CYBERLAW by CIJIC

DIREITO: A PENSAR TECNOLOGICAMENTE

Do we have one real perception of the true degree of technological intrusiveness into the lives of citizens?

At this «Cyberlaw by CIJIC», 2nd edition, we intend to bring to one legal and technological debate some of the most worrying questions related with the weakness of the traditional concepts of public law. Take, for example, old problems where, alleged, threats to state security compress ordinary individual freedoms. Cyberspace currently dominates daily life. Where can we find the protection of the legal-subjective positions of individuals in it?

Traditional juridical and legal programs will lose all effectiveness, sliding into nominal, if the rule of law gives up to respond to the daily problems of netizens.

We all face new legal dimensions. In face of the ineluctable conclusion that the Internet is a global resource, which we dare say, incompatible, par excellence, with the old concept of territorial sovereignty of State, which scientific criteria need to be included in the construction of a dogmatic approach to the regulation of cyberspace? Furthermore, can it be regulated? Which - if any - new international, worldwide, legal solutions we must strive for?»

FACULDADE DE DIREITO
UNIVERSIDADE DE LISBOA

CIJIC
Centro de Investigação Jurídica do Ciberespaço
da Faculdade de Direito de Lisboa

CYBERLAW by CIJIC

DIREITO: A PENSAR TECNOLOGICAMENTE

CYBERLAW by CIJIC Revista científica sobre *cyberlaw* | Número 02 junho 2016 | Grátis

DIREITO:
A PENSAR TECNOLOGICAMENTE

internet:

- international tribunal for the internet
- open and free Internet
- internet governance
- access to internet

outros: · international cooperation

CYBERLAW by CIJIC

EDIÇÃO N.º II – JUNHO DE 2016

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

A CIBEREDUCAÇÃO E A CIBERSEGURANÇA

CYBEREDUCATION AND CYBERSECURITY

SALOMÉ DE JESUS VIEIRA[1]

E

FERNANDO JORGE RIBEIRO CORREIA[2]

[1] Aspirante Salomé de Jesus Vieira. Correio electrónico: salome.jesus.vieira@marinha.pt
[2] Capitão-de-fragata Fernando Jorge Ribeiro Correia. Correio electrónico: ribeiro.correia@marinha.pt

ABSTRACT

The role of Information Technology (IT) in contemporary societies is predominant. The emergence of the Internet and the popularization of its use has changed the paradigm of corporate operation.

Industrial societies have turned into information societies, where knowledge and information are valued and have a key role. The Internet, primarily regarded as an absolute space of freedom that allowed access and sharing data instantly from anywhere in the world, is now seen as a factor of insecurity.

Cyberspace is susceptible to new forms of threat as crime in the virtual world. Cyber-attacks threaten citizens' privacy and freedom, undermine state sovereignty and may also disclose information that threatens national security.

The Information Security doesn't only depend upon available technology, but how the users use that technology to manage the information. Knowledge about how the technology works and how information is processed allows risk reduction and increase Information Security level, i.e., cybereducation is required to reach a security culture.

This work discusses the challenges that cyberspace brings us and maps the Cyberspace Security National Strategy with European Union follow the path of Cyberspace Information Security culture.

Keywords: cybersecurity, cybereducation, security culture, education model, Portugal.

RESUMO

O papel das Tecnologias de Informação (TI) nas sociedades atuais é preponderante. O aparecimento da Internet e a vulgarização do seu uso veio alterar o paradigma do modo de funcionamento das sociedades.

As sociedades industriais transformaram-se em sociedades da informação, onde o conhecimento e a informação são valorizados e têm um papel fulcral. A Internet, primeiramente considerada como um espaço de liberdade absoluta e que possibilitava o acesso e compartilhamento de dados instantaneamente e a partir de qualquer ponto do globo, é hoje vista como um fator de insegurança.

O ciberespaço está suscetível a novas formas de ameaça sobre a forma de crime no mundo virtual. Os ciberataques colocam em risco a privacidade e liberdade dos cidadãos, põem em causa a soberania do Estado e podem, ainda, divulgar informação que ameace a segurança nacional.

A Segurança da Informação não depende apenas da tecnologia disponível, mas essencialmente, a forma como os utilizadores empregam essa mesma tecnologia para gerir a informação. O conhecimento sobre o funcionamento da tecnologia e como a informação é processada permite reduzir os riscos e aumentar o nível de Segurança da Informação, ou seja, são necessárias acções cibereducação que conduzem a uma cultura de segurança.

