[37], interessando, para o presente estudo, a 1ª questão e a 3ª questão prejudicial:

> "1) *a) Quando os termos de um contrato privado obrigam uma das partes a fornecer um produto manufaturado em conformidade com uma norma nacional, adotada em execução de uma norma europeia (...) [Diretiva 89/106], a interpretação daquela norma pode ser submetida ao Tribunal de Justiça através de um pedido de decisão a título prejudicial, nos termos do artigo 267.o TFUE?*
>
> *b) Em caso de resposta afirmativa à [primeira questão, alínea a)], a norma EN 13242:2002 impõe que a observância ou incumprimento da mesma norma seja estabelecida unicamente com base em elementos colhidos em ensaios conformes às normas adotadas, sem mandato, pelo CEN […]se os respetivos resultados provarem de forma lógica o incumprimento da norma?* (…)";
>
> "3) *O órgão jurisdicional nacional que aprecia uma ação por incumprimento de um contrato privado com fundamento em incumprimento de um requisito de comerciabilidade ou aptidão […], é obrigado a presumir que o produto é de qualidade comerciável e apto para o fim a que se destina e, em caso afirmativo,*

37 Cfr. o artigo 267.º do Tratado sobre o Funcionamento da União Europeia

pode a presunção em causa ser ilidida exclusivamente através da demonstração de não conformidade com a norma EN 13242:2002 mediante provas efetuadas de acordo com os ensaios e protocolos referidos na norma EN 13242:2002 e efetuadas no momento do fornecimento do produto?[…]"

No que concerne à 1ª questão prejudicial, desdobrada em duas alíneas, colocou-se, pela primeira vez, na jurisprudência europeia, a questão a título prejudicial da competência do Tribunal interpretar a norma técnica harmonizada, e, o Tribunal pronunciou-se afirmativamente, dotando essa competência a título prejudicial[38]. Neste sentido, é percetível esta decisão no âmago da aplicação uniforme do direito da união, pese embora o organismo de normalização, neste caso particular o CEN, não seja qualificado de "instituições, órgãos ou organismos da União"[39], nos termos do artigo 267.º do TFUE, tratar-se-á de um ato delegado da Comissão Europeia, como já tivemos oportunidade de mencionar e, mesmo que o ato seja desprovido de efeito obrigatório[40], tal não obstaculiza a interpretação a título prejudicial do Tribunal.

Aliás, neste caso, o Tribunal foi ainda mais longe, abrangendo as normas harmonizadas ao Direito da União[41], foco o qual depreenderemos a reflexão, à luz dos modelos regulatórios, legitimado por um lado, pela Diretiva 89/106, complementando-a, como também pela publicação no Jornal Oficial da União Europeia das especificações técnicas imanentes da norma harmonizada, parametrizando-as como regras jurídicas por observar, sob prejuízo de não se garantir a eficácia jurídica[42] à norma harmonizada[43]. Por outro lado, não menosprezando a titularidade da elaboração desta norma ser confiada a um organismo de

38 Cfr. parágrafo 32.º
39 Cfr. parágrafo 34.º
40 Cfr. parágrafo 35.º
41 Cfr. parágrafo 40.º
42 Não deixa de ser interessante referir o parágrafo 60.º do Acórdão Global Garden de 2017 (processo T-474/15), o qual refere a intervenção do "advogado-geral M. Campos Sánchez-Bordona no n.º 54 das suas conclusões no processo James Elliott (…) mencionadas na audiência pela Comissão, as decisões relativas à publicação das normas harmonizadas são atos jurídicos suscetíveis de recurso de anulação" reforçando o caráter vinculativo destas normas harmonizadas e a tutela da Comissão e póstuma decisão de publicação.
43 Cfr. parágrafo 42.º, congrega eficácia jurídica material, permanecendo o afastamento da eficácia formal destas normas, pois caso tal ocorre-se, as normas emanadas dos organismos privados não careciam de escrutínio público, privatizando a função de legislar.

direito privado, é amplamente pautada por requisitos essenciais, promovidos, dirigidos e controlados por um mandato (M/125) erigido pela Comissão Europeia.[44]

Já no que concerne a 3ª questão prejudicial, o cumprimento destas normas técnicas efetiva a presunção da conformidade no respeito dos requisitos essenciais[45], prosseguindo estes o interesse público ao proporcionar os níveis de proteção adequados e, esta, por sua vez, permite a livre circulação no interior da União.[46] Por sua vez, não compete ao juiz nacional avaliar a "qualidade comerciável" do produto conforme a norma harmonizada, afastando o teor técnico. Posto isto, depreendemos os seguintes aspetos afetos à póstuma indagação do modelo regulatório:

- Competência prejudicial para interpretar a norma harmonizada, pertencendo ao Direito da União;
- Delegação aos OEN a produção de normas técnicas e supervisão, controlo e o mandato da Comissão;
- Eficácia jurídica material, tomando a complementaridade ao direito derivado e a publicação no Jornal Oficial;
- Afastamento da interpretação técnica, focando nos níveis de proteção adequados imanentes dos requisitos essenciais.

Simultaneamente, certas indagações devem sobrepor os aspetos elencados previamente, questionando se haverá o risco da delegação de decisões políticas ao privado sem mecanismos de controlo? Ao longo do trabalho, ilustrando os mecanismos de controlo dos Estados-Membros e da Comissão, reconhecemos a eficácia dos mesmos, afastando o risco intolerável, como a prossecução meramente do interesse privado.

Partindo da eficácia jurídica destas normas, deverá estas encontrarem-se publicitados e de acesso gratuito? Parece a resposta ser afirmativa, pois do momento que garantimos eficácia

44 Cfr. parágrafo 43.º
45 Cfr. parágrafo 41.º
46 Cfr. parágrafo 57.º, juntamente com o processo C-171/11 Fra.bo, sujeitando o organismo privado ao princípio da liberdade de circulação consagrado no artigo 34.º do Tratado sobre o Funcionamento da União Europeia.

à norma, carecerá do respeito, podendo ser perspetivado como obstáculos à conformidade. Podemos deduzir um novo modelo regulatório na UE, partindo deste caso do Tribunal?

Respondendo à questão de partida, o modelo regulatório na U.E alterou significativamente, aglutinando a regulação pública em parelha com a regulação privada, numa perspetiva de Co-Regulação, principalmente com a valoração das normas técnicas, em especial, as normas harmonizadas, não obstante a essencialidade da *Hard Law* e a *Soft Law*, como formas de regular que persistiram no tempo, bem como os princípios subjacentes à *Lex informatica,* regular através do código e garantir a segurança por defeito e à conceção.

NÓTULA FINAL

Poderá antecipar-se o aumento da tensão, já sentida, entre os organismos privados com o papel do Estado, assumindo o incremento da externalização de certas funções clássicas, vertendo para o privado, por vezes, confinando a um hiato discricionário. Na nossa abordagem, consideramos a necessidade de articular a atuação do privado com o público, garantindo a legitimidade democrática. Partindo dos ensinamentos de Plotke, 1997: *"A political representative looks toward the preferences of those they represent, toward others' preferences, and toward their own view of overall welfare. Political representatives recognize the existence of competing and general interests alongside those of their constituents. And they consider whether their constituents' choices are the best way to get what those constituents want." (apud* António Batista, 2010, pp. 491-514*).*

Qualquer entidade que possibilite a representação do coletivo, e, desta feita, espelhe a vontade geral dos constituintes, poderá configurar, para nós, condição suficiente para depreendermos a legitimidade democrática, até mesmo nos organismos privados, caso haja delegação dessa competência pelos órgãos públicos, tomando sempre como ponto de partida e ponto de chegada da produção da norma e, os privados, como ponto intermédio. Este é o modelo a seguir na regulação do ciberespaço, por esta envolver a afetação de interesses jurídicos fundamentais nesta nova geração de Direitos Fundamentais, a qual carece da salvaguarda por parte do Estado.

Em contraste, este Acórdão revoluciona o Direito Europeu e, em parte, revolucionará o modelo regulatório europeu, devido à reformulação do conceito de normas técnicas, em especial, as normas harmonizadas no seio da União Europeia, reconhecendo esta revolução com efeitos marcantes na regulação do ciberespaço. Conjuntamente, pelas caraterísticas intrínsecas no ciberespaço, este, por sua vez, carecerá de mecanismo inovadores, parcialmente exposto por nós, para ajustar-se à progressiva atualização tecnológica.

Compreendemos com maior profundidade o processo de normalização, subjacente aos organismos internacionais de normalização, organismos europeus, e, parcialmente o

organismo português, essenciais para a regulação do ciberespaço do futuro, protegendo os bens jurídicos indispensáveis à prossecução pública.

BIBLIOGRAFIA:

Almacinha, J. (2019). Introdução ao Conceito de Normalização em Geral e sua Importância na Engenharia, Repositório da Universidade do Porto, pp. 1-21

Bacelar Gouveia, J., (2013) A democracia na teoria do direito constitucional, obra coletiva "Liber Amicorum em homenagem ao Prof. Doutor João Mota de Campos, Coimbra: Coimbra Editora, 2013, 467-502 pp.

Baptista, A. (2010). Democracia e representação democrática. *Análise social n.º* 196, pp. 491-514, ISSN 0003-2573

Baron, J., Contreras, J. L., Husovec, M., Larouche, P., & Thumm, N. (2019). Making the Rules: The Governance of Standard Development Organizations and their Policies on Intellectual Property Rights. JRC Science for Policy Report, EUR, 29655.

Brízida Castro, R., (2016) Constituição e Ciberespaço: Argumentos Para um"Direito Constitucional Do Inimigo"? Conferência "Perspetivas Multidisciplinares em Cibersegurança", CIJIC, pp. 1-41

Daskalova, V., I., e Heldeweg, M., A (2019)., Challenges for Responsible Certification in Institutional Context: The Case of Competion Law Enforcement in Markets with Certification in Certification, Trust, Accountability, Liability, pp. 24-71

Frade, **C.**, (2003) A resolução alternativa de litígios e o acesso à justiça: A mediação do sobreendividamento , *Revista Crítica de Ciências Sociais* [Online], 65 | 2003, posto online no dia 01 outubro 2012, consultado o 05 janeiro 2020, URL : http://journals.openedition.org/rccs/1184 ; DOI : 10.4000/rccs.1184 pp. 107-128

Kallestrup, M. (2017). Stakeholder Participation in European Standardization: A Mapping and an Assessment ofT hree Categories of Regulation. Legal Issues of Economic Integration, 44(4), pp. 381-393.

Nogueira de Brito, M., (2018) Introdução ao Estudo do Direito, 2ª edição AAFDL Editores, pp.401-454, ISBN 9789726292005

Palmerini, E. (2013). The interplay between law and technology, or the RoboLaw project in context. In Law and technology (pp. 7-24). Pisa University Press.

Poiares, N. (2009), "Uma policialização da segurança privada", Polícia Portuguesa, janeiro-março, pp. 28-33, n.º 10, III Série, Lisboa: Direção Nacional da PSP. Retrieved from ResearchGate

Portalier, P., (2017) Myths and realities of the presumption of conformity, Scope and relevance of the presumption of product conformity with Union harmonisation legislation in 10 questions and answers, version 1c, pp. 1-10

Rott, P., (2019) Certification - Trust, Accountability, Liability, Studies in European Economic Law and Regulation, Springer International Publishing, vol. 16, pp. 1-250, ISBN 978-3-030-02499-4

Shaffer, G. C., & Pollack, M. A. (2009). Hard vs. soft law: Alternatives, complements, and antagonists in international governance. Minn. L. Rev., 94, 706.

Stemler, A. (2016). Regulation 2.0: The Marriage of New Governance and Lex Informatica. Vand. J. Ent. & Tech. L., 19, 87

Svantesson, D., J., B., (2019) Internet & Jurisdiction Policy Network,. Internet & Jurisdiction Global Status Report 2019., pp. 1-181

Teruel Lozano, Germán M.(2019) Fundamental Rights In The Digital Society: Towards A Constitution For The Cyberspace?. Rev. chil. derecho [online]., vol.46, n.1, pp.301-315. ISSN 0718-3437. http://dx.doi.org/10.4067/S0718-34372019000100301.

Vieira de Andrade, J., C., (2017) Lições de Direito Administrativo, 5ª edição, Imprensa da Universidade de Coimbra, DOI:https://doi.org/10.14195/978-989-26-1489-2, ISBN: 978-989-26-1488-5, pp. 1-130

Vilhena de Freitas, L., (2017) Direito Administrativo das Privatizações, in Tratado de Direito Administrativo Especial, Coord. Paulo Otero e Pedro Costa Gonçalves, Vol. VII, pp. 269-355, ISBN: 9789724064178

Waz, J., & Weiser, P. (2012). Internet governance: The role of multistakeholder organizations. J. on Telecomm. & High Tech. L., 10, 331

Sítios Consultados:

ETSI - https://portal.etsi.org/directives/38_directives_feb_2018.pdf

CENELEC - https://www.cenelec.eu/membersandexperts/referencematerial/index.html

CEN - https://www.cen.eu/about/GovStructure/GeneralAssembly/Pages/default.aspx

ITU - https://www.itu.int/en/history/Pages/ConstitutionAndConvention.aspx

ISO - https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/statutes.pdf

IEC - https://www.iec.ch/members_experts/refdocs/iec/stat_2001-2018e.pdf

Normas Harmonizadas Europeias: https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards_pt

O FENÓMENO DO PHISHING

ANTÓNIO RAMOS CARVALHO [1]

1 Mestrando em Segurança da Informação e Direito do Ciberespaço no Instituto Superior Técnico da Universidade de Lisboa (IST-UL), em parceria com a Faculdade de Direito e com a Escola Naval; Mestre em Ciências Militares Navais, Especialidade de Marinha; Especialização profissional em Comunicações e Sistemas de Informação.

RESUMO

A sociedade em que vivemos, comumente apelidada de sociedade da informação, tem vindo a oferecer um leque alargado de potencialidades para os estados e para os cidadãos, no qual a internet, os computadores, os telemóveis, os e-mails e os SMS fazem parte indissociável do seu quotidiano.

Porém, a utilização massiva da informática e da internet, se, por um lado, desempenha um papel essencial para o desenvolvimento, por outro, assume-se como plataforma facilitadora da prática de atos ilícitos, contra as pessoas, o património ou a própria estrutura organizativa da sociedade.

Neste âmbito, o fenómeno de *phishing* tem tido um crescimento exponencial ao longo dos últimos anos, e, em consequência das elevadas quantias monetárias que são subtraídas ilegalmente com esta atividade, tem existido uma crescente preocupação no seio da nossa sociedade, com os impactos sociais e económicos resultantes da concretização desta técnica fraudulenta.

O presente artigo tem como objetivo discutir o fenómeno de phishing, efetuando uma análise da problemática decorrente do modus operandi em Portugal, no que concerne ao seu enquadramento jurídico-penal, concretamente no âmbito da Falsidade Informática (art.º 3) e do Acesso Ilegítimo (artº 3) da Lei do Cibercrime, e ainda ao abrigo da Burla Informática e nas Comunicações (art. 221 do Código Penal).

Palavras-Chave: Cibercrime, Ataques Informáticos, Phishing, Correio Eletrónico e Combate ao Cibercrime.

ABSTRACT

Modern society, frequently called as information society, has been providing a huge potential for the states and for the citizens. Nowadays, the internet, the computers, the mobile phones, the emails and the SMS are an essential part of our daily lives. For instance, in 2018 the number of active internet users worldwide ascended to 4.021 billion, about 53% of the world population[1].

However, the massive use of information technology and the internet, if on the one hand plays an essential role for development, on the other, it assumes itself as a facilitating platform for the practice of illicit acts, against people, estate and the own structure of society.

In this context, the phenomenon of phishing has been growing exponentially over the past few years. Due to the high monetary amounts that are illegally subtract from phishing activity, there has been a rising concern within our society, about the social and economic impacts resulting from the use of this fraudulent technique.

In summary, this paper discusses the phishing phenomenon, doing an analysis of the problem arising from the modus operandi in Portugal, with regard to its legal-penal framework. In particular, it will be analyzed under the crime of Computer Falsehood (art. 3) and Illegitimate Access (art. 3) of the Cybercrime Law, and under computers and Communications spoof (art. 221 of the portuguese Penal Code).

Keywords: Cybercrime, Cyber Attacks, Phishing, Email, Cybercrime Law.

1 According to *Digital 2018* reports from *We Are Social* and *HootSuite*, available in: https://hootsuite.com/pages/digital-in-2018 [21-02-2020].

1. INTRODUÇÃO

Ao longo da última metade do século XX, assistiu-se a uma rápida evolução tenológica, permitindo que as sociedades gerassem elevados índices de crescimento económico e social, e desencadeando o desenvolvimento e adoção de novas Tecnologias de Informação e Comunicação (TIC), as quais moldaram a forma como as pessoas vivem e comunicam entre si, sendo atualmente, vitais ao funcionamento das sociedades modernas.

Esta nova sociedade, comumente apelidada sociedade da informação, tem vindo a oferecer um leque alargado de potencialidades para os estados e para os cidadãos, no qual a internet[1], os computadores, os telemóveis, os e-mails e os SMS fazem parte indissociável do quotidiano.

Porém, a utilização massiva da informática[2] e da internet, se, por um lado, desempenha um papel essencial para o desenvolvimento, por outro, assume-se como plataforma facilitadora da prática de atos ilícitos, contra as pessoas, o património ou a própria estrutura organizativa da sociedade. É neste contexto que Venâncio (2011, p. 15) refere que "as especificidades da criminalidade informática colocam-se, não só na transferência de comportamentos ilícitos para o ambiente digital, como na tipificação de novos crimes com elementos caracterizadores de natureza digital".

Deste modo, a criminalidade informática[3] é uma realidade incontornável da nossa sociedade, em constante mutação e evolução, tendo neste âmbito Garcia Marques e Lourenço

1 A origem da internet remonta ao período da presidência de *Eisenhower* nos Estados Unidos da América (EUA), durante a Guerra Fria. Após o lançamento pelos soviéticos do satélite espacial Sputnik, o presidente criou a agência ARPA (*Advanced Research Projects Agency)*, em 1957, com o objetivo de juntar um conjunto de cientistas de renome e competência comprovada, para incrementar a tecnologia espacial. A amplitude de matérias coberta pela ARPA levou à criação de vários departamentos especializados. Na área da informática nasceu o IPTO (*Information Processing Techniques Office*). Neste âmbito, um conjunto coincidente de descobertas desencadeou as fundações da futura internet (Belfiore, 2010).

2 Segundo José Ascensão (2001, p. 203), a informática é "um instrumento automático de elaboração e comunicação de dados".

3 Em virtude de ser um crime praticado através da internet, existem várias terminologias para designar este tipo de criminalidade, tais como: criminalidade informática, cibercriminalidade, cibercrime, entre outras. Apesar das

Martins classificado este conceito como sendo "todo o ato em que o computador serve de meio para atingir um objetivo criminoso ou em que o computador é o alvo desse ato ou em que o computador é objeto do crime" (Marques, 2006, p. 641).

De facto, nos dias de hoje verifica-se um crescimento exponencial das burlas informáticas e as fraudes financeiras à escala internacional. Estima-se que em 2017, mais de 978 milhões de adultos, em 20 países, foram vítimas de cibercrime[4]. Esta tendência verificou-se também em Portugal. De acordo com o Relatório Anual da Segurança Interna (RASI, 2017)[5], o crime de acesso ilegítimo aumentou 13%, a sabotagem informática 32% e a falsidade informática 41%.

Simultaneamente, acompanhando esta evolução, a técnica fraudulenta, denominada por *Phishing*[6], tem tido um crescimento exponencial ao longo dos últimos anos[7], a qual consiste numa forma de furto de identidade *on-line*, que poderá resultar na perda de dados pessoais, particularmente de dados de acesso às contas bancárias, tendo como consequência a subtração de património monetário das vítimas destes crime. Com efeito, o *phishing* assume-se como uma ameaça bastante séria a todos os utilizadores da internet[8], e, por conseguinte, gera uma preocupação constante nas entidades de investigação e nos setores económicos, sobretudo dos utilizadores dos serviços de *homebanking*.

Neste contexto, o presente artigo tem como finalidade definir *phishing* e efetuar uma análise da problemática decorrente do *modus operandi* em Portugal, sobretudo no que respeita ao seu enquadramento jurídico-penal. Para esse efeito, na primeira parte do artigo, serão elencadas algumas das principais causas que estiveram na origem desta atividade criminosa

disposições legais previstas para a criminalidade informática, não existe um conceito expressamente consagrado na lei e uniformemente sedimentado na doutrina e jurisprudência (Marques, 2006).

4 De acordo com Norton (2018); *2017 Norton Cyber Security Insights Report. Global Results*. Disponível em: https://us.norton.com/cyber-security-insights-2017 [06-02-2019].

5 Vd. in Relatório Anual de Segurança Interna de 2017, disponível em: https://www.parlamento.pt/Paginas/2018/abril/EntradaRelSegurancaInterna.aspx [06-02-2019].

6 Este termo, segundo Francisco Luís (Luís, 2011) provém da palavra inglesa *fishing*, fazendo alusão à tentativa de que as vítimas "mordam o anzol" e "caiam" no esquema. Para este efeito, existe a ilusão de que o isco é genuíno. De facto, um atacante terá que criar um "isco" credível e convencer o utilizador a mordê-lo. A nomenclatura *phishing* surgiu em 1996, aquando a sua menção teve lugar num *newsgroup* denominado como *alt.onlineservice. america-online*.

7 Segundo Nelson Amador (2012), da totalidade dos casos de cibercrime identificados em Portugal, 75 % são referentes ao *phishing*. Seguem-se, por ordem, os casos de acesso ilegítimo, dano informático, pornografia de crianças, *software* ilegal e sabotagem.

8 Por exemplo, de acordo com o Special Eurobarometer 423 – Cyber Security Report, aproximadamente 28% dos utilizadores da Internet na União Europeia (UE) não se sentem confiantes para utilizar os serviços de *homebanking* ou para efetuar compras através da internet.

e definido *phishing* ao abrigo da jurisprudência portuguesa. Posteriormente, na segunda parte do artigo, será analisado e caracterizado, resumidamente, o *Modus Operandi* do *phishing* em Portugal, efetuando-se, ainda, um breve enquadramento jurídico-penal da atividade de *phishing,* no âmbito da Falsidade Informática (art.º 3) e do Acesso Ilegítimo (artº 3) da Lei do Cibercrime, e ainda ao abrigo da Burla Informática e nas Comunicações (art. 221 do CP)[9].

9 Face à "economia" do presente artigo, não será efetuado o enquadramento jurídico-penal da atividade de *phishing* ao abrigo das seguintes normas: contrafação, imitação e uso ilegal de marca (art. 323º do DL nº 36/2003, de 5 de Março - Código da Propriedade Industrial); dano relativo a programas ou outros dados informáticos (art. 4º LC); branqueamento (art. 368º-A CP); associação criminosa (art. 299º do CP); apropriação ilegítima em caso de acessão ou de coisa achada (art.º 209º CP); O "furto de identidade" (uso de e-mail e designações bancárias) e o princípio da legalidade.

2. PHISHING

> *"Envio aos internautas de mensagens de correio eletrónico, com a aparência de terem origem em organizações financeiras credíveis, mas com ligações para falsos sítios Web que replicam os originais, e nos quais são feitos pedidos de atualização de dados privados dos clientes"* (CNCS, 2020).

Este novo fenómeno criminal resulta do termo em inglês "*fishing*" e consiste numa das técnicas informáticas que viabiliza o cometimento de burlas informáticas, visando especificamente, tal como o próprio termo deixa antever, "pescar" informação pessoal e confidencial dos utilizadores da internet. Acresce que, geralmente, este tipo de informação obtida ilegalmente, na maioria dos casos, sem que o utilizador se aperceba, é de natureza financeira / bancária, e visa ser utilizada posteriormente, para benefício dos criminosos informáticos, com o consequente prejuízo para as vítimas (Azevedo, 2016).