O presente trabalho discute os desafios que o ciberespaço nos coloca e mapeia a Estratégia Nacional de

Segurança do Ciberespaço a fim de se caminhar para uma cultura de segurança da informação no ciberespaço.

Palavras-chave: cibersegurança, cibereducação, cultura de segurança, modelo de formação, Portugal.

1. INTRODUÇÃO

O conhecimento humano surge da necessidade permanente de entender o mundo que nos rodeia. Trata-se de uma ferramenta fundamental que o Homem utiliza não só para a sua sobrevivência, mas também para se relacionar com o seu semelhante.

A necessidade e a dúvida são os fatores impulsionadores do desenvolvimento das capacidades do ser humano e as inovações tecnológicas sempre acompanharam a evolução humana e foram desenvolvidas com o objetivo de facilitar e aprimorar as atividades necessárias para a subsistência do homem." (Efing, 2012, p. 23).

Atualmente vivemos na "Era da Informação", e qualquer tentativa de definição da sociedade da informação[1] em que nos inserimos, mostra-se redutora. A sua complexidade e amplitude é tal que podemos definir características, mas não dar uma definição concreta de sociedade da informação.

A expressão "sociedade da informação" realça o papel da informação na sociedade, por vezes também designada por "sociedade do conhecimento", na medida em que o conhecimento é gerado a partir da informação. Esta inversão de paradigma veio relativizar o espaço e o tempo, uma vez que as novas tecnologias, como a Internet, permitem o acesso e a partilha de dados a partir de casa instantaneamente.

Cada vez mais, a nossa vida profissional, pessoal e social depende da tecnologia. Já não há uma distinção clara entre a casa e o local de trabalho. As diferentes dimensões da nossa vida estão correlacionadas. Contudo, o preço a pagar pela globalização e inovações tecnológicas é o fim da envolvente estruturada, organizada e facilmente previsível em que nos encontrávamos.

A Internet assume-se como "uma dimensão de comunicação livre", é "um símbolo de liberdade e de capacidade para dominar o tempo e o espaço" (Wolton, 1999, p. 92), pela sua acessibilidade, universalidade e por conduzir o processo de globalização.

Contudo, apesar do seu papel fundamental, a Internet também compreende riscos, nomeadamente para a segurança e defesa nacionais. Apesar de numa primeira análise se

1 Um dos primeiros autores a referir o conceito de Sociedade da Informação foi o economista Fritz Machlup, no seu livro publicado em 1962, *The Production and Distribution of Knowledge in the United States*. Contudo, o desenvolvimento do conceito deve-se a Peter Drucker que, em 1966, no seu livro *The Age of Discontinuity*, fala pela primeira vez numa sociedade pós industrial em que o poder da economia assenta num novo bem precioso: a informação. (Crawford, 1983, pp. 380-385)

considerar a Internet como um espaço por excelência de liberdade absoluta e sem fronteiras, a realidade porém, leva-nos a observar o ciberespaço como um local não somente virtual e físico mas isento de regulamentação jurídica, onde os mais diversos crimes se podem manifestar" (Martins, 2012).

Assim, constata-se que temos uma necessidade emergente de educar os cidadãos para uma melhor utilização das novas tecnologias, uma vez que a chave para a prosperidade futura e para os modos de vida qualitativamente diferentes está na aprendizagem dos processos de manipulação, transmissão, armazenamento e obtenção de informação (Lyon, 1992, p. 1).

O ciberespaço é um assunto cada vez mais relevante, tanto a nível nacional como internacional. Somos confrontados com todas as suas capacidades, assim como com os aspetos positivos e negativos que resultam da sua utilização. Contudo, o conhecimento sobre o seu real funcionamento, bem como as suas vulnerabilidades e sujeições, dificilmente serão mapeadas por completo.

É necessário confrontar os desafios que o ciberespaço nos coloca com a capacidade de resposta desenvolvida, uma vez que a necessidade de cibersegurança é hoje mais importante que uma defesa bélica eficaz.

Novas formas de ameaça surgiram com a evolução tecnológica, mudando a dimensão do teatro de operações, do espaço físico para o ciberespaço, onde nos confrontamos com um inimigo que se tornou invisível perante os nossos olhos (Martins, 2012).

Os ciberataques põem em risco a privacidade e liberdade dos cidadãos, ameaçam a segurança nacional e até mesmo a soberania do Estado. Torna-se cada vez mais imperativa a necessidade de proteger a informação, uma vez que esta já não se encontra armazenada num espaço singular e preciso, mas sim no ciberespaço.

No ciberespaço, o controlo de acesso à informação torna-se mais difícil, podendo esta ser utilizada de forma abusiva, por indivíduos mal-intencionados, para servir interesses ilegítimos e afrontar os direitos, liberdade e segurança dos cidadãos.

De acordo com o Special Eurobarometer 404 – Cyber Security Report[2], as perdas devido a cibercrimes representam biliões de euros por ano, e estima-se que existem mais de 150.000 vírus e outros tipos de *malware* em circulação e aproximadamente um milhão de pessoas vítimas de cibercrime por dia. Os resultados apresentados no relatório indicam que 28% dos utilizadores da Internet na UE não está confiante da sua capacidade para usar serviços como *online banking* ou comprar bens *online*. Contudo, 70% afirmam estar razoavelmente ou muito confiantes, valores estes muito semelhantes aos obtidos no Special Eurobarometer 390[3], pesquisa efetuada em 2012.

Foi ainda apurado que 10% dos utilizadores sofreu fraude *online,* 6% foram alvo de roubo de identidade, 12% não conseguiram aceder a serviços *online* devido a ciberataques, 12% dos utilizadores tiveram a sua conta pessoal acedida de forma indevida (*hacker*), 7% foi vítima de fraude bancária *online* e 14% afirma ter encontrado, acidentalmente, material que promove o ódio racial e extremismo religioso.

Posto isto, e tendo como ponto de partida este panorama, considera-se essencial colaborar para a consciencialização e ação política no que respeita à cibersegurança. Ao Estado reconhece-se a capacidade última de proteger os seus cidadãos, e para isso é necessário fazer frente a estas ameaças que são uma constante diária. A cibereducação é uma competência que deve ser leccionada na atividade formativa de cada cidadão e é da responsabilidade do Estado incluir este tema nos programas de formação.

O presente trabalho encontra-se dividido em cinco secções. Na primeira secção é feito um enquadramento do tema. Na secção seguinte é apresentado um mapa de conceitos, onde são incluídos alguns tópicos que ajudam a enquadrar o tema do trabalho. Na terceira secção é abordado de forma sucinta o tema da partilha de informação nas redes sociais. O tema da cibereducação é apresentado na secção quatro. Finalmente, as conclusões são apresentadas na secção cinco.

2 Relatório elaborado por *TNS Opinion & Social*, a pedido *da European Commission, Directorate-General Home Affairs*, composto pelos resultados de uma pesquisa feita aos 27 países que constituem a UE e à Croácia, entre maio e junho de 2013. Disponível em: http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf (consultado a 09/11/15).
3 Disponível em: http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf (consultado a 09/11/15).

2. MAPA DE CONCEITOS

2.1 SEGURANÇA

O termo segurança abrange diversas aceções. Em linhas gerais, pode-se afirmar que este conceito deriva do latim *securitas*, que se refere à qualidade daquilo que é seguro, ou seja, aquilo que está protegido de quaisquer perigos, danos ou riscos. Quando se diz que algo é seguro, significa que é algo estável e indubitável. A segurança é uma certeza, mas também uma necessidade.

2.2 SEGURANÇA DO INDIVÍDUO

Segundo o artigo 27º n.º1 da Constituição da República Portuguesa (CRP): "Todos têm direito à liberdade e à segurança". Contudo, só é possível beneficiar de liberdade e segurança num ambiente de justiça, como previsto no artigo 28º da Declaração Universal dos Direitos do Homem, de 10 de Dezembro de 1948: "Toda a pessoa tem direito a que reine, no plano social e no plano internacional, uma ordem capaz de tornar plenamente efetivos os direitos e as liberdades enunciados na presente Declaração".

O conceito de "segurança humana" ou segurança do indivíduo surgiu nos anos 1990 e veio alargar a noção tradicional de segurança, antes centrada na segurança dos Estados. Passou-se a atribuir mais valor ao próprio indivíduo.

A segurança do indivíduo visa proteger os indivíduos contra ameaças, criminalidade, violações dos direitos humanos, invasão de privacidade e ameaça à reserva de intimidade. Aponta ainda para ameaças como a fome, doença, pobreza, violação sexual, imigração, desemprego e tráfico de pessoas.