De um modo mais detalhado, segundo o Supremo Tribunal de Justiça[10], o *phishing* pressupõe:

> "*uma fraude eletrónica caracterizada por tentativas de adquirir dados pessoais, através do envio de e-mails com uma pretensa proveniência da entidade bancária do recetor, por exemplo, a pedir determinados elementos confidenciais (número de conta, número de contrato, numero de cartão de contribuinte ou qualquer outra informação pessoal), por forma a que este ao abri-los e ao fornecer as informações solicitadas e/ou ao clicar em links para outras páginas ou imagens, ou ao descarregar eventuais arquivos ali contidos, poderá estar a proporcionar o furto de informações bancárias e a sua utilização subsequente*".

10 Cfr. Acórdão no processo 6479/09.8 TBBRG.G1.S1. Supremo Tribunal de Justiça. [Em linha]. Lisboa (18-12-2013). Disponível em: http://www.dgsi.pt/jstj.nsf [22-02-2020].

Geralmente, o processo mais comum utilizado para a captura da informação concretiza-se, inicialmente, com o envio em massa de mensagens de correio eletrónico de conteúdo fraudulento (SPAM[11]), sob a capa de instituições ou empresas oficiais, podendo, inclusive, conter logotipos e imagens dessas organizações[12]. Com efeito, nesta primeira fase, o criminoso informático tem como objetivo ludibriar o utilizador, levando-o a acreditar que está a receber um *e-mail* cujo remetente é um organismo de natureza público-privado (instituições bancárias, seguradoras, entidades governamentais, entre outros (Verdelho, Phishing e outras formas de defraudação nas redes de comunicação, 2009)).

Simultaneamente, conforme elucida P. Verdelho (2009), o *e-mail* recebido pela vítima poderá incluir uma ligação para uma página web, que, após ser clicada, irá redirecionar o utilizador para essa página falsa, a qual é uma reprodução aproximada do site oficial que os criminosos informáticos pretenderam recriar. Nesta página falsa será solicitado ao utilizador a atualização, validação ou confirmação dos seus dados pessoais, com o pretexto de evitar algum tipo de quebra de segurança. Deste modo, os criminosos informáticos conseguirão obter os dados confidenciais da vítima, a partir dos quais, por exemplo, poderão aceder à sua conta bancária, e, por conseguinte, realizar transferências de montantes de dinheiro sem o consentimento da vítima.

Por outro lado, outra técnica considerada ainda mais sofisticada e perigosa, e que tem sido desenvolvida em simultâneo com o *phishing*, denomina-se por *pharming*, a qual importa sucintamente descrever e elucidar o seu significado, dado que, em diversas ocasiões, é confundida com o *phishing*. Neste caso concreto, o já citado acórdão do STJ de 18 de dezembro de 2013[13], clarifica o seu significado, referindo que esta modalidade de fraude *online* consiste em:

11 Segundo G. Marques e L. Martins (2006, p. 655) *Spam* consiste no "envio maciço de mensagens de correio eletrónico não solicitadas, em quantidades que podem não apenas causar incómodo como chegar ao ponto de bloquear o sistema de receção por saturação".

12 Por norma, as mensagens são enviadas para milhares de endereços de e-mail que foram previamente recolhidos na internet, por diversas formas. Neste âmbito, um aspeto importante que importa elucidar consiste no facto de, geralmente o envio dos e-mails ser através de computadores que se encontram sob o controle dos criminosos, e incluem principalmente, servidores web com fragilidades de segurança e em alguns casos computadores pessoais infetados com vírus (p ex. cavalos de troia) criados intencionalmente para permitir o envio de e-mails em massa (spam). Esta rede de computadores infetados por *softwares* maliciosos, controlada remotamente por criminosos, denomina-se por *Botnet* (AVAST, 2019).

13 Cfr. Acórdão no processo 6479/09.8 TBBRG.G1.S1. Supremo Tribunal de Justiça. [Em linha]. Lisboa (18-12-2013). Disponível em: http://www.dgsi.pt/jstj.nsf [22-02-2020].

> "*suplantar o sistema de resolução dos nomes de domínio para conduzir o usuário a uma pagina Web falsa, clonada da página real, baseando-se o processo, sumariamente, em alterar o IP*[14] *numérico de uma direção no próprio navegador, através de programas que captam os códigos de pulsação do teclado (os ditos keyloggers*[15]*), o que pode ser feito através da difusão de vírus via spam, o que leva o usuário a pensar que está a aceder a um determinado site – por exemplo o do seu banco – e está a entrar no IP de uma página Web falsa, sendo que ao indicar as suas chaves de acesso, estas serão depois utilizadas pelos crackers*[16]*, para acederem à verdadeira página da instituição bancária e aí poderem efetuar as operações que entenderem, destinando-se ambas as técnicas (phishing e pharming) à obtenção fraudulenta de fundos*".

Por conseguinte, o *pharming* consiste igualmente na difusão via *spam*, mas desta feita de ficheiros ocultos, os quais de forma encoberta instalam *software* malicioso[17] nos computadores ou sistemas informáticos das vítimas. Deste modo, o utilizador do computador não tem margem para desconfiar de algum indício suspeito, ao contrário do que sucede no *phishing*, onde existe a receção de um e-mail. A partir desse momento, o utilizador acredita que está a aceder a uma página escolhida por si, mas está, na verdade, a aceder ao IP de uma outra página web, controlada pelo criminoso informático (Guimarães, 2013).

O *phishing*, tal como a maioria dos comportamentos maliciosos que ocorrem na web, é uma atividade de dimensão transnacional, que surgiu inicialmente ligada à

14 O IP é a sigla de *Internet Protocol*, o qual é o endereço específico de um equipamento na internet, e estabelece como os pacotes de dados vão da origem ao destino (Marques, 2006).
15 *Keylogger* é um programa de computador do tipo *spyware* cuja finalidade é registar tudo o que é digitado, quase sempre a fim de capturar senhas, números de cartão de crédito (AVAST, 2019).
16 De acordo José Matos (2009, p. 97), *cracker* é "alguém que "quebra" códigos de segurança em sistemas pessoais ou em redes, ou obtém ilicitamente códigos de licença de programas".
17 Também denominado por *Malware*, são programas informáticos destinados a perturbar, alterar ou destruir todos ou parte dos módulos indispensáveis ao bom funcionamento de um sistema informático. São exemplos, os vírus, os vermes, os cavalos de Troia, entre outros (APDSI, 2019).

obtenção de dados de cartões de crédito, mas que atualmente tem como principal alvo os serviços de *homebanking*[18] (Barreira, 2015).

Neste sentido, concordando com Venâncio (2011, p. 15), consta-se que as "práticas e capacidades da informática, e em particular da internet, potenciam a internacionalização da criminalidade", tornando assim, mais difícil a reconstituição do percurso das informações entre o emissor e o recetor, e por conseguinte permitindo a dissimulação de atos e agentes criminosos.

18 Também denominado como banco internético (do inglês *Internet banking*), *e-banking*, banco online ou "banca eletrónica", é um serviço concedido pelas instituições bancárias aos seus clientes, permitindo-lhes executar uma série de operações bancárias, por telefone ou online, relativamente às contas dos quais sejam titulares Ac. STJ de 18/12/2013, Proc. 6479/09.8TBBRG.G1.S1 (Ana Paula Boularot) in http://www.dgsi.pt [22-02-2020].

3. TIPOS LEGAIS DE CRIME ASSOCIADOS AO PHISHING

Relativamente ao enquadramento legal do *phishing*, conforme refere Pedro Verdelho (2009), este não é claro, salientando que a maioria das jurisdições apenas pune várias parcelas desta forma de atuar, não qualificando autonomamente esta atividade complexa enquanto crime. Não obstante, o mesmo autor (2009) acrescenta que numa primeira análise, terá que se ter em linha de conta que subjacente ao *phishing* estará sempre a elaboração e emissão de mensagens de correio eletrónico de conteúdo enganoso, com indicação falsa do remetente (SPAM). Assim, ao considerar-se que uma mensagem de correio eletrónico se trata de um documento enquadrável, tal como defende Pedro Verdelho (2009, p. 414), no artigo 255.º, alínea a) do CP, "esta parcela do *phishing* poderá ser enquadrada sem dificuldades na previsão do crime de falsificação, previsto e punido pelo artigo 256.º, n.º1 do Código Penal".

Por seu turno, no que concerne à criação de uma página *Web* falsa, em tudo idêntica à página institucional de uma organização bancária, já se afigura como uma construção jurídico-penal bastante mais complexa (Verdelho, 2009). Neste sentido, abordar-se-á, em seguida, de uma forma sucinta, se este *modus operandi* do *phishing* poderá, ou não, ser individualmente enquadrado nos seguintes tipos legais de crime: Falsidade informática (Art.º 3 da LC), Acesso ilegítimo (Art. 6º LC) e Burla informática e nas comunicações (art.º 221 CP).

3.1 Falsidade informática (Art. 3º da LC[19])

No que concerne à falsidade informática, verifica-se que, conforme enuncia Pedro Verdelho (2015, p. 257), este é um crime complexo, o qual em termos genéricos "pretende transpor para o ambiente digital a proteção conferida aos mesmos interesses da falsificação do mundo real, prevista no código penal" (arts. 255º ss). Não obstante, conforme elucida José Ascensão (2001, p. 222), verifica-se que se trata de um tipo novo e não apenas um tipo qualificado em relação ao art. 256º CP. Logo o art. 3º/1 exclui a aplicação do art. 256º CP.

19 Lei n.º 109/2009 de 15/9, Disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis [22-02-2019].

No mesmo sentido, não se pode recorrer ao art. 256º como tipo geral que regeria os aspetos não especificamente regulados pelo atual art. 3º LC.

O bem jurídico que se pretende proteger no crime de falsidade informática, segundo a jurisprudência do AC do TRL, de 9 de janeiro de 2007[20], é a segurança nas relações jurídicas, e, no âmbito da temática tratada, respeitará concretamente à segurança nas transações bancárias. Por conseguinte, trata-se de um crime informático em sentido estrito, porque os atos de falsificação incidem sobre os dados informáticos ou o tratamento de dados por um sistema informático. (Brito, Falsidade Informática (art. 3º LCib), 2017).

Os elementos objetivos do crime de falsidade informática, conforme refere Pedro Verdelho (2010, p. 506), consistem em "introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos".

Como referido anteriormente, o primeiro passo levado a cabo pelos grupos criminosos, que se dedicam à captura de elementos bancários dos utilizadores dos serviços de *homebanking*, assenta na criação de páginas Web falsas, correspondente a um *site* na internet e supostamente pertencente a um banco ou entidade emissora de cartões de crédito.

Segundo Paulo Teixeira (2013), os agentes do crime, ao criarem e manterem o *site* idêntico ao do banco, preenchem a conduta prevista no nº 1 do art. 3º da Lei 109/2009, pois "*com intenção de provocarem engano nas relações jurídicas, interferem num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem"*. Por sua vez, o nº 2 agrava a responsabilidade dos agentes quando *"as ações descritas incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado"*, como

20 Cfr. AC TRL 5940/2006-5, [Em linha]. Lisboa (09-01-2007). Disponível em: http://www.dgsi.pt/jstj.nsf [22-02-2020].

claramente se constituirá o sistema de *homebanking*, enquanto plataforma de comunicação entre a instituição de crédito e o respetivo cliente.

Por outro lado, importa referir que alguns autores defendem que estes atos são meramente preparatórios de outros tipos legais de crime[21], e por conseguinte não puníveis. Neste caso, destaca-se a posição defendida por Pedro Verdelho (2009, p. 414), ao mencionar que:

> "*mais complexa é a criação de uma página web falsa, correspondente a um site Internet suposta e enganosamente construído como pertencendo legitimamente a um banco ou uma entidade emissora de cartões de crédito. Discute-se o enquadramento de uma página web no conceito de documento constante da alínea a) do artigo 255º do artigo 4º da Lei da Criminalidade Informática (Lei nº 109/91, de 17 de Agosto), que prevê a falsidade informática*".

Não obstante, Paulo Teixeira (2013) defende que o simples facto de o *site* estar criado e existir a possibilidade de um utilizador vir a aceder a este domínio falso, acreditando que está na página do seu banco, preenche os elementos objetivos necessários para que o autor incorra na prática do crime de falsidade informática. Neste sentido, o mesmo autor (2013), acrescenta que os agentes do crime incorrem na prática dos crimes de falsidade informática e burla informática e nas comunicações[22], dado que os respetivos tipos protegem interesses diferentes, não existindo consunção, nem um eventual concurso aparente. Neste sentido, Paulo Teixeira (2013, p. 23), conclui que "é cometido um crime de falsidade informática na forma continuada, nos termos dos art. 30º, nº2 e art. 79º do CP".

21 Defendem estes autores a ideia de que as mensagens por si só constituem um mero "furto de identidade" (da pessoa coletiva que é a instituição bancária) e portanto não punível em termos da legislação penal nacional, na medida em que por si só não são adequadas à produção do prejuízo patrimonial. Neste sentido, concordando com Paulo Teixeira (2013, p. 22), discorda-se desta posição, dado que o bem jurídico protegido é "a segurança das relações jurídicas e não o património, bem jurídico que virá a ser de facto afetado, mas numa fase ulterior e não neste momento".

22 Segundo Paulo Teixeira (2013), existe um concurso real heterogéneo entre o crime de falsidade informática e o crime burla informática e nas comunicações, não existindo uma relação de sobreposição ou intersecção entre os dois tipos.

3.2 Acesso Ilegítimo (Art. 6º LC)

O conceito de Acesso Ilegítimo, conforme clarifica Pedro Venâncio (2011), respeita principalmente às infrações relativas às ameaças à segurança (confidencialidade, integridade e disponibilidade) dos sistemas informáticos. Por conseguinte, o bem jurídico protegido é a segurança do sistema informático.

No que concerne à conduta típica do acesso ilegítimo, esta assenta no facto de se aceder, por qualquer modo, a um sistema informático, sem a permissão legal ou sem autorização do proprietário, nos termos do n.º 1 do Art.º 6 da LC, bem como no facto de o agente "ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as ações não autorizadas" (nos termos do n.º 2, do Art. 6º da LC). Deste modo, conforme refere a jurisprudência do Ac. do TRG de 17 de novembro de 2008[23], trata-se de "um crime de perigo abstrato e constitui uma barreira para evitar a prática de outros ilícitos de maior gravidade". Com efeito, o crime fica consumado com o acesso não autorizado nos termos da al. a), do nº 4, do Art. 6º, a tomada de conhecimento de um segredo comercial ou industrial, ou de dados confidenciais protegidos por lei, configura circunstância agravante do crime de acesso ilegítimo.

Relativamente ao tipo subjetivo, constata-se que foi eliminada a exigência do elemento subjetivo especial da ilicitude vertida no Art. 7.º da LCI[24], "intenção de alcançar, para si ou para outrem, um benefício ou vantagem ilegítimos", facto que deixa claro que o crime consiste apenas no acesso doloso[25] não autorizado a um sistema informático, independentemente do móbil do agente ou o meio por ele utilizado (Brito, 2017).

Neste contexto, perante o *modus operandi* das ações de *phishing*, verifica-se que os agentes do crime agindo dolosamente, adotam uma conduta suscetível de se enquadrar no

23 Cfr. Acórdão no processo 2233/07 Tribunal da Relação de Guimarães. [Em linha]. Lisboa (17-11-2008). Disponível em: http://www.dgsi.pt/jstj.nsf [22-02-2020].
24 Lei n.º 109/91, de 17/8, disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=151&tabela=lei_velhas&nversao=1&so_miolo= [22-02-2020].
25 Em qualquer das modalidades de dolo previstas no Art. 14º do CP, Lei n.º 48/95, de 15/5 disponível em http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=109&tabela=leis [22-02-2020].

previsto nºs 1 e nº 2 do art. 6º da LC, uma vez que, podem aceder ao sistema informático da vítima, sem a sua permissão e sem o seu conhecimento. Além disso, face aos criminosos tomarem conhecimento de dados confidenciais, protegidos por lei, nos termos da al. a), do n.º 4 do art. 6º é agravada a punibilidade do ilícito (Teixeira, 2013).

Face ao exposto, e conforme afirma Pedro Teixeira (2013), encontram-se preenchidos os requisitos dos nºs. 2, e al. a) do nº4 do art. 6º da LC, pelo que, por conseguinte, trata-se de um crime agravado, dispensando a necessidade de queixa-crime para o procedimento criminal[26].

Por fim, quanto ao concurso, embora existam outros autores que possuam posições dissonantes[27], para Pedro Teixeira (2013), existe um concurso efetivo real entre o crime de acesso ilegítimo e o crime de burla informática e nas comunicações. A primeira razão avançada pelo autor (2013), assenta no facto de que o fenómeno de *phishing* não poderá reduzir o efeito ilícito do art.º 6 a um ato de execução da burla informática e nas comunicações além do que os agentes do crime terão acesso a vários dados pessoais da vítima, arquivados no seu computador.

Concomitantemente, Pedro Teixeira (2013, p. 36), ainda enfatiza que: "*com a consunção do art. 6º da LC pelo art. 221º do CP o agente seria apenas punido pela prática de um ilícito, o que a nosso ver não iria ter em linha de conta a prática pelo mesmo, num momento anterior, de outro tipo de crime autónomo*".

26 Neste âmbito importa esclarecer que, conforme menciona Pedro Venâncio (2011), o tipo legal do "Acesso Ilegítimo" se encontrava já contemplado, quer no revogado Art. 7º da LCI, quer no Art. 2º da CCiber., pelo que o procedimento criminal dependerá de queixa, sendo um crime semi-público, exceto nos casos previstos no nsº 2 e 4 do art.º 6 da LC, conforme já mencionado.

27 Neste âmbito, por exemplo Pinto de Albuquerque defende que "há uma relação de concurso aparente (consunção) entre o crime de burla informática e os crimes de falsidade informática, dano relativo a dados ou programas informáticos, sabotagem informática, acesso ilegítimo e a interceção ilegítima, sendo estes factos prévios não puníveis" (Albuquerque, 2010, p. 691)

3.3 Burla Informática e nas comunicações (art. 221ºCP)

Neste crime o bem jurídico protegido é, conforme elucida Almeida Costa (1999), o património numa aceção jurídico-económica, ou seja, como o conjunto de utilidades económicas detidas pelo sujeito e cujo exercício ou fruição a ordem jurídica não desaprova[28].

De igual modo, conforme refere Almeida Costa (1999), a burla informática constitui um crime de execução vinculada, dado que se restringe à exigência de que a lesão do património se produza através da utilização de meios informáticos, e que não se reconduza ao *modus operandi* da burla do art. 217 CP. Do mesmo modo, Teresa Quintela de Brito (2017) elucida que o crime de burla informática, além de ser um crime de execução vinculada, também poderá ser classificado como um crime de dano/lesão do bem jurídico, por a sua consumação depender da provocação de um prejuízo patrimonial (diminuição do ativo/aumento do passivo), bem como um crime material/de resultado, uma vez que a sua consumação depende de um evento espácio-temporalmente destacado da ação, que consiste na saída dos bens ou valores da esfera de disponibilidade da vítima.

No que diz respeito às ações desenvolvidas pelos agentes do crime para a condução da atividade de *phishing*, estas visam sobretudo a tentativa de captura das credenciais bancárias do serviço de *homebanking* da vítima. Para tal, a vítima irá aceder, sem tomar conhecimento desse facto, a uma página Web falsa, que tenta reproduzir o mais fielmente possível o sítio original do seu banco, induzindo-a a introduzir os seus dados bancários. Com efeito, os criminosos na posse destes elementos irão aceder à conta bancária da vítima, lesando o seu património (Teixeira, 2013).

Decorrente deste modo *modus operandi*, conforme menciona Rita Santos (2005), infere-se que esta atividade se diferencia da burla clássica, pela ausência do momento intersubjetivo que a caracteriza, ou seja, existe burla informática nos casos em que o prejuízo patrimonial decorre diretamente da operação informática, totalmente automatizada em que a intervenção humana não corresponde a um controlo efetivo e crítico do resultado do

28 Segundo, Almeida Costa (1999), incluem-se no património os direitos subjetivos patrimoniais (de carácter real ou obrigacional), os lucros cessantes e demais expectativas legítimas de obtenção de vantagens económicas.

tratamento informático de dados. É neste sentido que Almeida Costa (1999, p. 330), concomitantemente afirma que:

> "*a burla informática concretiza-se num atentado directo ao património, i. e., num processo executivo que não contempla, de permeio, a intervenção de outra pessoa e cuja única peculiaridade reside no facto de a ofensa ao bem jurídico se observar através da utilização de meios informáticos*".

Com efeito, tal característica diferencia-o da burla comum, que, como sobressai do art. 217º do CP, pode ser cometida por recurso a qualquer erro ou engano quanto aos factos que o agente astuciosamente provocou[29] (Brito, 2017). Perante estes factos, Pedro Teixeira (2013) refere que o crime de burla informática é um tipo de crime não negligente e necessariamente doloso, em que, a "*intenção*" exigida não é compatível com o dolo eventual (art. 14º do CP). Acresce que, e de acordo com o mesmo autor (2013), outro aspeto, que diferencia a burla informática da burla tradicional, assenta no facto de a consumação do prejuízo patrimonial se verificar como uma consequência adequada da conduta do agente em que não se pode desprezar a intervenção da vítima, sobressaindo desta distinção, a relação de exclusão[30] entre o crime de burla e o crime de burla informática, dados os diferentes modos de execução.

Outro aspeto que importa clarificar prende-se com o facto dos agentes do crime terem de aceder à conta bancária da vítima, sem o seu consentimento, para posteriormente concretizarem o levantamento das verbas disponíveis. Este acesso não autorizado, *a priori*, enquadra-se nos elementos objetivos da prática de um crime de acesso ilegítimo, dado que o agente do crime age, "sem permissão legal ou sem para tal estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo acede a um sistema informático" (nº1, art. 6 LC). Sendo agravado em virtude de "através do acesso, o agente tiver

29 Concretamente, este facto distingue-a da burla do art. 217 CP, dado que, nesta, a atuação ardilosa do agente tem de produzir um erro ou engano sobre a vítima, que a leva a praticar um ato de diminuição patrimonial (própria ou alheia), existindo, conforme elucida Teresa Quintela de Brito (2017, p. 3), "um duplo nexo de imputação objectiva (do engano da vítima à acção do agente; da diminuição patrimonial à indução em erro da vítima) ".
30 Neste caso concreto, Teresa Quintela de Brito (2017, p. 4), denomina-a por relação de alternatividade ou de exclusividade típica, dado que, conforme a mesma clarifica "as situações enquadráveis, no art. 221º nunca realizam o tipo de burla do art. 217º".

tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei ” (al. a), nº4, art. 6 LC). Não obstante, apesar do crime de acesso ilegítimo se constituir como um meio para a realização do crime de burla informática, não constitui o elemento essencial deste crime. Assim, o acesso não autorizado à conta bancária da vítima será consumado pelo crime do qual é o meio de execução (Teixeira, 2013). Por conseguinte, conforme elucida Rita Santos (2005), neste caso em que a prática deste ilícito pressupõe, em regra, o acesso ilegítimo a um sistema ou rede informáticos ou a interceção não autorizada de comunicações eletrónicas, verifica-se que existe uma relação de consunção pura, sendo que, as incriminações previstas no art. 6º LC são absorvidas pela consagrada no art. 221º, nº1 do CP.

4. CONCLUSÕES

Numa primeira análise, verifica-se claramente que em virtude do crescimento exponencial do número de casos de *phishing* registados em Portugal nos últimos anos, e consequentemente, das elevadas quantias monetárias que são subtraídas ilegalmente com esta atividade, existe uma crescente preocupação no seio da nossa sociedade, com os impactos sociais e económicos resultantes da concretização desta técnica fraudulenta.

No que concerne ao *modus operandi* do *phishing*, constatou-se que esta se inicia com o envio da remessa maciça de mensagens de correio eletrónico (spam), que incluem uma ligação para uma página na web falsa. Nesta primeira fase, o pirata informático visa enganar a vítima, fazendo-a acreditar que está a receber um *e-mail* cujo remetente é a sua entidade bancária. Em seguida, a vítima clica na hiperligação referida na mensagem de correio eletrónico, deparando-se com uma página semelhante ao *site* oficial do seu banco, onde lhe será solicitada a identificação através da introdução do nome de utilizador e palavras-passes referentes à sua conta bancária, ou de outras informações confidenciais como o número de conta, número de contribuinte ou outros dados pessoais. Deste modo, os piratas informáticos passam a conhecer os códigos secretos relativos às contas bancárias da vítima, permitindo-lhes o acesso a estas e a realização de transferências de montantes sem conhecimento, nem consentimento do titular da conta (Verdelho, 2009).