Em suma, todos têm direito à segurança, ao reconhecimento dos direitos fundamentais e de viver em liberdade e com dignidade.

2.3 CIBERESPAÇO

Ciberespaço pode ser definido como um "ambiente virtual onde se agrupam e relacionam utilizadores, linhas de comunicação, *sites*, fóruns, serviços de Internet e outras redes" (Gobierno de España, 2011, p. 43).

De acordo com a Dicionário Editora da Língua Portuguesa, ciberespaço é definido como um "espaço virtual constituído por informação que circula nas redes de computadores e telecomunicações".

No atual mundo globalizado, o ciberespaço é visto como um espaço virtual, "que a par dos tradicionais domínios da interação humana como a terra, o mar, o ar e o espaço, é o meio onde se desenvolvem as atividades económicas, produtivas e sociais das nações mais desenvolvidas". (IDN, 2013, p. 9)

"O ciberespaço é assim um ambiente em si mesmo, onde se deve ter em linha de conta tanto a sua componente tecnológica, isto é, as vulnerabilidades inerentes ao seu emprego e ameaças que possam afetá-los, como os fatores humanos, uma vez que são estes que caraterizam os utilizadores deste ambiente" (IDN, 2013, pp. 9-10).

2.4 CIBERAMEAÇAS

Ameaças que surgem na sequência da utilização massiva das TI ligadas em rede e que podem afetar infraestruturas críticas para o equilíbrio funcional da sociedade, assim como o sistema político internacional. Como exemplos de Ciberameaças existe o *hacking*, o *hacktivismo*, o ciberterrorismo e a ciberespionagem.

O termo *hacking* refere-se a ações realizadas com recurso a ferramentas de *software* e *hardware* para exploração de vulnerabilidades dos sistemas informáticos com o objetivo de aumentar o nível de acesso ou controlo sobre os mesmos.

Hacktivismo é a ação conduzida por indivíduos ou grupos que utilizam meios informáticos e "veem a Internet como um veículo para promover e catalisar as suas causas e disseminar a sua mensagem" (Santos, 2011, p. 27). A ideologia defendida pode ter motivações distintas, desde políticas a religiosas, mas o objetivo final é comum: chamar a atenção da opinião pública para determinado assunto.

O ciberterrorismo consiste no uso das TI para ameaçar e realizar ataques políticos deliberados com grande impacto nos sistemas de redes de computadores e infraestruturas críticas. Promove o medo e o terror, "é um novo tipo de atividade criminal, (…) que materializa a convergência do ciberespaço com o terrorismo" (Santos & Bessa, 2008) que desencadeia determinadas ações políticas.

Ciberespionagem é caraterizada pela exploração de vulnerabilidades encontradas em *sites* para ter acesso a informação sensível. "É perpetrada por estados que procuram adquirir conhecimento e recolher informações, que lhe podem conceder uma vantagem estratégica sobre terceiros" (Pereira, 2012). A ciberespionagem é motivada pela vantagem competitiva sobre Estados ou ainda por benefícios financeiros provenientes da venda de informação roubada.

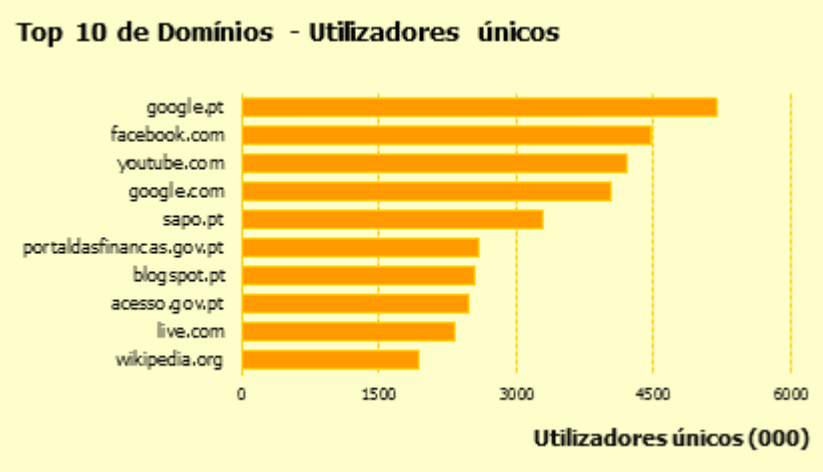
3.PARTILHA DE INFORMAÇÃO E AS REDES SOCIAIS

A utilização massiva das TI tem transformado a sociedade. Atualmente, a Internet é uma ferramenta que permite ao utilizador efetuar múltiplas tarefas. Não só é uma ferramenta de trabalho, mas também de diversão, indispensável a qualquer indivíduo.

Existem riscos associados à utilização da Internet, nomeadamente das redes sociais, dos quais é necessário ter conhecimento, estar alerta, agir em conformidade e, sobretudo, em segurança.

Segundo uma notícia do Público, publicada em Novembro de 2014, os Portugueses usam mais as redes sociais do que a média europeia.[4] Cerca de "70% dos utilizadores de Internet em Portugal usavam no ano passado [2013] redes sociais, significativamente acima dos 57% que eram a média dos 28 Estados-membros".

Em adição, conforme dados obtidos em 2016 e mostrados na Figura 1, é possível constatar que o motor de pesquisa do Google é a rede social eleita pelos utilizadores, estando em segundo lugar no Top 10 dos Domínios utilizados.



Fonte: Marktest, Netpanel *meter*

Figura 1 - Top 10 Domínios em milhares de utilizadores únicos de Abril de 2016

A navegação dos Portugueses na Internet é distribuída, essencialmente, em torno do Google, Facebook e YouTube. O Facebook, que é hoje a rede social com mais adesão.

4 Disponível em: http://www.publico.pt/tecnologia/noticia/portugal-acima-da-media-da-ue-no-acesso-a-redes-sociais-online-1675356 Consultado a: 19/11/2015.

Em 2009 era notícia por ter ultrapassado o número de utilizadores do Hi5, que chegou a atingir os 3,2 milhões em Portugal.

O gigante da informação, a Google, oferece os seus serviços ao mais comum dos utilizadores quase sem custos diretos. Esta é a percepção que cada um tem quando acede aos serviços como o Gmail, Google Maps, Google+, Hangouts, ou o Drive. Porém o acesso a estes serviços trás custos indirectos bastantes elevados para cada um: a informação pessoal que é disponibilizada quando viajamos, quem são os nossos amigos, que tipo de pesquisas fazemos, que informação guardamos na nuvem. Claro que todos nós podemos consultar o que disponibilizamos ao Google[5] e visualizar a quantidade de informação de cada um de nós torna público, porém sem termos consciência do que estamos a fazer.

A questão que se coloca, e que se tem vindo a tornar cada vez mais imperativa é de que forma se pode proteger os utilizadores dos perigos associados à utilização das redes sociais, e dos restantes domínios da Internet, quando estes, que reivindicaram pela criação de leis de proteção de dados pessoais estão hoje a publicar de livre e espontânea vontade os seus próprios dados nos perfis das redes sociais.

Os dados publicados voluntariamente pelos utilizadores das redes sociais vão deixando um rasto e são passíveis de se criar uma identidade digital acessível a qualquer outro utilizador. Há uma inconsciência generalizada, e uma despreocupação global com este assunto.

Os utilizadores expõem-se demasiado, revelando informações privadas e dados pessoais verdadeiros, o que pode acarretar consequências como roubos de identidade, assédios por parte de desconhecidos, raptos e violações.

Não há um conhecimento dos riscos associados e muito menos uma noção, ainda que básica, do que implica navegar na Internet. Os riscos atuais são bastantes e se não se educar os utilizadores para a cibersegurança estes não serão minimizados.

É nesta sequência que se compreende a necessidade emergente da cibereducação, isto é, consciencializar e educar os cidadãos para a importância da cibersegurança. Saber utilizar um computador não finda com o saber manuseá-lo e utilizar Internet não é tão

5 http://history.google.com

simples como apenas aceder e navegar em *sites*. A gestão da informação, pessoal ou da organização, é um tema emergente que todas as entidades que manuseiam informação devem saber como fazer. Conhecer os mecanismos, políticas e procedimentos de segurança pode não ser suficiente. É necessário também ter conhecimento sobre como a tecnologia funciona.

4. CIBEREDUCAÇÃO EM PORTUGAL

A cibereducação, para muitos utilizadores de Tecnologias de Informação e Comunicação (TIC), é o conhecimento estritamente necessário para o desempenho das suas funções numa organização. A cibereducação é considerada como sendo a aprendizagem da utilização de ferramentas e aplicações. Porém, a cibereducação não é apenas saber utilizar ferramentas de escritório, ou navegar na Internet, é também saber como gerir o que de mais-valia todos temos, a informação.