Relativamente ao enquadramento legal do *phishing*, notou-se que, conforme menciona Pedro Verdelho (2009), este não é claro, constatando-se que a maioria das jurisdições apenas pune várias parcelas desta forma de atuar, não qualificando autonomamente esta atividade complexa enquanto crime. Não obstante, o mesmo autor (2009) acrescenta que, numa primeira análise, terá que se ter em linha de conta que subjacente ao *phishing* estará sempre a elaboração e emissão de mensagens de correio eletrónico de conteúdo enganoso, com indicação falsa do remetente (SPAM). Assim, ao considerar-se que uma mensagem de correio eletrónico se trata de um documento enquadrável, tal como defende Pedro Verdelho (2009, p. 414), no artigo 255.º, alínea a) do CP, "esta parcela do *phishing* poderá ser enquadrada sem dificuldades na previsão do crime de falsificação, previsto e punido pelo artigo 256.º, n.º1 do Código Penal".

Por sua vez, no que concerne à criação de uma página *Web* falsa, em tudo idêntica à página institucional da instituição bancária, já se afigura como uma construção jurídico-penal bastante mais complexa (Verdelho, 2009). Perante este facto, analisou-se de uma forma sucinta, este *modus operandi* do *phishing* ao abrigo dos seguintes tipos legais de crime: Falsidade informática (Art.º 3 da LC), Acesso ilegítimo (Art. 6º LC) e Burla informática e nas comunicações (art.º 221 CP).

Decorrente desta análise, verifica-se que a dificuldade de abordagem do fenómeno de *phishing* se encontra, por um lado, refletido na escassez de jurisprudência nesta área no ordenamento jurídico português, e por outro, da necessidade da existência de um conhecimento profundo que engloba, tanto questões de natureza técnica, como de natureza jurídica.

Com efeito, a cibercriminalidade, como é corroborado como Pedro Teixeira (2013, p. 114), é efetivamente um dos

"fenómenos que, provavelmente, veio lançar um dos maiores desafios nas estruturas judiciais e de investigação criminal, desde logo pela relativa impunidade com que cada vez mais é praticada, fruto de uma maior sofisticação das técnicas e tecnologias empregues, bem como pela sua celeridade, assim como pelo seu caráter transnacional e a sua volatilidade".

Neste sentido, para os Estados poderem fazer face aos novos desafios que a cibercriminalidade acarreta, é fundamental desenvolver e fomentar medidas eficazes de prevenção. Estas podem traduzir-se através da implementação de políticas de sensibilização e aumento da cibereducação da sociedade, e pelo desenvolvimento e incremento da formação especializada dos profissionais que trabalhem nesta área, aliada à disponibilização de mais e melhores meios, tanto humanos como materiais.

BIBLIOGRAFIA

Albuquerque, P. P. (2010). *Comentário do Código Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem* (2ª ed. ed.). Lisboa: Universidade Católica Portuguesa.

Amador, N. (2012). *Cibercrime em Portugal: Trajetórias e Perspetivas de Futuro.* Lisboa: Instituto Superior de Ciênciais Policiais e Segurança Interna.

APDSI. (6 de 2019). *Glossário da Sociedade da Informação.* Fonte: APDSI: http://www.apdsi.pt/index.php/portugues/menu-secundario/glossario.html

Ascensão, J. O. (2001). Criminalidade informática. *Direito da Sociedade de Informação, II*, 203-228.

AVAST. (22 de 2 de 2019). *Academia de Ameaças Online*. Fonte: AVAST: https://www.avast.com/pt-br/c-online-threats

Azevedo, A. (2016). *Burlas Informáticas: Modos de Manifestação.* Braga: Universidade do Minho.

Barreira, M. (2015). *HOME BANKING - A REPARTIÇÃO DOS PREJUÍZOS DECORRENTES DE FRAUDE INFORMÁTICA.* Lisboa: Faculdade de Direito da Universidade Nova de Lisboa.

Belfiore, M. (2010). *The Department of Mad Scientists.* Nova Iorque: Harper Perennial.

Brito, T. Q. (2017). Acesso Ilegítmo. *Cibercrime* (pp. 1-6). Lisboa: FDUL.

Brito, T. Q. (2017). Burla informática e nas telecomunicações. *Cibercime - 2016/2017* (pp. 1-9). Lisboa: FDUL.

Brito, T. Q. (2017). Falsidade Informática (art. 3º LCib). *Cibercrime 2016-2017* (pp. 1-12). Lisboa: FDUL.

CNCS. (23 de 2 de 2020). *Glossário*. Fonte: Centro Nacional de Cibersegurança Portugal: https://www.cncs.gov.pt/recursos/glossario/

Costa, A. (1999). *Comentário Conimbricence do CP, Tomo II.* Coimbra: Coimbra Editora.

GNR. (23 de 2 de 2020). *Phishing*. Acesso em 23 de 2 de 2020, disponível em GNR: https://www.gnr.pt/cyberFraudesNet.aspx

Guimarães, M. (2013). A fraude no comércio electrónico: o problema da repartição do risco por pagamentos fraudulentos. In Infracções Económicas e Financeiras. Em *Estudos de Criminologia e de Direito* (pp. 581 - 597). Coimbra : Coimbra Editora.

Luís, F. (2011). Proteger o dinheiro – Home banking, Conselhos aos utilizadores. *Inforbanca*(88), 10-11.

Marques, L. M. (2006). *Direito da Informática* (2ª ed. ed.). Coimbra: Almedina.

Matos, J. (2009). *Dicionário de Informática e Novas tecnologias.* Lisboa: FCA - Editora de Informática, (Ed.), Lidel.

Santos, R. C. (2005). *Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos.* Coimbra: Coimbra Editora.

Teixeira, P. G. (2013). *O fenómeno do Phishing - Enquadramento jurídico-penal.* Lisboa: Universidade Autónoma de Lisboa.

Venâncio, P. (2011). *Lei do Cibercrime - Anotada e Comentada* (1.ª Edição ed.). Lisboa: Coimbra Editora.

Verdelho, P. (2009). Phishing e outras formas de defraudação nas redes de comunicação. Em *Direito da Sociedade da Informação (Oliveira Ascensão, coordenação).* (Vol. III, pp. 407-419). Coimbra: Coimbra Editora.

Verdelho, P. (2010). *Anotação à Lei n.º 109/2009, de 15 de setembro.* Lisboa : Universidade Católica Editora.

Verdelho, P. (2015). Em C. J. Santos, *Enciclopédia de Direito e Segurança* (pp. 255-263). Lisboa: Almedina.

SOCIAL NETWORKS AND PUBLIC OPINION MANIPULATION IN DEMOCRATIC REGIMES

NATHÁLIA CARVALHO SCHMIDT DE DEUS [1]

1 Lawyer and Master student at Faculty of Law in the University of Lisbon, in Public International Law, 2018/2020; Master student in Information Security and Cyberspace Law in the University of Lisbon; "Instituto Superior Técnico" of Lisbon and Naval School of Portugal, 2019/2021.

ABSTRACT

Based on a multi – dimensional view, this article aims to analyze the acts of public opinion manipulation in democratic regimes. Therefore, a juridical approach has been used in the perspectives of International Law and Domestic Law with bases on technological science to facilitate the understanding of certain means of executions in the control of social media.

Keywords: Social networks, technology, botnets, Law, Democracy, Public Opinion, control, manipulation.

1.INTRODUCTION

The evolution of media enables us through social networks a popular participation once unthinkable in the democratic activity of the present day.

It should be noted that there is no exact definition for democracy, but it would be the only power organization safeguarding individual freedom and all the elements that structure it, such as political pluralism, freedom of expression, freedom of information, freedom of communication.

If the direction of public opinion in a particular sense tends to bind democratic decisions and, if the result materializes in the way of secret scrutiny or through popular participation by referendum, the analysis in the field of the source of formation of these opinions in the media is required. Using the development of this view we can generate concrete and diffuse effects within society.

If the democratic regime is established in the structures provided by the legal certainty of fundamental rights, the decisive political impetus on the part of its citizens cannot be threatened to limit their free expression of will and consequently cause a chilling effect that hinders the free development of society. The present activity of online information exchange is an area still under regulatory development by states, which are far from establishing definitive rules by mutual agreement, even due to the dynamism that is outlining technological developments. Because of this, several political and economic crises are being noted and the issue of democratic regimes is a subject of much discussion today.

In turn, the network comes in opposition to the rigid and centralizing forms of social and political entities, when it presents an idea of decentralization, an aspect that produces social transformations.

The goal of this report is to establish an approach to the existence of what types of domestic and international legal violations are subject to acts that manipulate public opinion and their means of enforcement in social networks. But in order to do so, two aspects need to be distinguished: law from the point of view of the internal politics of a state; and law from a foreign policy point of view.

2. THE MANIPULATION OF PUBLIC OPINION IN STATE POLITICS

There are many ways usually used to manipulate public opinion, from fake news that violates the good name of the agents and political entities, or even through truthful news affecting personality rights, or the use of sensationalist images that touch a particular collective group, or the use of messages of superficial and political content that tend to manipulate recipients without instruction on subjects or without a sense of criticism. These are the manipulative forms that have existed for many years offline and have not been triggered by an incisive influence on the general public tending to direct some sense in state internal politics to a point of destabilizing it. However, the current manipulation methods are generated by machines that have such potential to reach a massive number of people and much more effectively than a mere influence by television.

We should be able to distinguish between: publications made by responsible journalism under guarantee of press rights corollary of freedom of expression in the pursuit of publication of information in the public interest and publications published by anonymous or sponsored individuals, used with political interests, which aim to use manipulative technological tools of public opinion. The first one has an investigative role within democracies and interference by public authorities must be restricted so that it does not cause an inhibitory effect on their performance or "chilling effect"; the second one refers to the ways of using the media for the behavior of certain illicit acts or of personal interests, often anonymous and not intended to inform. The first is protected by freedom of expression, by international law of the human person, should not have the intention of helping those in power or in groups of political parties; but the second, the interest in helping the policies of entities and the use of instruments of "information operations" that is the use of information technology to achieve government objectives[1].

1Torsten Stein; Thilo Marauhn, *International Law Aspects of Information Operations*, ZaöRV 2000, p.1. Available in: https://beck-online.beck.de/Bcid/Y-300-Z-ZAOERV-B-2000-S-1-N-1, (last access in 03/28/2019).

The right to freedom of propagation rooted in the freedom of expression is understood to be a defense mechanism against the state "prohibiting all direct and indirect state interference, public or subtle, official or non-official, in the conformation and selection of schedule content or a particular program"[2]. Considering the democratic and constitutional relevance in the non-interference of public authorities in the areas of communication (art. 34º, item 4, "Constituição da República Portuguesa", hereinafter designated "CRP").

In reinforcement of this constitutional precept, art. 10 of the European Convention on Human Rights (hereinafter "ECHR") states that "everyone has the right to freedom of expression. This right shall include freedom of opinion and the freedom to receive or impart information or ideas without interference by any public authority and without consideration of borders..." In addition to its broad provision in several other international documents: Article 11 of French Declaration of Human and Citizen's Rights; Article 19 of the Universal Declaration of Human Rights (hereafter "UDHR"); Article 13 of the American Convention on Human Rights (ACHR).

All of these individual freedoms depend on the non-interference of any public authorities and may be considered, directly or indirectly, manifest or subtle, official or unofficial. Predictions in international documents play a role in guaranteeing these constitutionally guaranteed freedoms.

2.1. The online misinformation

All forms tending to manipulate public opinion vitiate the free manifestation of the collective will of a society, by which it can be called digital, since it is predominantly linked to digital media. Article 21.3 of the UDHR states that "the will of the people is the foundation of the authority of public authorities; and must be expressed through honest elections to be held periodically by universal and equal suffrage, by secret ballot or by an equivalent process safeguarding freedom of vote".

2 Raquel Alexandra de Jesus Gil Martins Brízida Castro, Constitution, *Law and Regulation of the Media: Contribution to the Study of the Portuguese Constitution of Communication*, PhD in Law, Legal-Political Sciences, University of Lisbon, Faculty of Law, 2014, p. 426.

However, any result achieved in the political context of online misinformation is due to a contaminated will to the detriment of its free expression due to the intention of misleading the electorate also contracting online social networking services, and the techniques used for the manipulation of public opinion in the private sphere are tools that endanger individual freedoms by their high incisive power. The violation of individual fundamental rights serves as a means of satisfying the objectives of persons exercising or about to exercise public power. These are people who use the vulnerability still existing in democratic regimes and their predisposed tools in the media to violate the regime or system itself.

Another context is the social networking services used by users made available by online platforms in the consent and acceptability of their security terms, which are legal relationships subject to contractual liability and must obey the laws in force, whether or not provided for in the contract.

Contractual liability arises from a "non-fulfillment or defective fulfillment of a pre-existing obligation resulting from a contractual wrongdoing". While non-contractual liability is a "breach of the general duty to abstain"[3].

As soon as there is a contract between the user and the online platform providing social networking services, we can conclude that the conflicts resulting from this agreement is resolved within the contractual liability area itself.

On the other hand, with regard to tortious liability, Article 485 (1) of the Civil Code provides advice, recommendations or information by stating that "simple advice, recommendations or information shall not hold anyone liable, even if there is negligence on their part". But there are three exceptions to Article 485 (2): a) "when the information provider has assumed responsibility for the damage that the information could cause; b)

3 Francisco dos Santos Amaral Neto, "Civil Liability", in João Bigotte Chorão (Dir), *Polis Encyclopedia Verb Society and State, Anthropology, Law, Economics, Political Science*, vol.5, Lisbon / São Paulo, Verb, pp. 466-474 (pp. 468-469).

when there was a legal duty to give advice, recommendation or information and was done with negligence or intent to prejudice; c) when the agent's procedure constitutes a punishable fact".

We know that within social networking platforms, political people join the service, with or without the acronym of the agency it represents. The duty to inform is done by official public act outside the context of social networks. Since the official means of publication exist, the use of social networks becomes merely optional and not substitute of the official means of publication. The use of social networks by public agents only serves to reinforce the disclosure of a particular subject, as it comprises a right submerged by the freedom of expression characteristic of the democratic regime. However, online communication networks may be used with the intent of harming users by misunderstanding the information provided.

If the public agent had a duty to disclose any information he should do so through appropriate administrative acts and not merely through social networks. If it only proceeded with the publication on social networks, it acted negligently, as it is not considered an official public act when using that legal faculty. When disclosing information online with the intent to harm on must likewise be subject to the obligation to indemnify. Finally, compensation will depend on what is considered to be a punishable fact in the context of communication via social networks.

The doctrine of tortious liability establishes as one of the presuppositions of violation the practice of an act that constitutes an abuse of law, embodied in articles 334, 484, 485, 486, 491, 492 and 493 of the Civil Code; Among them, Articles 334 and 485 deserve to be highlighted in the matter.

Even if he holds a public authority and he formally respects his powers that are conferred on him, exercising a right that is questionable to the fundamental values of the legal system[4], illegitimate acts are configured.

According to Article 334 of the Civil Code, it is found that abuse of the right is nothing more than the proprietor's manifestly exceeding the limits imposed by good faith, good morals or the economic and social purpose of that right. This is a violation of the legal prohibition that reveals an Aquilian liability situation.

It should be noted that this article is normally compared with the German BGB's §826 clause on good manners, but unlike that doctrine, Portuguese Civil Law does not require the presence of deceit, even in its eventual form of deceit, to damage is compensated[5]. If the information is provided in a manner that is distorted and contrary to good morals or the economic and social purpose, by the agent, there should be reimbursement even if the intent was not present.

The presence of the damage, which in the context of social networks, is linked to misuse of information, tending to violate personality rights and private rights, related to good name, reputation, the image of a collective person or group or even messages of violence and hatred, compensation should be provided when the prosecution of the agent is punishable.

Much has been mentioned about hate speech on social networks. Therefore, it is important to quote about the decision of the Strasbourg Court in the case of *Delfi AS v. Estonia*, where "hate speech" does not have a well-defined and universally accepted definition. The theme covers a wide range of hate messages, ranging from offensive to derogatory remarks and comments, stereotypes, abusive and negative, intimidating, inflammatory speeches that incite violence against specific individuals and groups. It

4 Manuel A. Carneiro da Frada, *A "Third Way" in Civil Liability Law? The problem of attributing damages caused to third parties by company auditors*, Coimbra, Almedina, 1997, p. 49.
5 *Ibid*., p. 51.

also reiterates that only the most notorious forms of hate speech, ie those that constitute incitement to discrimination, hostility and violence, are considered illegal[6].

2.2. Competition and Pluralism

Concerning competition and pluralism, acts aimed at promoting online misinformation through computer tools ultimately trigger the concentration of ownership. Competition rules must take into account media pluralism concerns[7], but techniques of manipulating public opinion are threats that put them at risk. Abuse of the above mentioned right, in the context of the media, can be referred to as "abuse of public opinion"[8].

The current Portuguese legal-constitutional order provides for freedom of expression and information, freedom of the press and media in Articles 37 and 38 of the CRP. The Constitution does not prohibit any sector of private or even non-economic /economic activity in the performance of these fundamental guarantees[9].

The monopolization of information is very dangerous especially in democratic regimes that may be susceptible of political manipulation. The use of information, when used as a manipulative computational management tool, other alternative media, plural and free competition in the information market, end up being a refuge that ensures the democratic principle.

The Constitution expressly enshrines as the fundamental principle of economic and social organization the principle of the subordination of economic power to democratic political power[10], and sets out certain priority tasks of the State, in particular, "to ensure the efficient functioning of markets so as to ensure balanced competition between

6 Delphi AS v. Estonia, Appl. No. 64569/09, judgment of 8 June 2015. Available in footnote 9, paragraph. 28, p. 70 at: http://hudoc.echr.coe.int/eng?i=001-155105 (last accessed 09/20/2019).
7 Raquel Castro, *ob.cit*., p.381.
8 *Ibid*., p.383.
9 Evaristo Sousa Mendes, *Annotation to Article 61, in Annotated Portuguese Constitution*, Tome I, 2nd Edition, MIRANDA / MEDEIROS, Coimbra, Coimbra Publisher, 2010, p. 1210.
10 Article 80, item (a) of the CRP ("Constituição da República Portuguesa").

companies ", but to this end," it is necessary to "counter monopolistic forms of organization and to repress abuses of dominant position and other practices harmful to the general interest"[11]. Ways of disseminating, for example, through automated services, online misinformation by private companies, even at the request or under the payment or exchange of favors, by anonymous political agents, endanger these constitutional precepts.

Even if there is a Regulatory body such as the ERC, the eminent Professor MIRANDA warns of the existence of an unconstitutional omission, considering that the assignment of his function is insufficient to all titles[12].

The concern to ensure the pluralism brought by the ERC, Media Regulator, is restricted to the functioning of the press market, in order to enable its transparency, the confrontation of information and the various currents of opinion, the quality of publications allowing a wide choice by consumers[13], which turns out to be an alternative when systems linked to social networks suffer manipulative threats of information by automated technological methods, to the detriment of the right to be informed. It should be noted that the right to information is a fundamental right and has a very significant link with the democratic principle. The development of public opinion depends on the guarantee of this right.

2.3. Violation of electoral rights

Techniques used to trigger mass online misinformation by political interests undermine the principle of equal opportunities and the treatment of various candidatures in election campaigns, as provided for in Article 113 (3) (a) of the CRP. These are techniques that give priority to the dissemination of mass publications that favor one

11 Article 81, item (f) of the CRP ("Constituição da República Portuguesa").
12 "The unconstitutional legislative omission has to do with the lack of enforceability to constitutional command. This omission is compounded by a constant phenomenon of concentration according to purely economic motives". Jorge Miranda, "Freedom of Social Communication and Public Service of Radio and Television", in Carlos Blanco de Morais and others (coord), *Media, Law and Democracy*, Coimbra, Almedina, 2014, p.28.
13 Raquel Castro, *ob.cit.*, pp. 397-398.

political party or political agent over the others, to the detriment of the equal opportunities sought in an electoral campaign. The equality sought is that which allows for parity of rights between candidates.

The freedoms guaranteed by the Constitution, such as freedom of propaganda and freedom of expression, cannot be confused with these techniques. The act of provoking disinformation affronts and disturbs the Democratic Rule of Law, while the principle of freedom of expression and freedom of propaganda is the corollary of the regime itself and its purpose is to protect it against any threats. The right to freedom of expression cannot be exercised as a tool that threatens the democratic regime itself, when its role is precisely to protect it.

The fairness of the electoral process and universal and equal suffrage by secret ballot depends on the internal legal and political security that ensures the free expression of the will of voters in accordance with Article 25 (b) of the International Covenant on Civil and Political Rights, at the disposal of : "Every citizen shall have the right and the possibility, without any of the forms of discrimination mentioned in Article 2 and without unfounded restrictions: (b) to vote and to be elected in periodic, authentic elections by universal and equal suffrage and by secret ballot, that guarantee the manifestation of the will of the voters ".

There are several techniques that tend to lead to online misinformation in order to manipulate public opinion. In addition to being user-made, they can be based on algorithms; advertising oriented; facilitated by technology[14].

To highlight, according to the practical code of misinformation of the European Union "the notion of "Disinformation" does not include misleading advertising, reporting errors, satire and parody, or clearly identified partisan news and commentary,

14 See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling Online Misinformation: A European Strategy, Brussels, 26.4.2018 COM (2018) 236 final, p. 6. Available in:https://ec.europa.eu/transparency/regdoc/rep/1/2018/PT/COM-2018-236-F1-PT-MAIN-PART-1.PDF, (last time accessed 12/27/2019).

and is without prejudice to binding legal obligations, self-regulatory advertising codes, and standards regarding misleading advertising"[15].

2.4. Perpetrated by users

When dealing with the activity of users, they are those characterized as end consumers of the services provided by social networks. Users share fake news and play that role in spreading misinformation by adopting a habitual practice of not checking its accuracy.

False news tends to spread in manner viral. In France, a fake news platform has been found to generate over 11 million interactions per month - five times more than reputable news brands. However, "in most cases, in France and Italy, fake news agencies do not generate as much interaction as established news brands"[16].

2.5. Based on Algorithm

Algorithms used for the purpose of generating online misinformation are prioritization-based tools when displaying business-driven information from the online platform and by adopting ways that focus on personalized, sensational, attention-grabbing content that will be shared by related users. Consequently, algorithms increase polarization and strengthen the effects of misinformation[17].

However, it is important to note how networks work and how these generated links may or may not have propagation potential.

15 EU Code of Practice on Disinformation, Preamble, available in: https://ec.europa.eu/digital-single-market/en/news/code- practice-disinformation (last time accessed 12/17/2019).
16 Measuring the reach of 'false news' and online misinformation in Europe, Reuters Institute https://reutersinstitute.politics.ox.ac.uk/our-research/measuring-reach-fake-news-and-onlinedisinformation- Europe (last time accessed 12/17/2019).
17 See Communication from the Commission to the European Parliament, Tackling Online Misinformation: A European Strategy, *ob.cit.*, p.6.

The notion of network itself reflects a characteristic of complexity. Regarding the latter, it should be noted that "Most systems do not work in a simple linear fashion"[18], that is, they work with nonlinear mathematical models. Thus, even identifiable behaviors of individual entities are insufficient to predict the evolution of the whole, and these systems are usually described in terms of probability. This complexity that assumes a mathematical modeling is known as "Network Science"[19].