A troca e partilha de dados em rede são feitas em diferentes níveis de um sistema de comunicações. De uma forma simplificada, podemos considerar quatro níveis de interação da informação: o nível geográfico, o nível tecnológico, o nível lógico e o nível interface do utilizador.

O nível geográfico representa a localização física dos sistemas de informação e comunicação, bem como onde, estão localizados os sistemas de armazenamento e processamento de dados. O funcionamento de cada um destes sistemas é regulamentado por leis cuja aplicabilidade é regional. O conhecimento legal é uma parte da cibereducação e é da responsabilidade de todos, principalmente de quem tem capacidade de decisão.

O nível tecnológico abrange os sistemas de comunicação, de processamento e armazenamento de dados. Este nível, maioritariamente, é considerado pelos utilizadores, como sendo da responsabilidade dos administradores de sistemas e dos técnicos de informática. O conhecimento tecnológico requerido para se actuar neste nível deve ser adequado às funções que cada um desempenha. Porém, todos os utilizadores de sistemas de informação usam tecnologia para aceder à Internet. O modo como os nossos dispositivos interagem com os sistemas de comunicação depende da tecnologia que está disponível em cada local. Compreender as diferenças de acesso à rede através de um acesso sem fios (Wifi aberto ou cifrado, ligação de dados), ou de um acesso por cabo, é essencial para se perceber que tipo de informação pode ser acedido com segurança.

O nível lógico está relacionado com os processos de formatação de dados, com os protocolos de comunicação entre sistemas, com os algoritmos usados no processamento da informação. Este nível pode ser bastante complexo para a maioria dos utilizadores dos sistemas de informação. No entanto, os protocolos usados nos processos de comunicação

podem ser do tipo binário ou de texto, pode ser cifrados ou abertos. Os protocolos binários são aqueles que, olhando para um cabeçalho, compreender o seu significado implica descodificar o que cada bit ou grupos de bits representam. Carecem de ferramentas próprias para o efeito. Os protocolos de texto são todos aqueles que enviam mensagens de controlo em texto que pode ser lido e interpretado por um humano. Conhecer como funcionam estes protocolos pode ser a diferença entre olharmos para um *mail* que tem um grafismo e um formato expectável, mas o seu conteúdo tem outro significado. Um protocolo com cifra significa que os dados dados que são trocados entre sistemas não são compreensíveis caso não se conheça a chave de cifra. Mas existem diversos tipos de cifra. O que significa em termos de segurança uma cifra de 128bits, ou uma cifra de 256bits? Qual o nível de segurança que é expectável quando se usa *Secure Hyper Text Transfer Protocol* (HTTPS)? Onde é que está a segurança do HTTPS? Com estas questões não se pretende que o utilizador conheça em detalhe o funcionamento dos protocolos, mas sim, saber as diferenças entre protocolos e que informação pode transferir com segurança entre sistemas.

O nível interface do utilizador abrange todos os atores que usam os sistemas de informação. Um utilizador deve conhecer as politicas de segurança que estão em vigor na sua organização, deve conhecer as fragilidades e vulnerabilidades da rede onde que está a aceder, deve saber quais as consequências que podem advir da partilha de informação, deve compreender quais as capacidade de segurança disponíveis na sua interface com a rede – dispositivo de comunicações fixo ou móvel. O utilizador executa múltiplas e complexas de troca de informação com outros níveis do ambiente de informação, onde, as suas ligações variam ao longo do tempo. Neste contexto, a segurança da informação está dependente do conhecimento que o utilizador tem do ambiente onde está inserido, e não apenas da segurança física do seu equipamento ou da segurança lógica das aplicações que usa.

O conhecimento necessário para se poder compreender as relações que existem entre estas quatro camadas deve ser publico, e disponibilizado pelos organismos públicos e privados que têm responsabilidade nesta matéria.

Em Portugal, têm-se observado uma crescente preocupação sobre a segurança da informação na Internet. Este facto pode ser verificado pelo número de seminários e conferências que tem sido realizados nos últimos anos. Entidades como a Associação para

as Comunicações, Eletrónica, Informações e Sistemas de Informação (AFCEA Portugal), o Centro Nacional de Cibersegurança (CNCS), o Centro de Investigação Jurídica do Ciberespaço (CIJIC), entre outras, têm contribuído para a divulgação de temas relacionados com a segurança da informação. Porém, esta capacidade de atuação deve ser considerada com um complemento e atualização de conhecimento adquirido.