For this, it is necessary to understand the dynamics of a complex network in the occurrence of an evolution, because the links are not distributed equally (randomly, in terms of mathematics), and are not organized in an orderly manner, presenting three main characteristics: 1) *small world networks*; 2) *scale-free networks* and; 3) *promote viral spread*[20]:

1) *Small world networks*: According to the "Watts-Strogatz Model" (WATTS & STROGATZ, 1998), what happens is that these networks are grouped into small densely connected subnets (clusters). It's necessary only a reduced number of connections to connect two links within the network. Reference is made to the idea of psychologist Stanley Milgram who, in the 1960s, demonstrated that any two individuals were just a few degrees apart (on average, six people would already be sufficient to establish a link between the two randomly chosen persons);

2) *Scale-free networks*: Their topology does not follow a linear scale and the number of links follows a power law distribution, unlike a normal distribution (Gaussian or "Bell curve"). The "Barabási – Albert Model" consists of connecting two links detected by chance through a path of "big links" or hubs, which concentrate a large number of links. Barabási makes a comparison of the US highway network (as a random network) where major cities are linked by the same number of highways (would be correlated to a Bell curve); to the air transport network that has hubs, which corresponds

18 David Byrne, *Complexity Theory and Social Sciences, An Introduction*, London, New York, Routledge, 1998, p.19.
19 Benjamim Loveluck, *Networks, Freedoms, and Control: A Political Genealogy of the Internet*, Petrópolis, RJ, Vozes, 2018, p. 198.
20 *Ibid*., p. 199.

to dense traffic (correlated to a power law distribution). These complex networks are those formed by the physical internet network, web hyperlinks, scientific literature citation networks, and some social networks;

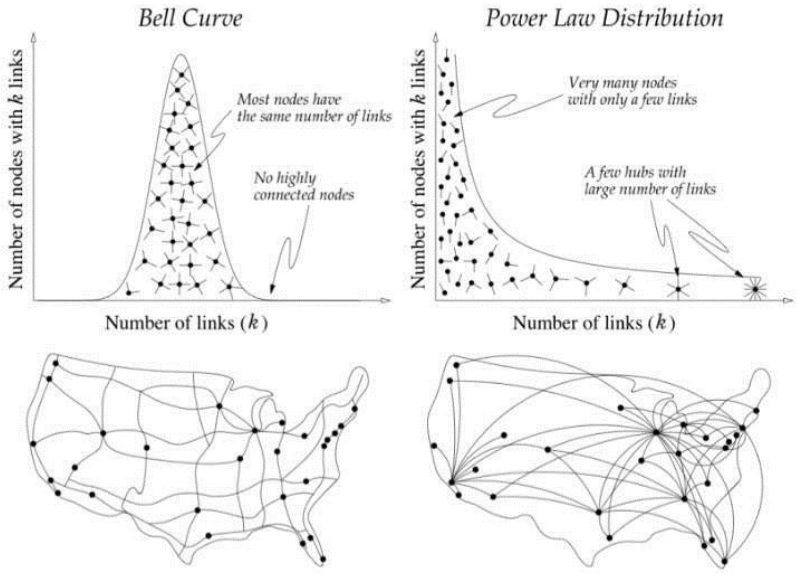


Figure 1: Random network and non-scaled network[21]

3) *Promote viral spread*: What happens is that within non-scaled networks, hubs promote infections in a sufficient number of people for the spread and circulation of the "epidemic". The form of the network that works in a distribution of a power law is enough to guarantee the spread and persistence of infections, which facilitates the diffusion process, that is, it depends on its architecture and not on the nature of the content in circulation.

This whole structure facilitates the phenomenon of social contagion in complex networks, which has the power to potentially bring about political and social changes

21 Albert-László, Linked, *The New Science of Networks*, Cambridge, MA, Perseus, 2002, p. 71.

and consequences in a given society or even in a global society by promoting viral spread.

We can also conclude that if viral spread depends on the infection of a sufficient number of people to promote the spread and circulation of the epidemic, this can be added to the tactic offered by the botnet tool, which exponentially increases the potentiality of the attack.

The centrality of hubs is a facilitator of the spread of infection and a generator of "epidemics", and its finding in complex networks allows to associate with the phenomena of social contagion on a large scale and may even raise adherence movements in political campaigns[22].

2.6. Advertisement oriented

This is a model based on digital advertising based on sensational and viral content. Through algorithmic decision making, agency-operated networks ensure real-time ad serving, facilitating the manipulation of the emotional part of users who are subject to misinformation.

The content may be sensational, but its viral spread is much more due to the network architecture when used in a distribution of a power law.

2.7. Facilitated by technology

Through automated services (referred to as "bots") they artificially extend the spread of misinformation. These mechanics can be facilitated by mock profiles (fake accounts) where no real user profiles are present, and which can be orchestrated on a large scale (referred to as "troll factory").

22 Benjamim Loveluck, *ob.cit.*, p. 203.

The new technology used by botnet attackers is an infected computers function in an automatic way to trigger performance without attackers immediate involvement. This kind of attack uses a control at a distance through the infected computer and botnet malware for the attackers[23].

It is important to know that botnet has a life cycle of five steps: initial infection, secondary infection, connection, malicious command and control, update and maintenance (Feily et al., 2009). The creation of a botnet starts from already known vulnerabilities on a victim system[24].

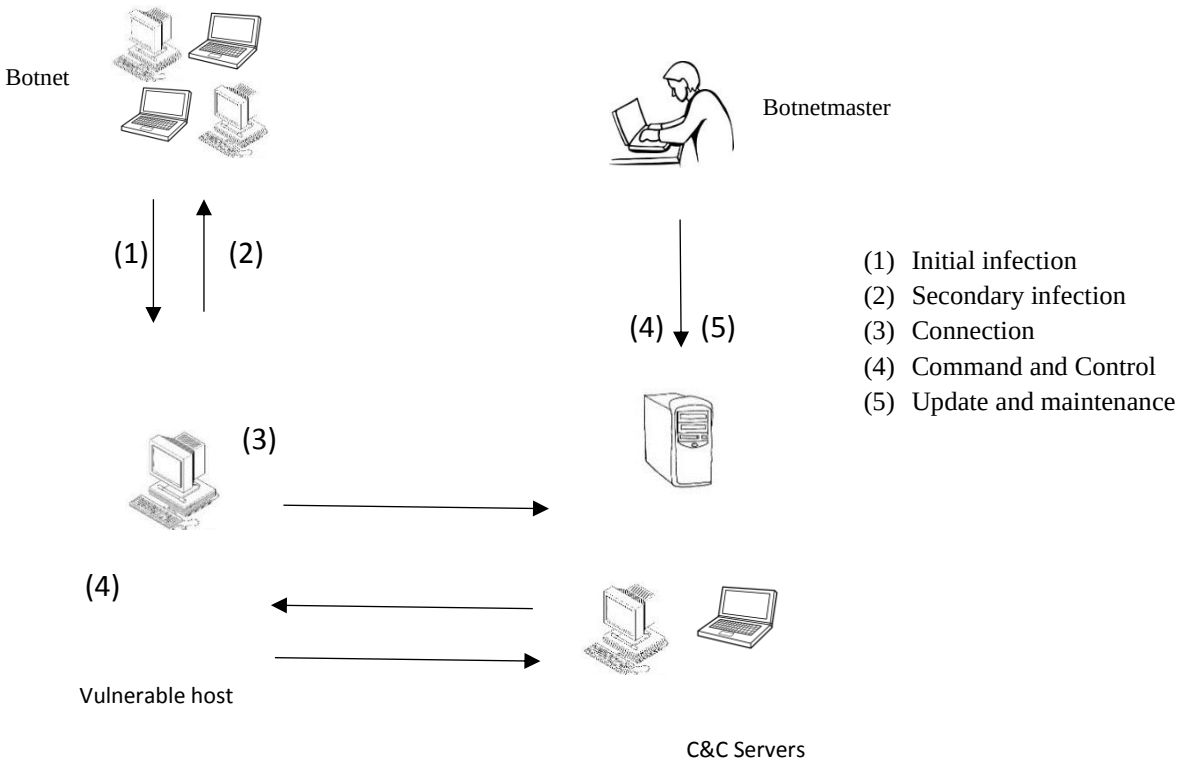


Figure 2: A "Typical Botnet Life-Cycle"[25]

23 Kishor Sarkar, *Cyber Security Botnet Attacks: Procedures and Methods*, Sarkar publication, 2018, p.12.
24 *Ibid.*, p. 16.
25 Maryam Feily; Alireza Shahrestani; Sureswaran Ramadass, *A Survey of Botnet and Botnet Detection, Impact Researsh Team*, Universiti Sains Malaysia (USM), 2009, p.269.

(1) *Initial infection*: This is a critical phase, when the Botmaster tries to exploit a known computer operating system's vulnerability to infect the user's machine[26]. During this phase, the attacker uses the scanning techniques for any known vulnerabilities, and infects victim machines through different exploitation methods. The spreading mechanism includes several infection strategies already used in worms, viruses and social engineering[27].

(2) *Secondary injection*: This phase starts by executing the dropper script code in the infected machine, by downloading the Bot binary from a specific Internet server using a File Transfer Protocol (FTP), HTTP, or Peer-to-Peer (P2P), and then setting up a newer Bot code on the victim's machine. The infected hosts execute a script known as shell-code. "The shell-code fetches the image of the actual bot binary from the specific location via FTP, HTTP, or P2P". The infected machine turns into a zombie (Bot)[28]. The bot application starts automatically each time when the zombie is rebooted[29].

(3) *Connection:* A new bot establishes a command and control (C&C) channel to communicate with the control server. "Upon the establishment of C&C channel, the zombie becomes a part of attacker's botnet army"[30]. Bots, remotely, controlled by a bot master, can conduct various malicious activities such as exploiting other machines, commencing DDoS attacks, and so on[31].

(4) *Command and Control:* The C&C channel is a kind of network protocol to communicate between a bot and a server controlled by an attacker. Moreover, the commands received through C&C channel can be

26 *Ibid.*
27 Kishor Sarkar, *ob.cit.*, p. 16.
28 Feily et al., *ob.cit.*, p. 269.
29 Kishor Sarkar, *ob.cit.*, p.16.
30 Feily et al., *ob.cit.*, p. 269.
31 Kishor Sarkar, *ob.cit.*, p.16

executed autonomously and automatically without the end-user's consent[32]. "The botmaster uses the C&C channel to disseminate commands to his bot army. Bot programs receive and execute commands sent by botmaster. The C&C channel enables the botmaster to remotely control the action of large number of bots to conduct various illicit activities"[33].

(5) *Update and maintenance*: The Botmaster may to add a new function to enhance the Botnets future attacks or to improve the evasion methods. The IP address of a new C&C server can be updated to keep it working and thus then prevent it from being blocked due to the evolution of Botnet detection techniques. "This process is called server migration and it is very useful for botmasters to keep their botnet alive"[34].

32 *Ibid.*, p.13.
33 Feily et al., *ob.cit.*, p. 269.
34 *Ibid.*

3. THE MANIPULATION OF PUBLIC OPINION IN THE CONTEXT OF FOREIGN POLICY

The use of social networks as a means of manipulating the formation of public opinion in the context of a foreign state must be viewed from the perspective of public international law.

Acts of espionage or cyber exploitation are usual forms of interference in the domestic politics of a foreign state. They are recognized as cyber actions that fall below the level of force use or non-kinetic activities. The purpose of cyber exploitation is to unauthorized access to information without affecting system functionality in order to gain clandestine advantage, so that the user does not notice any changes to the system or network. Unauthorized access to computers is made by tools called trapdoors or sniffers that are particularly useful for conducting such operations[35].

Cyber espionage, recognized as a form of cyber exploitation, presupposes the confidentiality of the IT system or the control of foreign intelligence services, and is aimed at gaining some advantage in accordance with secret interests. The interest of controlling the public opinion of a foreign state through the use of cyber exploitation tools can be considered as IO (information operations), which is the use of information technology to achieve government goals[36].

According to the Tallinn Manual I, State liability arising from an act of cyber espionage is not a matter of international law, exceptionally in the case of violation of specific international prohibitions as in the case of diplomatic communications[37]. These international bans are urged to understand acts that tend to provoke domestic state intervention, as it is not in the sole interest of collecting information from an adversary.

35 Marco Roscini, *Cyber Operations and the Use of Force in International Law*, United Kingdom, Oxford University Press, 2014, p. 17.
36 Torsten Stein;Thilo Marauhn, *Völkerrechtliche Aspekte von Informationsoperationen*, Zaö RV 2000, 1, p. 1. Available at: https://beck-online.beck.de/Bcid/Y-300-Z-ZAOERV-B-2000-S-1-N-1 (last time accessed 03/28/2019).
37 Tallinn Manual I, Rule 6 (a).

It should be remembered, however, that traditional espionage alone can be prosecuted under the national law of the adversary state affected, but under due process of law and under the protection of the International Law of the Human Person[38].

3.1. "Hybrid Threats"

"Hybrid threats" consist of activities designed to undermine a country's democratic values and fundamental freedoms by exploiting its vulnerabilities. To this end, disinformation campaigns use the media in order to control political narratives[39] for the manipulation of public opinion.

It is the obligation of a state not to intervene directly or indirectly in domestic matters of a foreign state. According to the Declaration on Enhancing the Effectiveness of the Principle of Abstention of Threat or Use of Force in International Relations, "States are required not to intervene directly or indirectly, for any reason, in the internal or external affairs of any other State"; as well as, it is the duty of states "to abstain from their relations of armed, political, economic or any other form of coercion against the political independence or territorial integrity of any state"; and "the inalienable right of every state to choose its political, economic, social and cultural system without interference from any other state" and the "inalienable right of every state to choose its economic, social and cultural political system without interference from any other state"[40].

Regardless of the active subject who uses these forms of online manipulation, these are acts that hinder the free expression of the will of a collective of people. Any result that occurs in this political context is due to a vice of will to the detriment of its free expression given the intention of misleading an entire national electorate. These

38 John F. Murphy, *Cyber War and International Law: Does the International Legal Process Threat to U.S. Vital Interests?* International Law Studies, 89 Int'l L. Stud. 309, 2013, p. 17. Available at: www.westlaw.com (last time accessed 10/16/2018).
39 Ana Maria Guerra Martins, *The Contemporary Challenges to European Union External Action*, Coimbra, Almedina, 2018, p. 407.
40 UN General Assembly, 42 Session Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Force in International Relations, 18 November 1987 (A /42/766), ANNEX, p. 288. Available at: https://undocs.org/sp/A/RES/42/22 (last time accessed 09/15/2019).

techniques have an incisive power to manipulate public opinion and if external influence is proven, they also violate the principle of nonintervention, political independence and the right to internal self-determination.

The right to internal self-determination referred to is the right to the political, social, economic and cultural development of the people within their own existing state[41].

Cyber operations aimed at achieving the objectives of internal affairs of another state, such as the manipulation of political elections, are acts that violate national sovereignty, subject to the principle of non-state intervention. Even if such an act is considered below the level of 'use of force' provided for in the UN Convention, according to the International Court of Justice, intervention is considered as a 'manifestation of a policy of force' which in the past, "Gave rise to the most serious abuses" and emphasizes that it has no place in international law[42].

Thus, it should be emphasized that a state cannot use technological vulnerabilities to generate internal crises and hinder its free political, economic and administrative development. Given this framework of destabilization of national security and defense, as well as to ensure the maintenance of the law and order, the responsibility of the States is due[43].

Moreover, according to the Universal Declaration on Information and Democracy, which establishes democratic guarantees in the global space of communication and information, with regard to the right to information, "having reliable information is

41 See Vienna Declaration and Program of Action, World Conference on Human Rights, Vienna, 14-25 June 1993, p. 3: "All peoples have the right to self-determination. By virtue of this right, they freely choose their political status and freely pursue their economic, social and cultural development". Available:https://www.oas.org/dil/port/1993%20Declaration%20and%20Program%20of%20Action%20adopted%20by%20Conference% 20World% 20of% 20Vienne% 20About% 20Human% 20in% 20June% 20of% 201 993.pdf (last time accessed 5/17/2019).
42 ICJ, International Court of Justice, Corfu Channel (United Kingdom v. Albania), Merits, Judgment, 9 April 1949, ICJ Reports 1949, p. 35. Available at: https://www.icj-cij.org/files/case-related/1/001-19490409-JUD-01-00-BI.pdf, (last time accessed 7/20/2019).
43 Ana Maria Guerra, *ob. cit.*, p. 407.

essential for exercise freedom of opinion, so that other human rights and all democratic practices are respected, including deliberation, elections, decision-making and accountability. The integrity of the democratic process is compromised when the information that may influence it is manipulated. (...) A commitment to the free pursuit of truth, the accuracy of the facts and the principle of "doing no harm" is necessary to preserve the integrity of the information. Disseminating misleading or incorrect information or covering up information that should be disclosed may impair people's ability to understand what is happening in their environment and the development of their skills"[44].

44 Universal Declaration on Information and Democracy promoted by Reporters Without Borders (RSF). Available at: https://rsf.org/es/el-espacio-global-de-la-comunicacion-y-la-informacion-un-bien-comun-de-humanidad (last time accessed 12/27/2019).

4. FINAL CONSIDERATIONS

Through this multidisciplinary report, it was possible to understand the techniques used in the use of social networks in order to manipulate public opinion. By understanding the forms of technological control in the use of botnets and the vulnerabilities presented that guarantee this intrusion, it is possible to analyze that there are harmful effects for which justice cannot abstain.

The very complexity characterized in social networks, in which phenomena use nonlinear mathematical models, which cause an evolution without direct correspondence to the behaviors of individual entities but described in terms of probability. A study that requires a specialty focused on "Network Science". The cause of the viral spread linked to the architecture of non-scaled networks, which looks more like the air transport network, mainly because the centrality of hubs, which works in a distribution of a power law, generating “epidemics”, assume a potential large-scale social contagion effect and may even lead to movements of adherence to political campaigns.

All this is taken into account when there is a concern to keep the democratic regime out of external threats. In accordance with the norms and principles of international law, the State has a duty not to intervene in the internal affairs of other States.

The manipulation of public opinion is also a matter of domestic state policy, when various internal interests linked to political parties and social movements are at stake. For this, some legal analyzes and notes were taken that take into account rights and freedoms, the optional use of these rights for personalities of the political public, and the abuse of these rights, among other forms of civil and constitutional provision.

It has been seen that manipulation of public opinion can pervade the internal interests of state political parties for an external threat of the national sovereignty. However, when it comes to information at home, care must be taken with the principles surrounding freedom of expression in order to ensure the Democratic Rule of Law. In contrast to this principle is online misinformation, which undermines the structural system of a society by endangering the protection of trust and the free will of voters in a democratic state.

Both, internally and externally, there is legal support for fundamental rights that ensure the Democratic Rule of Law. To this end, the abuse of law as a cause of civil liability is highlighted, as are the ways of ensuring the maintenance of competition and pluralism of information services, as well as the principle of equal opportunities and the treatment of various candidatures in election campaigns. In the context of state foreign policy, the State must protect itself against hybrid threats, and compliance with the principle of non-state intervention and the right to internal self-determination gain special relevance in this regard.

THE MOBILITY PROBLEM IN ORGANIZATIONS

MARCO REIS [1]

1 Master student in Information Security and Cyberspace Law in the University of Lisbon,IST and Lisbon Law School and Naval School of Portugal, 2019/2021.

ABSTRACT

Since the early days of digital technology adoption that Organizations have been concerned with protecting their assets and information through physical and logical barriers, meant to prevent unauthorized accesses. These barriers were used to create a perimeter separating what is outside from the internal network. This concept was particularly successful at a time when most of the Organization's users were sitting inside the perimeter, and everyone else was outside.

However, current times have presented severe new challenges to the classic model. Generalized internet access, smartphones and Cloud services have enabled users to go mobile without losing computational capacity or connectivity. Critical services are offered from remote locations. Devices move off and on-premises seamlessly. It's all happening very fast, and there's little that can be done to prevent this without hampering business agility and progress. The perimeter, as we knew it, doesn't exist anymore, and the internal network is really wherever the users or assets happen to be.

My aim with this Paper is to analyze a few possible ways Organizations can broaden and/or complement their traditional perimeter protections, to better handle the new mobility challenges being faced today, and enable more adequate protection to their information, users and assets, wherever they may be.

Keywords: Technology; *Organizations; Networks and IT systems; Security and safety; Perimeter (new).*

1.INTRODUCTION

"Thank you for coming.
We're going to make some history together today."

Steve Jobs introducing the first iPhone on Jan. 9, 2007

This is where it all started. Technology was finally sufficiently advanced to allow for an affordable device that offered, right in the palm of your hand, most of what computers were capable of. And cameras. And portable music players. And everything else developers could come up with trough the revolutionary app ecosystem.

Steve Jobs, the visionary that he was, recognized what this meant: mobility was about to move to the forefront of what technology was all about, and he was more than prepared to take the lead in a race that would shake up the industry, and leave most competitors either severely behind or in the dust[1] altogether.

1 (Hankin, 2019)

Figure 1 - Crowd recording a live event with their smartphones

The smartphone revolution[2] changed how people interacted with each other, consumed media, and used the internet. But it also changed **where** people did all these things.

2 (Molla, 2017)

2.PROBLEM STATEMENT

"By 2020, over half of the employees will work remotely, but we still have not figured everything out to make this work"

Amir Salihefendic, CEO, Doist - The State of Remote Work in 2018

Since starting to adopt technology long ago, Organizations have designed their Networks and IT systems with a Fort mentality. This typically means creating a perimeter, a set of barriers separating what is out from what is in, trying as much as possible to prevent any unwanted crossing of those barriers.

For a long time, this was very effective. Network and Systems were only accessible on- premises, and all the threats were kept out. Building a strong Fort was all that was needed.

Gradually, the slow but steady advance of technology started presenting additional challenges. The rise of the internet meant that a channel had to be created to interact with the outside from within. Such proposition proved impossible to resist, as there was simply too much value to be had from using the internet.

The solutions still seemed simple though. Content filtering started to be performed on the internet access, to try and prevent anything bad from coming in, or anything valuable from being sent out. Existing firewalls were improved so that more complex decisions could be made on what was allowed to cross the perimeter. But the truth of the matter was now evident: decisions were no long absolute but conditional. Organizations would have to start compensating by building and multiplying defense strategies, layering them together. Defense-in-depth[3] became a requirement.

3 (NIST, n.d.)

But not everything was bad. People still had to come to the office to access Organization resources. They still had the perimeter. Well, most of the time at least. Home internet access and Laptops became common, and suddenly it made sense that those devices should be allowed to work on company systems from the outside. The technology could support it, as Virtual Private Networks[4] (VPN's) could be used to extend the Network to the user location. They just had to be sure the anti-viruses were up to par on the endpoints.

And what about the Organizations they work with? Why shouldn't their most important partners share their network? It was just so convenient. No Organization operated alone anymore. Lower costs and higher agility and interoperability were there for the taking, at the cost of just a few more holes in the perimeter wall. They probably deployed Intrusion Prevention Systems[5] (IPS's) or some other now traditional perimeter defense commodities, just in case.

But then came the smartphones. Wi-Fi technology was now sufficiently developed as well. It was fast, it was reliable, and it was starting to appear everywhere. Not just in offices but at home, in shops and restaurants, hotels and shopping malls, airports and even airplanes. People started getting used to being online and connected all the time. They needed tools that they could use everywhere, and permanent access to the information they required.

Cloud services[6], a broader concept that also happens to enable internet-wide service, was the means through which all this could be achieved. And today it is already one of, if not the biggest business in technology. Because it is ideally poised to meet rising needs: the star sales lead needs it's critical business app while on the way to the next client meeting; the head of marketing needs a common platform to share files with the ad agency while waiting for his next flight; the finance controller is late and needs to connect to his scheduled monthly report meeting from his Uber to work. Everyone

4 (NIST, n.d.)
5 (NIST, n.d.)
6 (NIST, n.d.)

needs to do something, right now, no matter where from. That’s just the way things are done this day and age.

It's safe to say that the strategy needs to change.

3. CURRENT TRENDS

"Longevity in this business is about being able to reinvent yourself or invent the future"

Satya Nadella, CEO at Microsoft

Most historical companies in the information security space have recognized that their business model needs to change if they are to remain relevant at offering customers adequate means of protection, without hampering the ever-growing mobile workforce. And today a mobile workforce doesn't even necessarily mean that the employees work from home – although that trend is rapidly becoming the norm in many business models[7]. It may just mean that the employee has a smartphone and/or a laptop, and uses it to do additional work, planned or just because he can. After all, interacting with colleagues, customers or business partners can now be done at convenience.

On top of this, many new security companies have identified opportunities to disrupt the traditional players in this operating space, by offering more adequate and adjusted protection solutions to the mobile-first era, often leveraging cloud services and the as-a-service[8] model, that fit very well with internet focused strategies.

In most of these cases, the basic principles are the same: to replace the "border control" style approach with the idea that security must enforced where the users and information happen to be. And that trust must be earned. In other words, a "0-trust" model[9] approach where identity must be proven securely, and right of access dependent on pre-decided conditions.

These ideas are part of the fabric of Digital Transformation[10], which is a hot topic in today's world. Everyone recognizes the need for companies to adjust to these huge

7 (Buffer.com, 2019)
8 (Watts & Raza, 2019)
9 (Microsoft, 2019)
10 (Boulton, 2019)

changes brought on by very mobile and tech-savvy workforces and customer bases. Demands for flexibility, speed and service make time scarce to appropriately apply and enforce security, so it becomes critical to have the right strategy[11]. It must be adaptable to a much broader mix of use cases, and compatible with many different supporting infrastructure options, both internal and external.

After all, that transformation is very rarely immediate and sudden, which would have enormous costs and difficulties in migrating legacy systems, and systems with complex integrations and interfaces, all at once. On most medium and large companies that were already in operation this last decade, the most common scenario is a phased approach[12], where existing systems are gradually replaced with mobile-friendly and direct-to-cloud alternatives, or moved from on-premises to the cloud using "lift-and-shift" or other approaches[13], which doesn't really solve the legacy problem, but at least keeps companies moving in the right direction during a transition period that may take many years[14].

This naturally also applies to systems enforcing security. One can even make the case that changes to these systems need to be planned first, so that applications and data can be protected effectively once moved off-premises. If this move happens while you are still clinging to the appliances sitting in your data center, you're already too late.

11 (IBM, 2015)
12 (Kralj, 2017)
13 (Google Cloud, 2019)
14 (Ross, 2018)

4. THE NEW PERIMETER

"We can leverage new identity standards to fill the gaps left by the disappearance of the traditional perimeter as we know it... the value now lies in using identity as the new perimeter."

John Hawke, Senior Director of Business Strategy at CA Technologies

So, what remains unchanged with all these transformations happening, after abandoning your single, privately controlled infrastructure in favor of a hybrid or full cloud model?

Your users are still your users. And the company information is still your own.

Given the now public nature of access, Organizations just need to make sure that information is sufficiently protected at rest and in transit, and that identity management is performed at a level that offers adequate reliability and resilience. When you put it like this, it sounds simple. Because the nature of the problem is, in fact, easy to understand: everything is the same, but in different surroundings – both at the source of access, and at the destination.

Protecting information in transit usually means applying security to a significative number of different flows, like information being provided to and by stakeholders. E.g.: customers, suppliers, business partners, government entities; information uploaded or downloaded by employees; or interfaced systems exchanging information, either on-premises, in the cloud, or between both.

Doing the same for information at rest means protecting it while it is stored, be it in databases, disk storage, file sharing services, or user devices. Performing adequate identity management will be the way to make sure that only the intended and allowed

systems and users will be able to access and use the information during those stages, all the way through the information lifecycle up until it's secure deletion.

If Organizations make sure these protections are in place, then it shouldn't make a difference where systems and people physically are, and consequently the dependency on the perimeter for enforcing security is removed. Decision makers can start transitioning their businesses to a flexible model that is better prepared to serve their customers and will also make employees happier and more productive.

All this can be done without jeopardizing security. In fact, it can even possibly be increased in the process, because changes this transformational don't happen often at Organizations. It is usually the case that most on-premises systems and networks have been in place for a long time and don't have the ideal level of security in their design or implementation and may even be outdated due to lack of maintenance or support.

The most common scenario is that Organizations will have started with a baseline of network and core systems long ago, and have since spent their time adding new systems, building new features, gradually expanding their server and network base. Most replacements are only made out of necessity: either the requirements have changed and the current system is deemed obsolete or replaced; or the contract for a particular solution has reached its conclusion and the opportunity is taken to renew or replace the existing solution. This makes it so IT landscapes are much like the tree rings inside a tree: they are generally a product of how long Organizations have been in operation and are made up of different sections that have been put in place gradually over time. And because technology (and particularly security in technology) changed a lot over time, the "older rings" generally become liabilities.

Organizations can seize this opportunity and, with the right strategy[15] and architecture design, become much better prepared to deal with the new challenges of the present times.

15 (Brunswick & Olson, 2018)

It’s important to consider that enforcing security always comes at a cost. It may require extra investment, added complexity, reduced usability, or all of the above. This means that the user experience will probably be impacted when you increase your security posture. This may place you at odds with the initial intent of catering to your user base by enabling mobile access in the first place. That’s why it is so important, as is always the case when talking about security, to include communication and awareness initiatives in the project plan. People need to know what benefits they will get with the transformation initiatives, so that they will understand how adhere to the security requirements that come with them, and (ideally) even be glad to do so.

Designing the right processes, and choosing the right technology to support them, can mean the difference between successful projects and failed ones. That’s why an attempt to propose technical solutions to general problems must also be conceptual in nature.

In the context of this paper, a few types of solutions will be presented that may help Organizations achieve the recommended protection levels for mobile-first approaches. But, in reality, each Organization should begin its transformation journey with a deep understanding of the needs they must meet, the challenges to overcome, the characteristics of their business and people, and even their budget. And only then define the technological landscape that represents the best possible fit.

This being said, there are many types of solutions available in the market that aim to address the challenges presented in this paper. There are far too many of them to refer to individually, so the approach will be to try and refer a few of the more common and successful strategies that can be considered by all types of Organizations looking to address these same issues. And then offer examples of related tools that are available in the market with significant market penetration and success.

5. SECURING IDENTITY AND DEVICES

"Given a choice between dancing pigs and security,
users will pick dancing pigs every time."

Edward Felten, Deputy U.S. Chief Technology Officer

Enforcing identity security will always impact the owner of the identity, which in most cases will mean a person that will either be an employee or customer. Sure, there are other cases, but they can all be handled as specific sub-sets to which the same underlying principles apply: the process of authentication must be strong and reliable, with a complete identity management process in place; the source must be secure and compliant with company policies; and usage should be within pre-approved parameters and scope.

We further establish these vectors with the following definitions:

- **Strong Authentication** is defined as method of proving identity that depends on verified proof of at least 2 of 3 factors: something the user knows (e.g. password); something the user has (e.g. his smartphone); and something the user is (e.g. biometrics).

- **Reliable Authentication** refers to the level of reliability and resilience inherent to the process of authentication and the tools involved, so that they can't be subverted. This may be assessed through testing the implemented processes and technical solutions for design flaws and vulnerabilities.

- **Identity Management** is the process through which the company manages its users at the three critical user lifecycle stages: provisioning, update and removal. The process should be auditable, synchronized with all companies' systems, and highly resilient to human mistakes (e.g. forgetting to decommission an employee's user after he leaves the company).

- **Device and User Security** is the level of protection offered to users and the devices they use to connect to company assets and access company information;
- **Acceptable Use** means a way to associate roles with identity, so that actions can specifically be allowed or disallowed depending on role. Successful actions should also be dependent on meeting sets of security criteria (e.g. if a user accesses a system while in Portugal in one minute, and coming from China the other, then something is wrong and the action should be blocked; if a user is human but is performing actions that only a computer could perform, then something is wrong and the action should be blocked; etc.).

The basic premise is that if Organizations can adhere to these concepts without either requiring the user to be on-premises or forcing him to use a VPN to connect to the internal network, then access can safely be granted from a roaming context.

Presented here are a few of the more relevant operating spaces, as defined by Gartner[16], where current technologies can be instrumental in helping Organizations to achieve these goals.

5.1 User Identity and Access Management

Gartner Definition: *"Identity and access management (IAM) (…) addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet increasingly rigorous compliance requirements. IAM is a crucial undertaking for any enterprise. It is increasingly business-aligned, and it requires business skills, not just technical expertise. Enterprises that develop mature IAM capabilities can reduce their identity management costs and, more importantly, become significantly more agile in supporting new business initiatives."*

16 (Gartner, n.d.)

Solutions in this market seek to address the challenges related with authentication and identity management, usually providing the following set of base capabilities, among other more specific differentiators:

- **Strong, Multi-Factor Authentication:** secure authentication capabilities for your users from company devices or other sources, independent of location;
- **Single Sign-On:** improve usability by providing a single authentication step that proves identity, removing the need for additional authentication processes for corporate applications;
- **User Management, including Authorization, Application Access and Lifecycle:** manage complete identity process from a single central point, from initial provisioning to final decommission, including all role management and application access;

Examples:

- **OKTA**

https://www.okta.com/

"Complete access management platform for your workforce and customers, securing all your critical resources from cloud to ground"

- **PING IDENTITY**

https://www.pingidentity.com/en.html

"Intelligent access for customers, employees and partners so they can securely connect to cloud, mobile, SaaS and on-premises applications and APIs"

- **ONE LOGIN**

https://www.onelogin.com/

"OneLogin delivers the unparalleled protection and control you need with the simplicity users demand, so you can get back to business"

5.2 Endpoint Protection

Gartner Definition: *"An endpoint protection platform (EPP) is a solution deployed on endpoint devices to prevent file-based malware attacks, detect malicious*

activity, and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts. (…) Desirable EPP solutions are primarily cloud-managed, allowing the continuous monitoring and collection of activity data, along with the ability to take remote remediation actions, whether the endpoint is on the corporate network or outside of the office. (…)".

These solutions address some of the challenges related with securing the user and company devices. They represent an evolution from the traditional anti-virus solutions from the past, with the newer players in this space designed from the ground up to be particularly adjusted to a mobile focused user base and their devices, usually combining the following set of characteristics:

- **Cloud Based Protection:** security services are offered globally, independent of user and device location;
- **Next Generation Anti-Virus:** solutions don't only detect malware based on known signatures, but use a combination of specialized capabilities to detect and prevent unwanted behavior from unknown threats;
- **Flexible Agent:** endpoint agents are compatible with most relevant types of company assets, like smartphones, laptops, desktops, servers, and even virtual machines;

Examples:

- **CROWDSTRIKE**

https://www.crowdstrike.com/

"Cloud-native endpoint protection platform built to stop breaches."

- **CARBON BLACK**

https://www.carbonblack.com/

"In today's mobile world, endpoints are the new perimeter (…) Carbon Black prevents more threats, gives you actionable insights, and helps you operate faster and more effectively"

- **SENTINEL ONE**

https://www.sentinelone.com/

"The end of antivirus. Our autonomous AI Platform defeats every attack, every second of every day. The number one antivirus replacement."

5.3 Secure Web Gateway

Gartner Definition: *"(…) A secure Web gateway (SWG) is a solution that filters unwanted software/malware from user-initiated Web/Internet traffic and enforces corporate and regulatory policy compliance. These gateways must, at a minimum, include URL filtering, malicious-code detection and filtering, and application controls for popular Web-based applications, such as instant messaging (IM) and Skype. Native or integrated data leak prevention is also increasingly included."*

Far surpassing traditional proxies, the major players today can offer much more than just caching and content filtering for PC's on local internet access. Among the most popular capabilities are:

- **Content Filtering:** URL Filtering, Application Controls and Malware Detection over SSL Inspected Traffic;
- **Hybrid or Full Cloud Configurations:** in order to offer protection and policy enforcement to devices outside of the local network, local appliances can be combined with cloud services on some offerings to offer a Hybrid approach. Strictly cloud based solutions are also available;
- **Tamper-proof agents:** solutions will run agents on smartphones or laptops that will force internet traffic on those devices to be sent to the SWG from any location, acting like an always-on VPN client with added functionalities. Those agents will typically offer tamper-proof configurations so that, if defined by Organizational policy, protection and compliance can be enforced at all times;
- **Data Exfiltration Protection:** restrictions on service consumption (e.g. file sharing apps blocked), disallowed actions (e.g. block uploads) and several types of data loss prevention capabilities help Organizations protect against unwanted exfiltration of data.

Here are some of the major players today:

- **ZSCALER**

https://www.zscaler.com

"With complete cloud security stack (...) you can deliver airtight security to all users, on or off network"

- **SYMANTEC BLUECOAT**

https://www.symantec.com/products/secure-web-gateway

"An advanced network security service that enforces consistent internet security and compliance policies for all users regardless of location or device."

- **FORCEPOINT**

https://www.forcepoint.com/product/web-security

"Next-generation web security for tomorrow's global workforce"

6. CONCLUSION

"It is not the strongest of the species that survives, nor the most intelligent that survives. It is the one that is the most adaptable to change"

Charles Darwin, English Naturalist and Geologist

Most developed countries today are in a race to launch 5G[17]. This will offer higher internet speeds and lower latency for mobile devices, further increasing their capabilities and pushing even further the boundaries of what can be done remotely. The office, as we know it today, may soon become a thing of the past.

Organizations should embrace mobility as a key business critical capability, and re-design their security strategy accordingly. They will get a safer and more productive workforce, better protected assets and information, and a reinforced operational model that will be better adjusted to a new world that is already a reality.

As now commonly stated: *The perimeter is dead. Long live the (new) perimeter*.

17 (Cheng, 2019)

BIBLIOGRAPHY

Boulton, C. (2019, May 31). *What is digital transformation? A necessary disruption*. Retrieved from cio.com: https://www.cio.com/article/3211428/what-is-digital-transformation-a-necessary-disruption.html

Brunswick, D., & Olson, J. (2018, September 27). *The Common-Sense Guide to IT Systems Modernization.* Retrieved from cleo.com: https://www.cleo.com/sites/default/files/2018-10/it-systems-modernization-guide.pdf

Buffer.com. (2019). *State of Remote Work Report*. Retrieved from https://buffer.com/state-of-remote-work-2019

Cheng, R. (2019, 10 27). *The 5G wireless revolution, explained*. Retrieved from cnet.com: https://www.cnet.com/news/the-5g-wireless-revolution-explained/

Deloitte. (2019). *Tech Trends 2019 - Beyond the Digital Frontier.* Retrieved from deloitte.com: https://www2.deloitte.com/content/dam/Deloitte/br/Documents/technology/DI_TechTrends2019.pdf

Gartner. (n.d.). *Gartner About Page*. Retrieved from gartner.com: https://www.gartner.com/en/about

Google Cloud. (2019, November). *CIO's Guide to Application Migration*. Retrieved from services.google.com: https://services.google.com/fh/files/misc/cio_guide_to_application_migraton.pdf

Hankin, A. (2019, 06 25). *Three Companies the iPhone Killed*. Retrieved from investopedia.com: https://www.investopedia.com/news/three-companies-iphone-killed/

IBM. (2015). *Increasing Agility and Speed to Drive Business Growth.* Retrieved from ibm.com: https://www.ibm.com/downloads/cas/PLOBJO7W

Kralj, M. (2017, November 1). *Cloud Migration: Finding your path to value with the cloud*. Retrieved from accenture.com: https://www.accenture.com/us-en/blogs/blog-miha-kralj-phased-approach-to-cloud-adoption

Microsoft. (2019). *Zero Trust Maturity Model.* Retrieved from microsoft.com: https://go.microsoft.com/fwlink/p/?linkid=2109181

Molla, R. (2017, 06 26). *How Apple's iPhone changed the world: 10 years in 10 charts*. Retrieved from vox.com: https://www.vox.com/2017/6/26/15821652/iphone-apple-10-year-anniversary-launch-mobile-stats-smart-phone-steve-jobs

NIST. (n.d.). *NIST Computer Security Resource Center - Glossary - Cloud Computing*. Retrieved from nist.gov: https://csrc.nist.gov/glossary/term/cloud-computing

NIST. (n.d.). *NIST Computer Security Resource Center - Glossary - Defense In Depth*. Retrieved from nist.gov: https://csrc.nist.gov/glossary/term/defense_in_depth

NIST. (n.d.). *NIST Computer Security Resource Center - Glossary - IPS*. Retrieved from nist.gov: https://csrc.nist.gov/glossary/term/intrusion-prevention-system

NIST. (n.d.). *NIST Computer Security Resource Center - Glossary - VPN*. Retrieved from nist.gov: https://csrc.nist.gov/glossary/term/VPN

Ross, J. (2018, April 5). *Digital Is About Speed — But It Takes a Long Time*. Retrieved from mit.edu: https://sloanreview.mit.edu/article/digital-is-about-speed-but-it-takes-a-long-time/

Watts, S., & Raza, M. (2019, June 15). *SaaS vs PaaS vs IaaS: What's the Difference and How to Choose*. Retrieved from bmc.com: https://blogs.bmc.com/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/?print=pdf

THE CHALLENGES OF SMARTPHONE FORENSICS IN SUB-SAHARAN AFRICA

RICARDO J.G.N. DOS SANTOS [1]

1 Master Student of Information Security and Cyber Law Instituto Superior Técnico – Portugal
Contact: rjgndossantos@gmail.com.

ABSTRACT

The modernization of public and private services in sub-Saharan Africa has been challenging to the region, due to a massive adoption of information and communication technologies, such as mobile-centric solutions connected or not to overseas Cloud computing services, putting an overwhelming pressure on security forces and the judicial apparatus of these countries to deal accordingly with new criminal phenomena of cyberspace. As a result, building sustainable Smartphone Forensics capacity presents itself as the way forward, despite budgetary, legal and even political constraints that ultimately determine its effectiveness, in parallel with the obligation to comply with cyberspace security standards, some of them already in force, as a consequence of international treaties that bilaterally or regionally bind many of these countries.

Keywords: *Sub-Saharan Africa; Cyber security; Cybercrime; Law Enforcement; Smartphone; Forensics; Challenges*

1.FOREWORD

The information age has been a more constant presence in our daily lives, due to not only the speed and technological innovation it brings, but also with the almost near extinction of some activities that used to be part of modern societies, such as postal services, landline telephones, neighbourhood groceries and corner stores.

Not to mention services, both in private and government sectors, that have been replaced by e-mail, VoIP, e-commerce and many more, which, due to the immaterial nature of cyberspace, require security measures to be adjusted to this new reality.

Paving the way for the Fourth Industrial Revolution of real time, lower costs, modularity, and large-scale integration done by Cloud Computing[1], IoT[2], and other paradigms, the information age presents itself as a kind of unblocked expanding snowball, throughout cyberspace, giving way to new forms of social, economic and even political way of living, especially in countries with a considerable digitization rate of public and government services.

Sub-Saharan Africa is not apart from this global trend, precisely because of the great transformations it has witnessed over the last decade. Nevertheless, it remains a big unknown in the information age, due to great challenges it still has to deal with organized crime, terrorism and other vicious behaviours, which are increasing today in cyberspace.

In addition, sub-Saharan Africa has yet to create technological infrastructure and capacity to absorb the potential of information age technologies. Even having

1 See: https://www.ibm.com/cloud/learn/cloud-computing (accessed on 27/12/2019)
2 See: https://www.iotforall.com/what-is-iot-simple-explanation/ (accessed on 27/12/2019)

considerable digital mobile network coverage, this part of the African continent still has a low level of consumption of state-of-the-art computer services and solutions compared to other regions of the world, which in part defines the general characteristics of criminal behaviour there.

However, due to the phenomenon of globalization, knowledge exchange with global criminal networks is already a reality, which puts pressure on sub-Saharan African governments to respond diligently to this global scale threat by strengthening police cooperation mechanisms, both within Interpol and the regional economic blocs, with Europol being of particular note.

Thus, bearing in mind the particular characteristics of cybercrime in sub-Saharan Africa, building sustainable Smartphone Forensics capacity presents itself as the way forward, despite budgetary, legal and even political constraints that ultimately determine its effectiveness, in parallel with the obligation to comply with cyberspace security standards, some of them already in force, as a consequence of international treaties that bilaterally or regionally bind many of these countries.

2. GLOBAL OVERVIEW OF ORGANIZED INTERNET CRIME

A recent report [1] points out data as the key element on the security agenda of organizations and citizens as well, by strengthening data protection legislation, to tackle attacks such as ransomware. In effect, despite experiencing a decrease in global occurrences, ransomware has become more selective and focused on people and organizations.

For instance, in 2019 most visible attacks were against local governments, specifically in the United States. This trend had commenced earlier in 2018, when an attack paralysed the city of Atlanta for several weeks and only proved to be the tip of the iceberg. After that, more than half a dozen cities and public services across the US fell victim to ransomware, on a near-monthly basis, and in the most extreme situations, a state of emergency was declared[3].

Although spotted only in the US, these ransomware attacks have underscored the need for strengthening law enforcement international cooperation.

Source: Serianu, 2018 [2]

Figure 2 – A global overview of ransomware attacks in 2018

3 See: https://www.cpomagazine.com/cyber-security/top-10-ransomware-stories-of-2019/ (accessed on 27/12/2019)

Indeed, in January 2019, authorities from several US agencies, along with police and prosecutors from Belgium and Ukraine, as part of a Joint Investigation Teams assisted by Eurojust, seized the *xDedic marketplace* in an operation also supported by the German Federal Criminal Police Office and Europol, exposing more than EUR 60 million in fraud[4].

Another clear and growing concern are Supply Chain Attacks [1], i.e. the use of compromised third parties as a means to infiltrate networks affecting suppliers of third-party software or hardware, but also other business services.

For instance, large companies, which may have a multitude of third-party suppliers, some with a high degree of connectivity, bringing each one its own risk. Such risks are similarly incurred when a larger company acquires a smaller company which may have lower cyber security maturity[5].

Moreover, many companies are becoming increasingly reliant on third-party services such as the cloud, where malicious software, even signed with legitimate digital certificates, can appear to be an authentic software update[6]. These attacks have also affected large parts of business, resulting in costly production stoppages in Europe[7] and the USA.

Amongst them [1] are Distributed Denial of Service (DDoS) attacks, whose purpose resembles the previous ones, since the main element that drives them is extortion, particularly crypto currency. Besides, DDoS attacks are often linked to so-called hacktivism[8], which presents itself one of the greatest security challenges of democratic countries, since it acts, most of the time, as a faceless force with no explicit

4 See: https://www.europol.europa.eu/newsroom/news/xdedic-marketplace-shut-down-in-international-operation (accessed on 27/12/2019)
5 See: https://www.theguardian.com/business/2019/jul/09/marriott-fined-over-gdpr-breach-ico (accessed on 27/12/2019)
6 See: https://securelist.com/operation-shadowhammer/89992/ (accessed on 27/12/2019)
7 See: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/lockergoga-ransomware-family-used-in-targeted-attacks/ (accessed on 27/12/2019)
8 See: https://www.checkpoint.com/definitions/what-is-hacktivism/(accessed on 27/12/2019)

ideological alignment, but often linked to covert acts of sovereign states or hostile organizations.

It poses challenges on law enforcement agencies to gather digital evidence to determine the root cause of these criminal acts before they can be presented in Court, especially because of the massive use of sophisticated encryption and obfuscation methods.

Likewise, in spite of a noted decline[9], DDoS attacks remain one of the most prominent threats reported by the private sector [1], superseded only by *phishing* and other social engineering attacks, resulting in the interruption of online bank services, creating more of a public impact rather than direct financial damage.

Such attacks typically originate from low-capability actors, who can still leverage easily accessible DDoS-for-hire services[10] that exploit booters/ stressers. While most attacks can be successfully mitigated, emerging DDoS techniques, which may be significantly harder to defend against, such as memcached[11] amplified attacks remain a concern for the financial sector.

In 2018[12] and 2019[13], respectively, two large DDoS attacks using this technique were spotted. Notice that social networks and other content providers commonly use a memcached approach, which is likely to expose their servers to UDP based reflection attacks[14].

9 See: https://gbhackers.com/ddos-for-hire-service/(accessed on 27/12/2019)
10 See: https://www.csoonline.com/article/3180246/hire-a-ddos-service-to-take-down-your-enemies.html (accessed on 27/12/2019)
11 See: https://www.tutorialspoint.com/memcached/index.htm(accessed on 27/12/2019)
12 See: https://thehackernews.com/2018/03/biggest-ddos-attack-github.html(accessed on 27/12/2019)
13 See: https://www.imperva.com/blog/imperva-blocks-our-largest-ddos-l7-brute-force-attack-ever-peaking-at-292000-rps/(accessed on 27/12/2019)
14 See: https://www.imperva.com/learn/application-security/udp-flood/ (accessed on 27/12/2019)

In turn [1], there was also an accentuation of the recording of criminal sexual phenomena such as child pornography[15], which now is boosting[16], and related explicit content material[17], largely due to the popularization of smartphone use by minors, but also, raising additional concerns about the Darknet[18]. In effect, it is in these prolific web places where smuggling-related transactions[19], narcotics, scamming money and terrorism[20] have found a safe haven

In a word, Darknet remains the key online propeller for trade in an extensive range of criminal products and services and a priority threat for law enforcement [1], even with coordinated law enforcement reaction, combined with extensive DDoS counter-attacks that have generated distrust in the Tor[21] environment.

Even so, it seems existing market varieties and customer-base on Tor are making a full migration to new platforms, which have increased the number of single-vendor shops and smaller fragmented markets on Tor, including those catering for specific languages, supported by strong encrypted communication applications, likely to support illicit trade[22].

A final word on enabling factors of the above mentioned organized crime phenomena on the Internet [1]. The first is the wide array of Online Service Providers (OSP) exploited by terrorist groups, which presents a significant challenge to any disruption efforts, since they are exploiting emerging platforms for their online communication and distribution strategies associated, in some cases, to hacktivism.

15 See: https://www.europol.europa.eu/newsroom/news/14-arrests-in-takedown-of-massive-child-sexual-abuse-platform (accessed on 27/12/2019)
16 See: https://globalnews.ca/news/4153203/swedish-man-guilty-online-rape-convictions-upgraded/ (accessed on 27/12/2019)
17 See: https://www.nationalcrimeagency.gov.uk/news/five-years-in-jail-and-worldwide-travel-ban-for-british-teacher-who-wanted-to-abuse-young-filipino-children (accessed on 27/12/2019)
18 See: https://www.darkowl.com/what-is-the-darknet(accessed on 27/12/2019)
19 See: https://www.nytimes.com/2019/06/11/technology/online-dark-web-drug-markets.html (accessed on 27/12/2019)
20 See: https://www.counterextremism.com/press/extremist-content-online-isis-utilizes-dark-web-remain-online (accessed on 27/12/2019)
21 See: https://www.torproject.org/ (accessed on 27/12/2019)
22 See: https://www.theguardian.com/world/2019/may/03/german-police-close-down-dark-web-marketplace (accessed on 27/12/2019)

These terrorist attacks can rapidly turn viral before any OSP or law enforcement can react, exemplified here not only with the remarkable cases in Iraq and Syria[23], but also in New Zealand[24] and Nigeria[25], which are certainly not isolated events.

A second enabling factor is *phishing*[26], which remains an important tool in the cybercriminals arsenal, inducing victims to withdraw money[27] from their bank accounts. The big news currently is the inclusion of crypto currencies to propel these criminal acts, giving rise to *cyber mules*, which, like their narcotics counterparts, are used to traffic crypto currency.

In 2018, over the course of three months, law enforcement and private sector partners from over 30 countries participated in the fourth European Money Mule Action (EMMA) which ended up with the tracking of over 1.500 *cyber mules* and 140 *cyber mule's* organisers, resulting in 168 arrests. Financial sector participants reported 26,376 fraudulent *cyber mules'* transactions, preventing an estimated loss of over EUR 36 million. Two interesting related cases were reported in the United Kingdom[28] and the Netherlands[29].

23 See: https://www.project-syndicate.org/commentary/america-islamic-state-information-war-by-anne-marie-slaughter-and-asha-c-castleberry-2019-09?barrier=accesspaylog (accessed on 27/12/2019)
24 See: https://www.nytimes.com/spotlight/christchurch-attack-new-zealand (accessed on 27/12/2019)
25 See: https://www.ict.org.il/UserFiles/Cyber%20Report%203.pdf
26 See: https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html (accessed on 27/12/2019)
27 See: https://as.com/diarioas/2014/12/16/english/1418723895_163685.html (accessed on 27/12/2019)
28 See: https://www.europol.europa.eu/newsroom/news/6-arrested-in-uk-and-netherlands-in-%E2%82%AC24-million-cryptocurrency-theft (accessed on 02/01/2020)
29 See: https://financefeeds.com/europol-dutch-and-luxembourg-authorities-clamp-down-on-crypto-mixing-service-bestmixer-io/ (accessed on 02/01/2020)

3. A BRIEF ON DIGITAL FORENSICS

Digital forensics, or computer forensics, comprises the application of scientific investigatory techniques to digital crimes and attacks. Jason Jordaan, principal forensic scientist at DFIRLABS[30], has a good definition for that,[31] naming it as the identification, preservation, examination, and analysis of digital evidence, using a scientifically accepted and validated process and the ultimate presentation of that evidence in a court of law to answer some legal question.

In current global cyber security status, this poses a major challenge especially for countries that are cyclically lacking human, financial or material capacities, especially if dealing, for example, with Cloud Computing [3], [24].

Besides [4], the nature of the cases in which digital evidence is involved is generally borderless and the offense happens in a split second.

Thus, the findings derived from electronic evidence must therefore follow a standard set of guidelines to ensure it is admissible not only in a specific country's court of law, but also in the international criminal justice system. For that reason, understanding electronic evidence is a challenging process due to the fact the data can be scattered in several physical locations, sometimes across countries or jurisdictional borders effortlessly and in a matter of seconds.

And, of course, being highly volatile, the data are easily altered, overwritten, damaged or destroyed by the single stroke of a key. Therefore, the data can be copied without degradation, so that the lifespan of electronic evidence, unlike any other discipline of forensic evidence, is short before it is rendered useless.

30 See: https://www.dfirlabs.com/ (accessed on 02/01/2020)
31 See: https://www.csoonline.com/article/3334396/what-is-digital-forensics-and-how-to-land-a-job-in-this-hot-field.html (accessed on 02/01/2020)

An example of this is a smartphone. After five years, it may not be able to switch on or function properly. Based on these facts, therefore, electronic evidence must be processed and handled with due care.

On the other hand [4], the criteria for the admissibility of electronic evidence may differ from jurisdiction to jurisdiction. Any forensic investigator should always consider, as a basis for starting a case, the following (table 1):

Table 1 - General Criteria for the Admissibility of Electronic Evidence

General Criteria for the Admissibility of Electronic Evidence	
Authenticity	The evidence must establish facts in a way that cannot be disputed and be representative of its original state.
Completeness	The analysis of, or any opinion based on, the evidence must tell the whole history and not be tailored to match a more favourable or desired perspective.
Reliability	There must be nothing about the way in which the evidence was collected and subsequently handled that may cast doubt on its authenticity or veracity.
Convincing	The evidence must be persuasive as to the facts it represents, and must be able to convince the stakeholder of the truth in court.
Proportionality	The methods used to gather evidence must be fair and proportionate to the interests of the justice: the prejudice (i.e. level of intrusion or coercion) caused to the rights of any party should not outweigh the probative value of the evidence (i.e. its value as proof).

Source: Interpol, 2019 [4]

To achieve this purpose [4], a seven-step model is recommended for managing a case (figure 2). Moreover [4], prior to conducting a case, the Digital Forensics Laboratory personnel must ensure it is following and complying with relevant legislation.

One last remark to alert that following standardized guidelines is paramount, but innovations are also encouraged, especially in low-income countries [5]. For this reason, sometimes it is valid relying on low-cost forensics[32], setting up a functional and credible forensic workstation at the cost of a few hundred dollars [6] to create admissible evidence for legal proceedings in Court.

Figure 3 – A recommended model for collecting any electronic evidence
Source: Interpol, 2019 [4]

3.1 Smartphone Forensics

Of particular interest is the process of conducting Digital Forensics examination (figure 3) and analysis on mobile devices[33], where two levels of data acquisition are considered [4], respectively, physical data and logical data acquisitions.

While physical data acquisition includes all raw data, a logical copy typically only includes an allocated subset of those data. Physical data acquisition, at whole disk level, copies all data contained on the disk, including the partition scheme, partitioned area, and not partitioned area. Logical data acquisition on disk level copies only a logical partitioned area. The availability of forensic software tools for mobile devices is considerably different from that of personal computers [7]. While personal computers may differ from mobile devices from a hardware and software perspective, their functionality has become increasingly similar. Although the majority of mobile device

32 See: https://www.digitalforensicshub.com/index.html (accessed on 06/01/2020)
33 Desktops, Servers and other *fixed* devices

operating systems are open source[34], feature phone Operating Systems are typically closed.

This means that interpreting their associated file system and structure become difficult, not to mention a myriad of file system and structure permutations which may create significant challenges for mobile forensic tool manufacturers and forensic investigators.

The types of software available for mobile device examination include commercial and open source forensic tools [7], as well as non-forensic tools intended for device management, testing, and diagnostics. Forensic tools are typically designed to acquire data from the internal memory of handsets and Universal Integrated Circuit Cards[35] without altering their content and to calculate integrity hashes for the acquired data. Whilst non-forensic tools may allow unrestricted two-way flow of information and omit data integrity hash functions. Consequently, mobile device investigators typically assemble a collection of both forensic and non-forensic tools for their toolkit.

It should be noted, however [8], that the proliferation of smartphones on the consumer market caused a high demand for forensic examination of the devices. This could not be met by existing computer forensics techniques.

Figure 4 – Electronic data acquisition process in smartphone forensics
Source: Interpol, 2019 [4]

To remain competitive, original equipment manufacturers frequently change mobile phone form factors, operating system file structures, data storage, services,

34 Android Operating System. Further details here: https://www.android.com/ (accessed on 06/01/2020)
35 See: https://techterms.com/definition/uicc (accessed on 06/01/2020)

peripherals, and even pin connectors and cables. As a result, forensic examiners must use different forensic processes if compared to usual computer forensics.

A crucial aspect in smartphone forensics is the device isolation [7], since many mobile devices offer the user the ability to perform either a remote lock or remote wipe by simply sending a text message command[36] to the mobile device. Additional reasons for disabling network connectivity include incoming data[37] that may modify the current state of the data stored on the mobile device.

Outgoing data may also be undesirable as the current GPS location may be delivered to an advisory providing the geographic location of the forensic examiner. Therefore, forensic examiners need to be aware and take precautions when securing mobile devices mitigating the chance of data modification. Isolating the mobile device from other devices used for data synchronization is also important [7] to keep new data from contaminating the existing data.

If the device is found in a cradle or connected with a personal computer, pulling the plug from the back of the personal computer eliminates data transfer or synchronization overwrites, thus capturing data should be done by a qualified digital forensics professional. Isolating a mobile device from all radio networks[38] is also important [7] to keep new traffic, such as SMS messages, from overwriting existing data.

Besides, the risk of overwriting potential evidence, the question may arise whether data received on the mobile device after seizure is within the scope of the original authority granted.

36 For example, a text message.
37 For example, calls or text messages.
38 For example, Wi-Fi, Cellular and Bluetooth.

4. BUDAPEST CONVENTION ON CYBERCRIME

Finally, a brief look at the Budapest Convention, which is a comprehensive guiding document drawn up by the Council of Europe[39] in November 2001 and open for signature by its member and non-member States which have participated in its elaboration and for accession by other non-member States.

The Budapest Convention resembles a harmonious triangle whose vertices unfold three broad lines of action [9], respectively: (i) criminal conduct; (ii) tools and procedures and (iii) international cooperation. It is considered one of the most relevant documents on cybercrime and digital forensics.

With regard to criminal conduct, its scope covers illegal access; illegal interception; data interference; system interference; misuse of devices; fraud and forgery; child pornography; and intellectual property offences. About tools and procedures, it covers expedited preservation; search and seizure; production order; and interception of computer data.

Finally, with regard to international cooperation, the Budapest Convention sets out the terms of mutual assistance in criminal matters, covering the areas of extradition, spontaneous information, expedited preservation, and many more.

By March 2018 [9], the Budapest Convention was already explicitly or implicitly present in the cyber laws of 130 countries, of which 57 had already ratified and transposed them into domestic law. The vast majority are OECD countries.

39See: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (accessed on 06/01/2020)

5. SUB-SAHARAN AFRICA: OPPORTUNITIES, GEOPOLITICS AND MODERNIZATION

Located below the Sahel,[40] this poorly industrialized part of the African continent, which consists of 46 countries and in 2018 had 1.038.627.178 inhabitants, is now according to UNDP[41] experiencing steady economic growth and macroeconomic stability.

This is also accompanied by a flourishing private investment not only in the agricultural, telecommunications, finance, retail trade, housing and construction sectors, but also in new technologies, which are spreading rapidly across the continent, leading to a considerable progress in the areas of information and communication.

This scenario contrasts with the primary and extractive characteristics of the early stages of its economy, based on raw material exports, along with residual high and medium-income tourism.

This optimism is also shared by the World Bank [10], which points out Sub-Saharan Africa as the region that has been implementing the highest number of reforms every year since 2012. Consequently, the private sector is feeling the impact of these improvements, with the average time and cost to register a business, for example, declining from 59 days and 192% of per capita income in 2006 to 23 days and 40% of per capita income today.

Furthermore, the average paid-in minimum capital has fallen from 212% o to 11% of per capita income in the same period. Still according to the World Bank [10], Kenya and Rwanda are the most represented Sub-Saharan Africa countries in Doing Business 2019, due to growth in digitization, as well as business regulatory reforms. Kenya

40 See: https://www.britannica.com/place/Sahel (accessed on 06/01/2020)
41 See: https://www.africa.undp.org/content/rba/en/home/regioninfo.html (accessed on 06/01/2020)

simplified the process of providing value added tax (VAT) information by enhancing its existing online system, iTax[42].

Furthermore, in Kenya, the Ministry of Lands and Physical Planning implemented an online land rent financial management system on the eCitizen portal[43], enabling property owners to determine the amount owed in land rent, make an online payment and obtain land rates clearance certificates digitally.

On the other hand, Rwanda streamlined the process of starting a business by replacing its electronic billing machine system with new software that allows taxpayers to issue value added tax invoices.

The free software, which is provided by the office of their Revenue Authority, allows taxpayers to issue value added tax invoices from any printer, eliminating the previous requirement to purchase and set up a special billing machine[44] among other recent achievements.

The main reason for this sub-Saharan Africa awakening in the international arena seems to be the remarkable growth[45] of its middle class, which brings with it consumption habits very close to those in the most developed countries in the northern hemisphere.

They have been even often challenged by a Subaltern Globalization[46] carried across the Southern hemisphere by non-governmental organizations and international partnerships with African Diasporas in Europe and America, leading to an informed and better prepared middle class able to understand the geopolitical

42 See: https://itax.kra.go.ke/KRA-Portal/ (accessed on 06/01/2020)
43 See: https://www.ecitizen.go.ke/ (accessed on 06/01/2020)
44 See: https://www.rra.gov.rw/fileadmin/user_upload/20180328_vsdc_technical_specifications_v.4.pdf (accessed on 06/01/2020)
45 See: https://www.uhy.com/the-worlds-fastest-growing-middle-class/ (accessed on 06/01/2020)
46 See: http://www.allacademic.com/meta/p74466_index.html (accessed on 06/01/2020)

dynamics worldwide. Indeed, in the context of globalization and the current global financial crisis, new cooperation players are emerging in Africa[47].

These partners loosen financial constraints and conditionality, increase the room for manoeuvre and stimulate commodity markets, namely, substantial technology transfer and an outsourcing of production to Africa, especially with a view to accessing the North American and European markets.

The increase in product quality and production diversification suggests that territorial poles of competition are emerging, while the continent participates both in production segments that are integrated in global technical production and in cognitive processes, especially via multinational firms[48].

On the other hand, they also increase the risks of renewed indebtedness and potentially weaken the coordination of aid policies. Furthermore, Africa is now concerned with many problems that are global in scope, such as climate change, market instability, epidemiological risks, terrorism[49] and political instability[50].

Particularly important in this equation is the role of the People's Republic of China, which bets on a welfare model where the balance of countries' internal affairs is not accountable for mutual cooperation[51]. As a result, this Asian nation became not only the largest creditor in sub-Saharan Africa, but also the largest investor in Africa, often playing this friendly card in debt relief[52].

47 See: https://journals.openedition.org/poldev/138 (accessed on 06/01/2020)
48 See: https://journals.openedition.org/poldev/138 (accessed on 06/01/2020)
49 *Ibidem*
50 See: https://www.dni.gov/files/images/globalTrends/documents/GT-Africa_Democratization_ForPublishing-WithCovers.pdf (accessed on 06/01/2020)
51See:https://www.economist.com/briefing/2019/03/07/africa-is-attracting-ever-more-interest-from-powers-elsewhere (accessed on 06/01/2020)
52 See: https://beyond-ratings.com/publications/geopolitics-debt-chinafrica-relationship/(accessed on 06/01/2020)

5.1 Booming Mobile Connectivity

One of the consequences of this new positioning of Sub-Saharan Africa in the world is the expansion of information and communications technologies in a continent traditionally devoid of basic telecommunications and energy infrastructures capable of matching the information age. That is present especially in the hinterland, which created an opportunity for booming mobile connectivity, especially in countries that usually are leading their sub-regions. Indeed, Sub-Saharan Africa mobile network operators are eager today to contribute to the development of a strong information and communication technology industry. The importance of this boom is not only economic, but also, social [11].

Mobile internet connectivity brings about material increases in productivity, providing more efficient ways for consumers, workers and businesses to trade, communicate and access information. Besides and more importantly, the economic impact of mobile technology is also reflected in the industry's contribution to the global economy, which in 2017 amounted to $3.6 trillion or 4.5% of total Gross Domestic Product (GDP).

In many low and middle-income countries, this proportion is even higher – for example, in Sub-Saharan Africa it accounted for 7.1% of total GDP in 2017 [11]. In fact [12], mobile economy in Sub-Saharan Africa has been driven by various consumer needs across the region. Mobiles are not just a communication device but also the primary channel for getting online and a vital tool to access life-enhancing services.

This is particularly true in rural areas, where around half the population lives and where the provision of these services by conventional means is constrained by acute funding, skills and infrastructure gaps. Mobile network assets and services, such as APIs, IoT, mobile money and billing platforms, are enabling sustainable business models for key services across verticals in the region. The number of mobile internet subscribers in the region has quadrupled since the start of this decade; the technology is the only available platform for the majority of the population to get online.

In late 2017, there were 135 live mobile money services across the region, with 122 million active accounts, a figure which is expected to have significantly increased by 2025, when nearly 300 million people is expected to be online, the majority of them connecting via high-speed mobile broadband networks.

On the other hand [12], mobile money continues to flow rapidly across Sub-Saharan Africa. In 2017, the total value and number of mobile money transactions grew by 14.4% and 17.9% to reach $19.9 billion and 1.2 billion, respectively. Although East Africa remains the largest mobile money market, accounting for 56.4% of total users in the region, West and Central Africa have seen rapid uptake in recent years, helped by enabling regulatory policies.

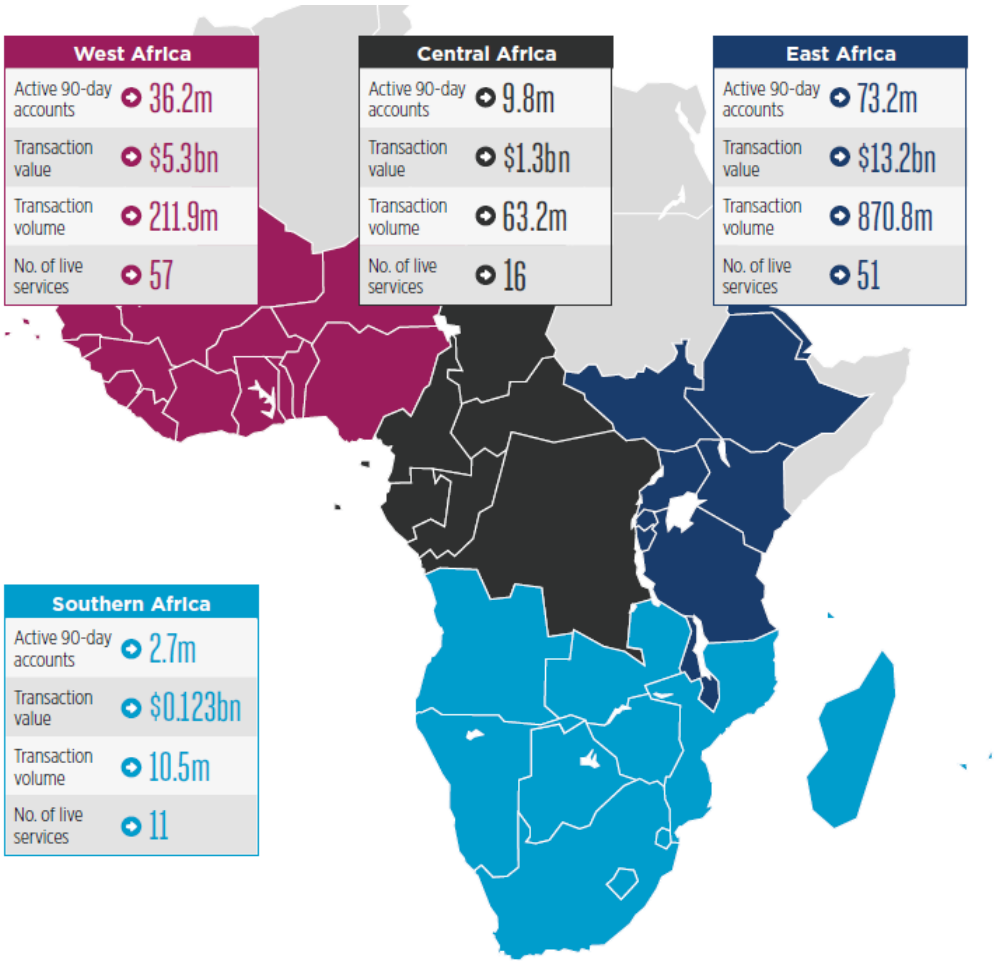
Both sub-regions have seen their share of the mobile money market double to 30.9% and 9.7%, respectively, over the five years to 2017. In addition [11] to the economic impact, mobile internet can drive material improvements in social outcomes (health, education and personal freedoms) and overall quality of life, average life evaluations and net positive emotions. In short, mobile technology has been contributing to the achievement of the UN Sustainable Development Goals.

Moreover [13], mobile internet connectivity will help overcome the traditional barriers of distance and limited access to healthcare, promoting education, innovation and job creation innovation hubs. Not to mention opportunities for established businesses to partner with start-ups and create thriving ecosystems of creativity and enterprises.

It is, ultimately, bringing the informal sector into the mainstream economy, by enabling banks and telecoms providers to reach out to previously unbanked customers with low-cost accessible services[53]. However 4G penetration remains limited, because the Sub-Saharan African mobile telecommunications market is highly dependent on 2G and 3G technologies, it limits operators' ability to monetize value-added services and

53 Note: A successful example is Kenya’s M-PESA

mobile connectivity, pushing mobile network operators to remain highly dependent on traditional voice and SMS revenues[54].



Source: GSMA, 2018 [12]

Figure 5 – Mobile money financial flow in Sub-Saharan Africa

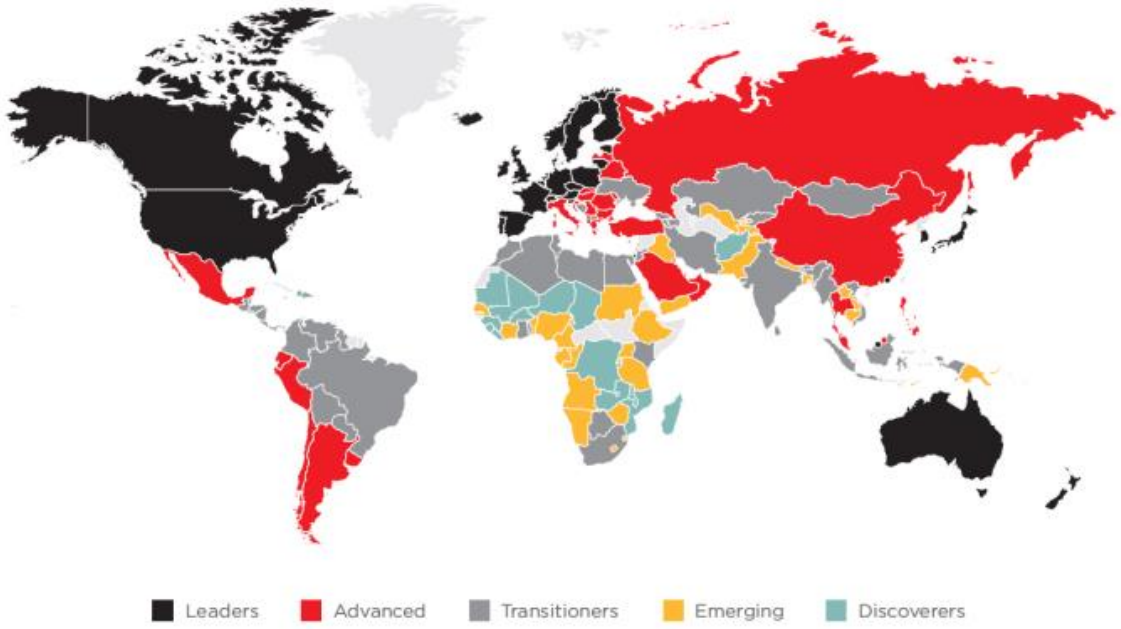
Figure 5 is taken from 2018 GSMA Intelligence report [11] which also states that Sub-Saharan countries have yet to start to reduce the gap on consumer readiness and affordability.

It means that the region will need to maintain its progress in this area while also accelerating improvements in infrastructure and the development of local content and

54 See: https://www.spglobal.com/marketintelligence/en/news-insights/blog/opportunities-and-challenges-for-african-telecommunications-industry-at-africacom-2018(accessed on 06/01/2020)

services. Although no country in Sub-Saharan Africa is in the advanced cluster of the mobile connectivity index[55], Mauritius is close to the threshold[56].

Furthermore, several other countries have been improving their performance since 2014, with four[57] joining the transitioners cluster and 10 moving from the Discoverers to the Emerging cluster. As a result, fewer than half of the countries in the region are now in the Discoverers cluster (compared to two thirds in 2014). In 2018 [14], there was a notable acceleration in network expansion in Sub-Saharan Africa, where coverage reached 70% – a considerable increase from 63% in 2017, and from 52% in 2014.



Source: GSMA, 2018 [11]

Figure 6 – Global mobile connectivity index

More than 80 million people previously unable to access 3G networks are now covered.

55 Note: The Mobile Connectivity Index measures a number of indicators, scored within a range of 0 to 100, with a higher score representing stronger performance in delivering mobile internet connectivity. For further details see: http://www.mobileconnectivityindex.com/
56 Note: In fact, Mauritius surpassed this level in 2019
57 Cape Verde, Ghana, Botswana and Kenya

Nigeria reached almost 75% coverage, whereas the Democratic Republic of the Congo reached more than 50%. Most of this expansion was driven by a programme of upgrading 2G sites, which were focused on voice and SMS services, to also support mobile internet services. The deployment of single Radio Access Network technology and U900[58] has allowed operators to roll out 3G in a more cost-efficient manner. U900 has been particularly effective by enabling the use of low-frequency spectrum bands for 3G, which is less costly than deploying in the 2100 MHz band. While the 900 MHz spectrum has historically been used for voice and SMS services, operators have been responding to the increasing adoption of internet-enabled feature phones and smartphones in the continent.

Between 2014 and 2018 [14], the penetration of smartphone connections in Sub-Saharan Africa increased from 10% to 30% of the population, with more Africans able to use their phones to access data services. It is now more viable for operators to move voice traffic to 3G by *refarming*[59] part of their 900 MHz spectrum, especially as some U900 technologies can easily be deployed through remote software upgrades and allow dynamic spectrum allocation between 3G and legacy services.

With 85% 2G coverage currently in Sub- Saharan Africa, it is expected that operators will continue to upgrade their sites over the next few years, narrowing the gap between 2G and 3G coverage. Moreover, upgrading 2G sites in remote areas will remain a challenge as the incremental costs associated with equipment, backhaul and power may not generate sufficient returns to justify the investment.

For the 150 million individuals in Sub-Saharan Africa that live in areas where there is no pre-existing mobile infrastructure[60], extending networks will remain a significant economic challenge. Given the lack of commercial sustainability in these areas, alternative solutions will be required. Still to close the gap [14] between the usage

58 See: http://www.telecomabc.com/u/umts900.html (accessed on 06/01/2020)
59 See: https://www.gsma.com/spectrum/wp-content/uploads/2017/11/10-Day-2-Session-3-How-to-Implement-Spectrum-Refarming-Shola-Sanni.pdf (accessed on 06/01/2020)
60 No 2G coverage

and drive digital inclusion. This means that mobile data needs to be affordable for even the poorest in society.

However, despite the falling cost of data, unaffordability for the poorest quintile[61] remains significantly higher than the 2% target for all regions. In Sub-Saharan Africa, the cost of 1 GB of data for the poorest quintile is almost 40% of their monthly income. In South Asia, for instance, the average affordability for that amount of data is only 1.2% of their monthly income.

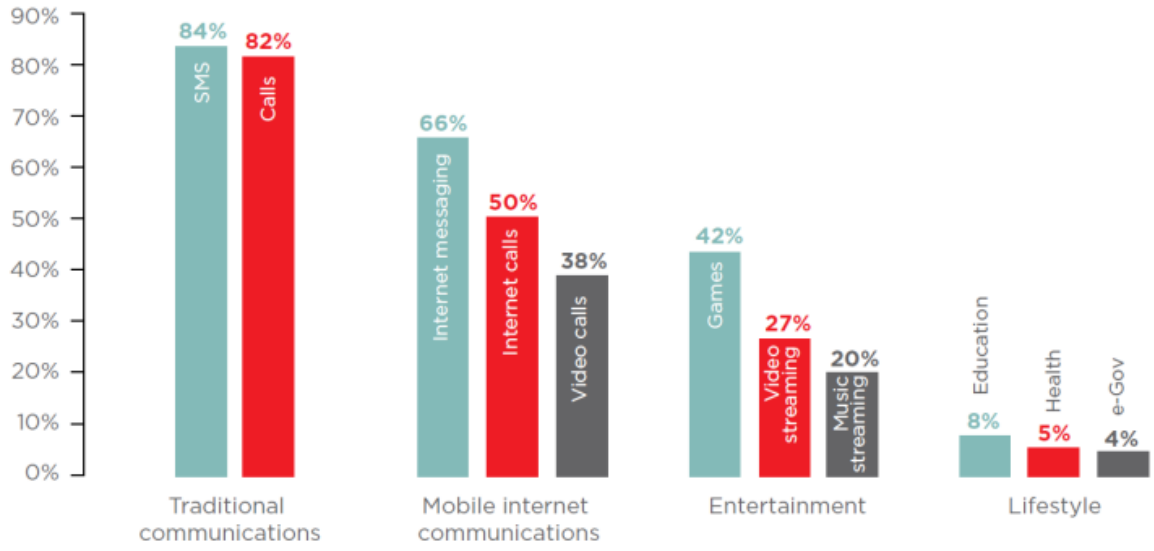
5.2 Poor 5G Prospects

Concerning to 5G coverage inception in Sub-Saharan Africa [15], it is clear that Sub-Saharan Africa has more of a demand-side than a supply-side problem for mobile broadband. This is evidenced by the significant mismatch between 4G network coverage and 4G adoptions across the region.

Over 800 million people in the region are still unconnected, 62% of which are already covered by a mobile broadband network. The reason for insufficient demand in the region is mainly socio-economic and exogenous to the telecommunications industry. And, most importantly, if the demand problem is still to be addressed, all stakeholders, especially governments, should work together to ensure that broadband usage can be optimised for consumers and businesses.

That is explained due to the fact that beyond the traditional use for making calls, many customers in developing countries use their smartphones for leisure and entertainment, especially watching free online video and playing games. As video overcomes the literacy challenge, its use will continue to grow and will increasingly account for the bulk of network traffic for most operators in the region.

61 Equivalent to 20%



Source: GSMA, 2019 [15]

In terms of regional engagement levels, sub-Saharan Africa is still at the bottom globally, but two aspects are striking [16]. The first is the exponential increase of mobile money relevance in the East African Economic Community doing business, galvanized by Kenya.

The second is the consumer profile in Sub-Saharan countries, which focus mainly on entertainment content or social networking rather than on productivity services or tools, which are also available, in contrast to the consumer profile from Europe, North America and the Far East, which is precisely the opposite.

5.3 Cyber Security Threats Landscape

In 2016 [17], a number of institutions in African countries were targeted by cyber security threats. In one particular case, the attack lasted more than 12 months – spanning from October 2015 until August 2016 - and it relied on a number of weaknesses in the organisations' information and communications technologies infrastructure and processes.

The hackers conspired with malicious insiders to install malicious keylogging[62] and remote desktop software on machines dedicated for the processing of financial transactions. The keylogging software was used to capture user keystrokes and send data (user account credentials, customer account information, email and chat messages) to an external cloud infrastructure.

Using these credentials, the attackers accessed the infected computers remotely and processed fraudulent Electronic, Mobile and ATM Funds Transfers. These attacks confirmed the vulnerability of the overall Sub-Saharan Africa networks and infrastructure. In effect, an assessment [17] conducted in various countries and inspection of network traffic in 10 different organisations across Africa determined 3 vectors, namely, BYOD[63], Insider threats, and Phishing Scams. In all organisations, traditional antivirus software could no longer match the new strains of malware targeting African organisations, such as Botnets[64], Ransomware, Spyware[65], Trojans[66] and Worms[67]. Common distribution channels included malicious files and links to malware hosting sites embedded in emails, social media sites, portable drives and BYOD devices.

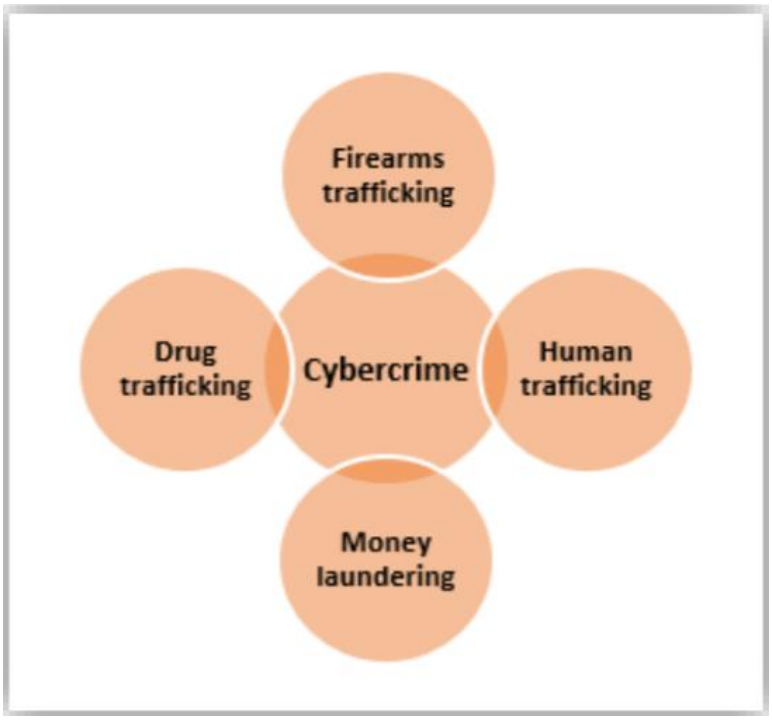
Peer to Peer (P2P)[68] connections have also been widely used for communications between infected machines and botnets. Notice that P2P connections are usually hard to detect and block at the network level using traditional methods. Thus, attackers are using this flaw to weaponise torrent software to deliver malware and enhance private communication capabilities with infected machines.

Some insights [17] revealed that Remote Access[69] software was one of the most commonly used for malicious purposes without the knowledge of the victim, along with

62 See: https://techterms.com/definition/keylogger (accessed on 06/01/2020)
63 Stands for *Bring Your Own Device*. For further details see https://www.techopedia.com/definition/29070/bring-your-own-device-byod (accessed on 06/01/2020)
64 See: https://www.techopedia.com/definition/384/botnet(accessed on 06/01/2020)
65 See: https://techterms.com/definition/spyware(accessed on 06/01/2020)
66 See: https://techterms.com/definition/trojanhorse(accessed on 06/01/2020)
67 See: https://techterms.com/definition/worm(accessed on 06/01/2020)
68 See: https://techterms.com/definition/p2p(accessed on 06/01/2020)
69 See: https://techterms.com/definition/remoteaccess (accessed on 06/01/2020)

other methods used to evade traditional antiviruses and achieve persistency. For example, the use of fileless malware,[70]which hide in locations that are hard to scan. Appendix I displays a summary of cyber security gaps in Sub-Saharan Africa in 2016. Overall [24], the nature of cybercrime cases on the continent are mostly cyber-enabled crimes, and not cybercrimes committed exclusively in cyberspace.

Cyber-enabled crimes are traditional crimes that increase the scale or reach of groups through the use of computers, computer networks, or other forms of information and communication technology.



Source: Interpol, 2019 [24]

Figure 7 – Criminal forms facilitated by cybercrime

70 See: https://us.norton.com/internetsecurity-malware-what-is-fileless-malware..html(accessed on 06/01/2020)

6. CURRENT STATUS OF SMARTPHONE FORENSICS IN SUB-SAHARAN AFRICA

The analysis of the current status of digital forensics readiness in sub-Saharan African countries can be stratified into four groups. This includes smartphone forensics, which is one of its specific branches [4], [7].

South Africa, which can also be classified as Advanced[71] at the continental level, stands out for complying with internationally recognized standards and good technological and legal practices [4]. Being totally sovereign in the area, South Africa cooperates either with the European Union, Interpol, or bilaterally with similar police institutions [18]. In effect, the South Africa Police Services has general law enforcement powers to investigate an Incident under Criminal Procedure Act 51 of 1977, which sets out the procedure to be followed by the South African Police when investigating a criminal offence, which includes cyber-related offences. In this case, different agencies work together to facilitate enforcement and compliance[72].

Second, there are the Transitioners countries, composed of Kenya, Nigeria, Rwanda, Mauritius, Ghana and Senegal, which partially comply with internationally recognized technological and legal standards and good practices [4].

Kenya, which operates with M-pesa[73], one of the world's largest mobile money transfer services [18], has made great progress in the area of smartphone forensics, especially in the training of forensic experts. It should be noted that Kenya had, in 2016, the highest number of professionals, with 1,400 cyber experts, which exceeded the

71 Note: for better understanding by the reader, a convention similar to the GSMA report [11] is used
72 See: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/south-africa (accessed on 13/02/2020)
73 Note: M-Pesa is a mobile phone-based money transfer, financing and micro financing service, very popular in Kenya, Tanzania, Afghanistan, South Africa, India, and also, in Romania and Albania.

figures from other countries in its region, who still had the disadvantage of usually not being trained or receiving *ad-hoc* training when a cyber-incident occurs[74].

But despite advances in the area of human resources and in the use of forensic technology[75], a serious conflict between civil society and the government persists after Kenya's president signed to law the contentious Computer Misuse and Cybercrimes Act[76]. This situation forced the suspension of the act and, consequently, the evaporation of the relevance of smartphone forensics for obtaining evidence to be presented in court.

Nigeria, on the other hand, had in 2016 the chilling rate of more than one out of every seven mobile devices in the country infected with mobile malware [18]. With important steps in the technological strengthening of law enforcement agencies, especially from 2015, to respond to this challenge, and the growth of a flourishing private sector in the area of digital forensics[77]. Even so, Nigeria still does not systematically comply with internationally recognized technological and legal standards and good practices [4]. However, Nigeria has given good indications of its intention to comply in the future [78].

In turn, Rwanda established a specialized Police department in charge of digital forensics and works closely with the local CSIRT[79] in case of computer security incidents [18]. That may include collaboration with local CERT[80] and Interpol to locate and identify the perpetrators. The country has achieved encouraging results[81]. The

74 See: https://www.ict.org.il/Article/2275/Cyber_threats_on_African_subjects#gsc.tab=0 (accessed on 13/02/2020)
75 See: https://www.cyberdigitalforensics.com/nairobi-digital-forensics (accessed on 13/02/2020)
76 See: https://techweez.com/2018/06/21/lsk-seeks-enjoined-case-against-cybercrimes-act/ (accessed on 13/02/2020)
77 See: http://cfinonline.org ; http://firstdigitalforensics.com.ng/our-clients.html ; https://www.premiumtimesng.com/news/more-news/205374-nigeria-police-launch-forensic-lab-abuja.html
78 See: https://www.vanguardngr.com/2017/05/cybercrimeu-s-support-nigeria-fight-fraud/ (accessed on 13/02/2020)
79 Note: CSIRT is a Computer Security Incident Response Team that is assigned the responsibility for coordinating and supporting the response to a computer security event or incident.
80 Note: CERT is a Community Emergency Response Team that deals with the evolution of malware, viruses and other cyber-attacks.
81 See: https://blog.comodo.com/comodo-news/new-rwandan-cybercrime-law-step-forward-in-african-cybersecurity/ (accessed on 13/02/2020)

government of Rwanda has also a partnership with global cyber security organization such as IMPACT[82] and other national CERT's [18]. Rwanda well deserves a case study for the effective way it has prioritized synergies[83], resources[84] and cooperation programs[85] for technological modernization with tangible results[86], a dynamic that also extends to the legal area[87].

Regarding Mauritius, its Police Force has a capable Cyber Crime Unit, which has received U.S. government training[88]. Organized hacking operations by indigenous criminal groups are very limited[89], but the extent of hacking operations conducted by external actors remains unknown[90].

Regarding Ghana, officially, there has been, until 2016, a relatively low incidence of cyber-crime in the country [18]. However, as of 2017, in line with their objective of dealing effectively with cyber-crime, the Ghana Police added another two cyber-crime units to the existing one at their headquarters in Accra [91]. Though they have not yet focussed on the root causes of cybercrime[92], which have placed Ghana at the top of the sub-Saharan African countries since 2010 [25]. Furthermore, the Ghana Police still rely on conventional crime laws relating to false pretence in the criminal Code Act 29/60 Section 131 and its associate statutes. Therefore, crimes committed under these laws are bailed offences and carry lesser punishments which cannot therefore deter the fraudsters

82 See: https://www.impactcybertrust.org/ (accessed on 22/02/2020)
83 See: https://www.africa.engineering.cmu.edu/(accessed on 06/01/2020)
84 See: https://www.maastrichtuniversity.nl/news/forensic-training-rwandan-police-officers-succesfully-completed(accessed on 06/01/2020)
85 See: https://www.interpol.int/ar/1/1/2016/Investigating-cyber-enabled-crimes-focus-of-joint-Rwandan-and-INTERPOL-exercise(accessed on 06/01/2020)
86 See: https://www.ktpress.rw/2018/06/new-forensic-lab-opened/(accessed on 06/01/2020)
87 See: https://www.rwandabar.org.rw/a-forensic-evidence-cybercrimes-electronic-evidence-and-data-protection-workshop/(accessed on 06/01/2020)
88 https://www.osac.gov/Country/Mauritius/Content/Detail/Report/e248beb4-219e-4708-a774-15f4aed12f9e
89 See: https://www.slideshare.net/curiousEngine/cybercrime-and-computer-misuse-cases-presentation ; http://www.elandsys.com/~sm/cybercrime-facebook-mauritius.html(accessed on 13/02/2020)
90 See: https://www.osac.gov/Country/Mauritius/Content/Detail/Report/e248beb4-219e-4708-a774-15f4aed12f9e
91 See: https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Cybercrime-Ghana-police-to-set-up-two-cyber-crime-units-751378 (accessed on 14/02/2020)
92 See: https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Police-Cybercrime-Unit-warns-Ghanaians-to-stop-watching-porn-with-office-computers-792082 (accessed on 14/02/2020)

from committing cyber offences [26]. This has been offset by contracting of state-of-the-art forensic investigation services in the private sector [93].

In third place are the Emerging Countries, namely Senegal, Togo, Côte d'Ivoire, Mali and Republic of Congo[94]. Despite partially complying with internationally recognized technological standards and good practices [4], their Police departments do not have clear scope and legal competences in relation to cyber-crime units. They are believed to support the fight against the most common criminal forms facilitated by cyber-crime [24]. This group of French-speaking countries has capacity-building programs in digital forensics, particularly with the European Union and Interpol[95], but also, bilaterally with France under the *Francophonie*[96].

Senegal maintains a division to investigate cyber-crimes within the Interior Ministry National Police [18], called Cell Investigations Cyber Crime Unit, which has recently been equipped with new technological means[97]. Notice that cybercrime is a relatively recent issue in Senegal's judicial system[98]. Other major stakeholders concerned include the Intelligence Agency, a specialized branch within the National Police that focuses on cyber-crime [18].

In Togo, the government maintains a division specially tasked to investigate cyber-crimes within the Information and Communication Technologies Agency that is under the Ministry of Security and Civil Protection [18]. Although the legal framework

93 See: https://e-crimebureau.com/cyber-forensics/ (accessed on 14/02/2020)
94 Also known as Congo-Brazzaville
95 See: https://www.interpol.int/en/News-and-Events/News/2019/Nigeria-and-INTERPOL-formalize-West-African-Police-Information-System-cooperation
96 See: https://www.francophonie.org
97 See: https://africabusinessagency.com/senegal-police-emploie-grands-moyens-cybersecurite/ (accessed on 14/02/2020)
98 See: https://www.snap221.info/cybercriminalite-la-justice-senegalaise-et-les-effets-pervers-dinternet/ (accessed on 14/02/2020)

has been adopted only recently in this country[99], the combined action of the judicial police and the prosecutor's office has already culminated in some cases in court[100].

In turn, Cote d'Ivoire signed a Microsoft partnership agreement for the establishment of an authorized IT Academy, which provides training to officers of the national police [18]. Despite this, national police performance is still quite limited[101] in view of the intricate ramifications of this country[102] with Internet Organized Crime [1].

Regarding Mali, this country, which has been experiencing a prolonged separatist conflict with the Tuareg community, maintains a division specially tasked to investigate cyber-crimes known as the Judicial Investigation Brigade[103], even though there are currently no specific laws governing cyber-security [18]. Indeed, only in the Criminal Code can any vague reference to cyber-crime be found[104].

For its part, Republic of the Congo maintains a unit within the National Police, tasked with investigating cyber-crimes, with all cyber security issues directly supervised by the Ministry of the Interior [18]. This unit uses an approach to repress citizens' deviant behaviours[105], a trademark of *Francophonie* countries.

Finally, the Discoverers, which are countries that do not formally have police units specialized in the combat and forensic investigation of cyber-crimes. However, they are frequently requesting outsourcing from Israel, France, USA, China, Russia, or

99 See: https://www.togofirst.com/fr/tic/0712-2164-togo-adoption-de-la-loi-sur-la-cybersecurite-et-la-lutte-contre-la-cybercriminalite (accessed on 14/02/2020)
100 See: https://lexpressiondz.com/info-en-continu/relizane-93-affaires-de-cybercriminalite-traites-en-2019-320353
101 https://www.aljazeera.com/news/africa/2014/08/cracking-down-cybercrime-ivory-coast-20148279503515697.html (accessed on 13/02/2020)
102 See: https://observers.france24.com/en/20090728-online-money-scammers-ivory-coast-fraud-crime (accessed on 13/02/2020)
103 See: http://bamada.net/cybercriminalite-au-mali-la-brigade-dinvestigation-judiciaire-demantele-un-reseau-de-fraudeurs (accessed on 13/02/2020)
104 Articles 264 and 271.
105 See: https://feministescongo.wordpress.com/tag/cybercriminalite/ (accessed on 13/02/2020)

regional[106] and global[107] companies. These countries generally do not comply with internationally recognized legal standards and good practices.[4] Capacity-building programs in digital forensics, particularly with the European Union and Interpol, are irregular or practically non-existent.

6.1 Malabo Convention Issues

In 2014, the Organization of African Unity adopted the Malabo Convention on Cyber security and Protection of Personal Data[108], which despite its breadth and relevance in the information age, has so far been ratified[109] by only 4 out of 46 sub-Saharan African countries respectively, Ghana, Guinea, Mauritius and Namibia.

In fact, a 2016 report [18] presented an overview of the 46 countries of Sub-Saharan Africa in terms of specific criminal law provisions on cybercrime and electronic evidence, showing that 11 countries seemed to have basic substantive and procedural law provisions in place[110] although implementing regulations may still be missing in some of these countries.

While 12 other countries seemed to have substantive and procedural law provisions partially in place [111], a significant part of Sub-Saharan Africa countries had neither specific legal provisions on cyber-crime nor electronic evidence in force, even

106 See: https://mybroadband.co.za/news/security/119280-interception-of-communications-in-sa-you-should-be-worried.html (accessed on 13/02/2020)
107 See: https://globalvoices.org/2016/05/16/the-government-of-mozambique-is-spying-on-its-citizens-according-to-verdade/ (accessed on 13/02/2020)
108 See: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (accessed on 06/01/2020)
109 https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf (accessed on 06/01/2020)
110 Botswana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda and Zambia
111 Benin, Gambia, Kenya, Madagascar, Morocco, Mozambique, Rwanda, South Africa and Zimbabwe

having drafted laws or amendments to existing legislation that reportedly had been prepared in at least 15 countries[112].

In some instances, bills had been presented to national parliaments. In others, the fate of draft laws is uncertain. Therefore [18], [19] the state of legislation on cybercrime and electronic evidence in Africa is not satisfactory (fig.7), since 20% of the countries seemed to have the minimum legislation in place.

Some other key findings arose as well, for example, from the strong focus on personal data protection issues, which is often confused with over criminalisation, particularly with regard to content and speech.

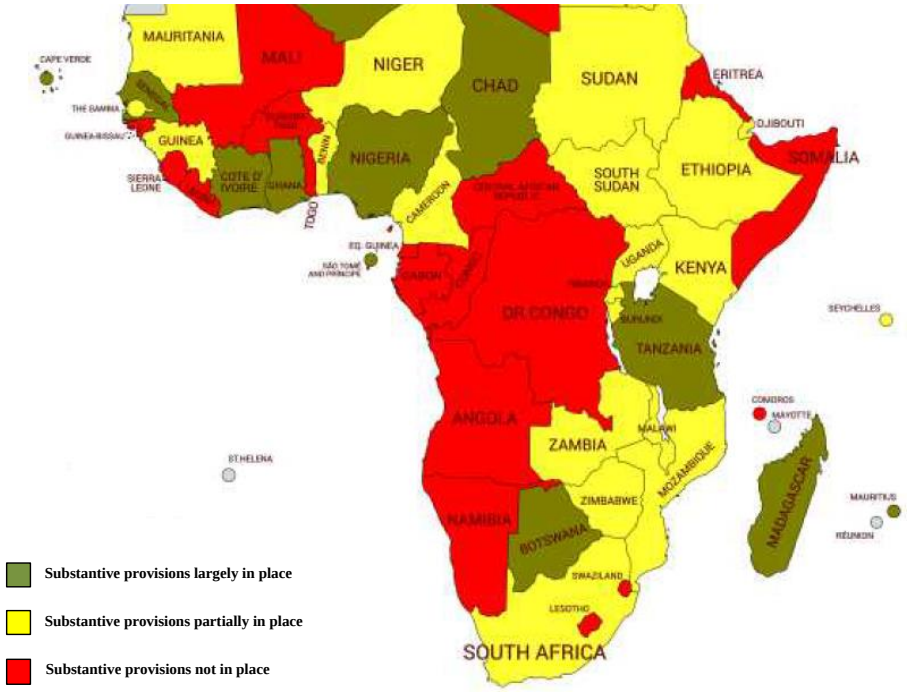
The slowness of member states in transposing the Malabo Convention into local law contrasts with the influx of foreign investment and the forward thinking of some Transitioners states, which are heavily, committed to information and communication technologies, such as Nigeria and Rwanda[113].

A comparative analysis [9] of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime suggests that Malabo is broader than the Budapest Convention in regard to electronic transactions; personal data protection and cyber security and cybercrime. Furthermore [9], the Malabo Convention unites different aspects related to information technology law, also including certain non-digital and non-criminal justice issues.

With regard to these three broad lines of action of the Budapest Convention, there is an almost complete alignment with the Malabo Convention on criminal conduct and tools and procedures. On the other hand, there is almost no alignment with respect to specific provisions and the legal basis for international cooperation in cyber-crimes and obtaining electronic evidence.

112 Burkina Faso, Djibouti, Ethiopia, Guinea, Kenya, Lesotho, Mali, Namibia, Niger, South Africa, Swaziland (e-Swatini), Togo, Tunisia, and Zimbabwe

113 https://busa.org.za/wp-content/uploads/2018/03/Public-7-Continental-Free-Trade-Agreement-Establishment-10-03-2018.pdf(accessed on 06/01/2020)



Source: Lucchetti, 2018 [9]

Figure 8 – Current status of Malabo Convention in Sub-Saharan African countries

Another point [9] that also draws attention is the high adoption rate (fig. 8) of the Budapest Convention as a reference model for the elaboration of local cyber laws, which contrasts with that of the Malabo Convention.

Source: Lucchetti, 2018 [9]

Figure 9 - Adoption rate of the Budapest Convention in Sub-Saharan Africa

6.2 Extrajudicial Surveillance

It seems that Sub-Saharan governments are more prone to *deploy sophisticated network eavesdropping tools against their citizens, kicking out any hopes of duly endorsing the* African Union Convention on Cyber Security and Personal Data Protection [114].

Supported mostly by US, French and Israeli expertise and technology [115], in most cases **spying on dissidents** [116] **living in the country and abroad is the main agenda, if not the only one, of an overwhelming part of** Sub-Saharan security forces. The situation has gotten prompt reaction from civil society[117], claiming, among others, against those restrictions.

As a result, the transposition of the Malabo Convention into local law should preserve the viability and usability of the internet as a platform for communications in Africa, in order to enhance its effectiveness as a driver of commerce, education, health, and development generally.

It should be emphasized that improving digital security is crucial to this effort, helping to expand global access to information and communications technologies. However, improving cyber security also entails protecting human rights [118].

114 See: https://www.cybersecurityintelligence.com/blog/african-states-quick-to-adopt-network-surveillance--738.html(accessed on 06/01/2020)
115 See: https://www.theafricareport.com/22841/inside-africas-increasingly-lucrative-surveillance-market/(accessed on 12/02/2020)
116 See: https://www.cybersecurityintelligence.com/blog/ethiopian-cyber-spies-left-clues-behind-3011.html(accessed on 06/01/2020)
117 See: https://techweez.com/2018/06/21/lsk-seeks-enjoined-case-against-cybercrimes-act/ (accessed on 12/02/2020)
118 See: https://www.accessnow.org/access-now-brief-african-countries-can-shape-cybercrime-laws-protect-rights/(accessed on 06/01/2020)

7. DISCUSSION

The selectivity and financial damage that comes from cyber-attacks [1], particularly in countries that have already ratified the Budapest Convention, suggests that, from the perspective of criminals, the risk pays off.

On the other hand [1], the great difficulty in decoupling these attacks from the most varied forms of cyber activism is also evident, which may come from political or religious extremism, as well as from anti-establishment movements.

Other evidence [1] is the great difficulty that law enforcement agencies are facing in containing the cybercrime phenomenon, even at the regional or community level, largely because of the persistence of Darknet, whose monitoring, control and possible eradication could be achieved by, for example, more robust Online Service Provider control mechanisms. Nevertheless, this issue is particularly complex in Europe, where the process of balancing individual rights and freedoms is critical[119].

As a recent criminal phenomenon [1], cyber mules have helped to make phishing more sophisticate, which is the most relevant form of cybercrime in sub-Saharan Africa [2], [17], [18]. In order to manage this situation and other types of attacks against victims located in this region, it seems undisputable that Open-Source software still presents itself as an alternative [6] to circumvent these countries' chronic budget deficit in terms of information security, not only as isolated initiatives[120], but as long-term programs.

That does not contradict recommendations of reference bodies [4], [7] in the sense that a study of similar solutions in other regions of the world, with socioeconomic characteristics very similar to the reality of sub-Saharan Africa, is justified.

119 See: https://ec.europa.eu/info/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules_en(accessed on 06/01/2020)
120 See: https://linux4afrika.de/en/ (accessed on 06/02/2020)

An objective analysis [9] of the state of transposition of both the Budapest Convention and the Malabo Convention into the legislation of sub-Saharan African countries shows the dual nature of the problem facing their governments.

While there are answers to the questions of local socio-economic development, the aggressive nature of neoliberal globalization, embodied in multinational corporations and related services [13], as well as the UN technical and financial assistance bodies [10],[20], cannot be ignored. That has resulted in the widening, in many cases, of the structural disparities and social inequity inherited from colonialism. **However, opting for simplistic crack-down approaches on whistle-blowers, or spying on dissidents living domestically and abroad, does not seem to be the best answer to their challenge. At worst, this can only mean a transposition of every day's reality into cyberspace.**

It also seems [9] **that the Malabo Convention was nothing more than an imperfect imitation of the Budapest Convention, with some political folklore, which copies the uncertainties and insecurities of African governments regarding the information age. The standard is that, when in doubt, the alternative is to refer to the Budapest Convention - which explains its higher adoption rate if compared to Malabo's.**

To be sure what could be expected was a greater investment in institutional capacity building of the judiciary, keeping the actions initiated long before the Malabo Summit [20]. The good news is that Sub-Saharan Law Societies appear to be up-to-date with the latest developments in cyber law[121].

Notable too, are many contributions of African scholars, who remain committed to creating a legally sustainable digital forensics, such as the University of Pretoria in South Africa [21], a country which has been experiencing particularly sophisticated

121 See: https://www.lexafrica.com/cyber-law-block-chain-technology/(accessed on 06/01/2020)

ransomware attacks[122] and the University of Lagos in Nigeria [22], [23], considered today the African superpower of smartphones.

In conclusion, in that same reasoning, it is confirmed that the booming mobile connectivity [11], [12], [15], [16] currently taking place in sub-Saharan Africa is still dictated by the market of neoliberal globalization. In fact, since the Washington Consensus[123], the relocation of the means of production and financial transactions has become the *modus operandi* of a large number of companies in the OECD countries.

They will be the largest providers of these *quasi* low-cost services, once installed in sub-Saharan Africa, in spite of a remarkable lack of digital literacy and financial ability to pay for them nowadays. That is a very interesting aspect, since usually most consumers in sub-Saharan Africa have opted to spend their money on entertainment-related content [15]. Therefore, some of the rare success stories in the countries of the region, such as the mobile money penetration in East Africa, galvanized by Kenya, need to be studied very carefully, as well as the cyber security gaps presented here [2], [17], [18], which should also be framed in the same perspective.

Lastly, the analysis of the current status of smartphone forensics in sub-Saharan African countries shows that almost all of them do not fully comply with internationally recognized standards and good technological and legal practices [4]. Even with large investments or capacity-building programs in human resources, forensic facilities and tools from the European Union and Interpol [18], [20], mistrust persists between law societies and the governments.

Furthermore, in most of the countries, there is no well-defined structure regarding the powers and attributions of cyber-crime units within the Police departments, which often overlap with intelligence services. Thus, combined with the absence of cyber

122 See: https://www.bbc.com/news/technology-49125853(accessed on 06/01/2020)
123 See: https://www.gsid.nagoya-u.ac.jp/sotsubo/Washington%20Consensus.pdf (accessed on 06/01/2020)

legislation in most of the countries [9], the digital evidence obtained this way does not proceed in court.

8. CONCLUSION

Three important aspects can be highlighted from this discussion.

First, unlike countries in the northern hemisphere, the nature of cybercrime cases on the African continent are mostly cyber-enabled crimes, and not cybercrimes committed exclusively in cyberspace. Consequently, cyber units are shaped to act more as ancillary services to the police departments and not to coordinate across specialized cyber security areas, such as combating and preventing cyber terrorism, cybercrime, cyber espionage and cyber activism. This scenario puts them in a position of subordination, which removes the effectiveness of the response and prevention of crimes with ramifications to Organized Internet Crime.

Secondly, with mobile technology being the most widely used technology standard for accessing digital services and solutions in sub-Saharan Africa, in-depth knowledge of smartphone forensics should be at the top of the European Union and Interpol's capacity-building programs priorities. However, that has not been happening, since these bodies have a Eurocentric perspective of containing cyber-enabled crimes, namely the Darknet's African connections with the international drug, people and arms trafficking and money laundering, which are also at the top of the OECD countries' security agenda.

Thirdly, the recognition of the duality of criteria, in general, in the application of the law in Sub-Saharan Africa, which gives priority to the crime of opinion or public morality, and not to the eradication of criminal forms that are much more serious and harmful to this region of the African continent, such as *Cyber Sakawa* and many more.

Particular attention is drawn to the duplicity which the vast majority of signatory countries to the Budapest Convention deal with this repressive stance in Sub-Saharan Africa. On the one hand, they are supporting capacity-building programs for the adoption of internationally recognized legal standards and good practices. On the other

hand, provide the means and technological knowledge for extrajudicial surveillance, compromising the consolidation of the rule of law. Therefore, realistic conditions should be created globally for Sub-Saharan governments to return to their traditional role of facilitators to address the current challenges of the smartphone forensics in Sub-Saharan Africa. *Dixit*.

9.REFERENCES

[1] EC3 - European Cybercrime Centre. *Internet Organised Crime Threat Assessment (Iocta) 2019*. Europol. 2019 Available for download here: https://www.europol.europa.eu/iocta-report

[2] Serianu. *Africa Cybersecurity Report 2017. Demystifying Africa's Cyber Security Poverty Line.* 2017. Available for download here: https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf

[3] Ben Martini, Kim-Kwang Raymond Choo. *An Integrated Conceptual Digital Forensic Framework For Cloud Computing.* Digital Investigation 9 (2012) 71–80. Elsevier. 2012. Available for download here: https://www.sciencedirect.com/science/article/pii/S174228761200059X

[4] INTERPOL. *Global Guidelines For Digital Forensics Laboratories*. INTERPOL Global Complex for Innovation. 2019. Available for download here: https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf

[5] Naing Linn Htun & Mie Mie Su Thwin. *Proposed Workable Process Flow with Analysis Framework for Android Forensics in Cyber-Crime Investigation*. The International Journal Of Engineering And Science (IJES) || Volume || 6 || Issue || 1 || Pages || PP 82-92|| 2017 ||ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805. Available for download here: https://www.researchgate.net/publication/313049731_Proposed_Workable_Process_Flow_with_Analysis_Framework_for_Android_Forensics_in_Cyber-Crime_Investigation

[6] Matthew McMillon. Building a Low Cost Forensics Workstation. SANS Institute. 2003. Available for download here: https://www.sans.org/reading-room/whitepapers/incident/building-cost-forensics-workstation-895

[7] Rick Ayers, Sam Brothers and Wayne Jansen. Guidelines on Mobile Device Forensics. NIST Special Publication 800-101 Revision 1. 2014. Available for download here: https://csrc.nist.gov/publications/detail/sp/800-101/rev-1/final

[8] Bijoy Boban. *An Analysis on Iphone and Smart Phone Forensics*. Cyber Law and Computer Forensics. Lovely Professional University, Phagwara, Punjab, India. 2014.

Available for download here: https://www.academia.edu/6716305/AN_ANALYSIS_ON_iPHONE_AND_SMART_PHONE_FORENSICS

[9] Matteo Lucchetti. *Cybercrime Legislation in Africa Regional and International Standards*. GLACY+. Cybercrime Pogramme Office of the Council of Europe (C-PROC). 2018. Available for download here: https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-05.pres_cybercrime_legislation_in_africa_12apr2018_matteo_l.pdf

[10] World Bank. *Doing Business 2019. Training for Reform.* 2019. Available for download here: https://www.doingbusiness.org/content/dam/doingBusiness/media/Annual-Reports/English/DB2019-report_web-version.pdf

[11] Kalvin Bahia. *State of Mobile Internet Connectivity 2018.* GSM Association. 2018. Available for download here: https://www.gsmaintelligence.com/research/?file=c0bcc185be555f77478a8fdf986ea318&download

[12] GSM Association. *Sub-Saharan Africa. The Mobile Economy 2018*. 2018. Available for download here: https://www.gsmaintelligence.com/research/?file=809c442550e5487f3b1d025fdc70e23b&download

[13] PriceWaterHouseCoopers. *Disrupting Africa: Riding the Wave of the Digital Revolution.* 2017. Available for download here: https://www.pwc.com/gx/en/issues/high-growth-markets/assets/disrupting-africa-riding-the-wave-of-the-digital-revolution.pdf

[14] Kalvin Bahia & Stefano Suardi. *The State of Mobile Internet Connectivity 2019.* GSM Association. 2019. Available for download here: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/07/GSMA-State-of-Mobile-Internet-Connectivity-Report-2019.pdf

[15] Kenechi Okeleke, David George and Emeka Obiodu. *5G in Sub-Saharan Africa: Laying the Foundations*. GSM Association. 2019. Available for download here: https://www.gsmaintelligence.com/research/?file=7d4569ab4c1f69b82e9ad8f179ba92ef&download

[16] Jan Stryjak & Michael Meyer. *Evaluating Mobile Engagement*. GSM Association. 2018. Available for download here: https://www.gsmaintelligence.com/research/?file=e608440880a26e2d36bd073a1245d26c&download

[17] Paula Musuva-Kigen, Martin Ekpeke, Emmanuel Inkoom,Beatrice Inkoom,Dadi Masesa,Brencil Kaimba,Kevin Kimani,Martin Mwangi,Barbara Munyendo,Faith Mueni,Daniel Ndegwa, Stephen Wanjuki, Nabihah Rishad, Samuel Keige, Jeff Karanja, Hilary Soita, Andrew Njuguna Ngari,Bryan Mutethia Nturibi,Denzel Ndegwa,Edward Owino,Gloria Gesicho,Ian Omondi Bwana,James Waiharo, Joylyn Chepkurui Kirui and Kenneth Mbae. *Africa Cyber Security Report 2016*. Serianu. Available for download here: https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf

[18] Symantech. *Cyber Crime & Cyber Security Trends in Africa*. 2016. Available for download here: https://www.thehaguesecuritydelta.com/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf

[19] Lewis C. Bande. *Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities.* International Journal of Cyber Criminology Vol 12 Issue 1 January – June 2018. 2018.Available for download here: https://www.cybercrimejournal.com/BandeVol12Issue1IJCC2018.pdf

[20] UNCTAD. *Harmonizing Cyberlaws and Regulations. Experience of the East Africa Community.* 2012. Available for download here: https://unctad.org/en/PublicationsLibrary/dtlstict2012d4_en.pdf

[21] Michael Kohn, JHP Eloff and MS Olivier. *Framework for a Digital Forensic Investigation*. Information and Computer Security Architectures Research Group (ICSA). Department of Computer Science University of Pretoria. 2006. Available for download here: https://www.researchgate.net/publication/220803284_Framework_for_a_Digital_Forensic_Investigation

[22] Ajetunmobi, Rukayat A, Uwadia, Charles O, and Oladeji, Florence A. *A Survey and Critique of Digital Forensic Investigative Models*. International Journal of

Computer Science and Information Security (IJCSIS),Vol. 14, No. 12, December 2016.Available for download here: https://www.academia.edu/31243408/A_Survey_and_Critique_of_Digital_Forensic_investigative_Models

[23] Rukayat A. Ajetunmobi, Charles O. Uwadia, Florence A. Oladeji.Computer *Forensic Guidelines: A Requirement for fighting Cyber Crime in Nigeria now?* Department of Computer Sciences, University of Lagos. 2016. Available for download here: https://www.academia.edu/31328029/Cybercrime_-_A_Case_for_Computer_Forensic_Guidelines_in_nigeria

[24] George Grispos, Tim Storer, William Bradley Glisson. *Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics*. University of Nebraska. 2012. Available for download here: https://www.academia.edu/2777260/CalmBefore_the_Storm_The_Challenges_of_Cloud_Computing_in_Digital_Forensics

[24] Interpol. *Overview of Serious and Organized Crime in Africa. Analytical Report.* ENACT (Enhancing Africa's response to transnational organized crime). 2018. Available for download here: https://www.interpol.int/content/download/12850/file/Overview%20of%20Serious%20and%20Organized%20crime%20in%20Africa-EN.pdf

[25] Warner, J. *Understanding Cyber-Crime in Ghana: A View from Below*. International Journal of Cyber Criminology (IJCC), Vol. 5 (1): 736–749. 2011. Available for download here: https://www.ripandscam.com/pdf/Cyber-crime-in-Ghana.pdf

[26] Boateng, R. Longe, O.B. Mbarika, W.A.V. Avevor, I. Isabalija, S.R. *Cyber Sakawa - Cybercrime and Criminality in Ghana*. Journal of Information Technology Impact. Vol. 11, No. 2, pp. 85-100. 2011. Available for download here: https://www.researchgate.net/publication/220889824_Cyber_Crime_and_Criminality_in_Ghana_Its_Forms_and_Implications

Appendix I
Table 2 – Cyber security gaps in Sub-Saharan Africa in 2016

Theme	Scenario	Consequence	Mitigation	Identified Gaps
Understanding of Cybercrime	Perceptions are different on what is an act of Cybercrime.	No standard definition. No collaboration between countries to fight cybercrime	Clear-cut definitions of cybercrime and cross-border co-operation to improve legal sanctions	How African companies can collaborate and share information on cybercrime
Monetary investments in cyber security solutions	Limited or no investments in cyber security solutions	Organisations are losing money through cybercrime	Cater for cyber security during Annual budgets. Proactive Investments in analysis and incident response.	Metrics to determine minimum budgetary allocations for cyber security for different industries
BYOD	High BYOD usage with low rates of best practice policies	Acceptable usage of company resources not defined. High risks associated with such devices	Define BYOD policies. Compliance within the workplace. Effective measures in place	Policies and best practices for the workplace
Cyber Security Management	In-house management of cyber security. Cyber security roles combined with other IT roles	Individuals assigned cyber security roles in organisations are more often overloaded with other tasks within the organisation and/or lack the necessary skill set to handle cyber incidents.	Develop in-house CSIRT, defined Information Security Departments or managed security services.	Developing, operating and maintaining cyber security functions at the work place.
Information Security	Few individuals with	Company employees lack	More training on different	Training more information

Theme	Scenario	Consequence	Mitigation	Identified Gaps
Certification & Technical Training	sufficient security technical training	basic information about information security foundation principles, best practices, important tools and latest technologies.	Information Security standards. Acquire information security certifications.	Security professionals
Employee Training	Employee training done mainly after a cyber security incident	Sharing information with unknown entities. Poor internet practice. Lack of preparedness after an incident assessment	Conduct regular people based risk. Develop an employee security awareness program	Developing and running and effective security awareness programs
Reporting of Cyber Crimes	High number of cybercrime is not reported to police, and for those that are reported, very few are followed through to prosecution.	Immature cyber security bills, laws and processes. Lack of user awareness	Adopt more mature processes for cybercrime prosecution. Involve more sectors during development of cyber laws. Universities, local groups, organisations and cyber security specialists. Raise awareness to citizens on reporting of cybercrimes	Escalation matrix for country wide cybercrime reporting.
External Threat Analysis	Publicly accessible IP infrastructure has unnecessary services enabled,	Unauthorized access to critical systems. High	Monitoring the latest security vulnerabilities published.	Standard configuration for systems. Continuous

Theme	Scenario	Consequence	Mitigation	Identified Gaps
	including content management and remote administration. Misconfigured SSL certificates and encryption settings.	increase of widespread attacks leveraging vulnerable infrastructure	Updating the security configuration guideline	testing and monitoring
Internal Cyber Threat Analysis	Use of obsolete systems and apps. Use of clear text and insecure protocols. Server misconfiguration. Use of default Credentials	Unauthorized access to critical systems. Vulnerable systems	Configuring all security mechanisms. Turning off all unused services. Setting up roles, permissions, and accounts, including disabling all default accounts or changing their passwords. Applying the latest security patches. Regular vulnerability scanning from both internal and external perspectives	Password management and best practice. Patch management best practice. Emergency patch management practices
Internal Traffic Analysis	Malware on systems. Botnets in private Infrastructures	Undetected malware on systems. Delayed incidence response	Continuous monitoring Incident response plan	Managing 24X7 monitoring. Traffic monitoring and analysis

Source: Serianu, 2017 [17]