A base para se efetuar uma partilha de informação com segurança deve ter origem em matérias lecionadas durante o percurso académico de qualquer utilizador, adaptadas aos diferentes níveis de ensino. No ensino básico e secundário temos os adolescentes e jovens, grandes consumidores de novas tecnologias, que devem conhecer as vulnerabilidades dos sistemas que eles usam e como se podem proteger. As ações de formação do nível utilizador e do nível lógico devem estar direcionadas para a realidade que eles têm dos sistemas de informação e para perceção que têm de segurança. Deve ser aplicado o conceito de política de utilização aceitável, ensinando quais os limites que podem ser alcançados garantindo a segurança da informação que partilham.

No ensino superior temos homens e mulheres que estão a adquirir conhecimentos para ingressar no grupo da população ativa. São formados com competências necessárias para entrarem no mercado de trabalho, de acordo com a vocação de cada um. Matérias como a Gestão da Informação, a Segurança da Informação e a Gestão da Segurança da Informação devem fazer parte de todos os cursos do ensino superior, independentemente de os cursos não terem uma vertente tecnológica ou de gestão. Em alguma fase da atividade profissional, qualquer utilizador vai ter que usar sistemas de informação e ser responsável pela gestão de conteúdos. A profundidade das matérias associadas aos quatro níveis de interação da informação deve estar adaptada a cada curso, ou seja, não se pretende que um advogado substitua um engenheiro, ou vice-versa, mas o engenheiro tem que ter conhecimento legal sobre a utilização dos sistemas de comunicação e da informação, e o advogado deve compreender os processos de armazenamento e processamento da informação em rede, p.ex.

5. CONCLUSÕES

Este trabalho teve como objectivo enquadrar os temas da cibersegurança e do ciberespaço, e apresentar uma plataforma que permita identificar necessidades que levem à implementação do conceito de cibereducação a todos os utilizadores da Internet.

A segurança da informação no ciberespaço não deve ser interpretada como, um conjunto de políticas e procedimentos que são da responsabilidade das pessoas e organismos que administram os sistemas de comunicações, processamento e armazenamento de dados. A segurança da informação é da responsabilidade de todos os utilizadores de sistemas de comunicação em rede. O mapa de conceitos apresentado identifica alguns temas que se enquadram na actividade de qualquer utilizador que aceda a serviços em rede.

Quando é realizada uma pesquisa na Internet, em *sites* de redes sociais, como o Facebook, Instagram, Youtube, entre outros, a quantidade de informação pessoal que os utilizadores destes serviços disponibilizam de forma aberta é uma consequência da falta de conhecimento do que estão a fazer, ou seja, é falta de cibereducação. Este facto pode ser observado na criança que utiliza o *smartphone* dos pais e descarrega qualquer tipo de aplicação, no adolescente ou jovem que quer ser popular entre os amigos e disponibiliza conteúdos pessoais, no adulto que quer mostrar que a sua vida não é monótona e que tem mais actividade social que os seus amigos.

Uma política de utilização aceitável para acesso a serviços em rede permite minimizar os riscos de segurança da informação. Deve ser do conhecimento de todos os utilizadores. Cada utilizador deve conhecer os procedimentos e mecanismos de segurança que estão associados à política de utilização aceitável e compreender as consequências que o desrespeito por estas regras podem trazer para cada um e para a organização.

A cibereducação é uma matéria que deve estar presente no percurso académico de qualquer pessoa, desde o ensino básico. A cibereducação deve ser continuada com acções de actualização durante a vida profissional de cada um.

6.BIBLIOGRAFIA

EFING, António Carlos e FREITAS, Cinthia Obladen de Almendra (2012), ***Direito e Questões Tecnológicas Aplicados no Desenvolvimento Social (Vol.2),*** 1ª ed., Curitiba, Juruá Editora.

Gobierno de España *(2011), Estrategia Española de Seguridad: Una responsabilidad de todos,* Madrid.

IDN *(2013), Estratégia da Informação e Segurança no Ciberespaço (caderno nº12),* Instituto de Defesa nacional. Disponível em pdf em http://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf

LYON, David (1992), ***A Sociedade da Informação. Questões e Ilusões***, Oeiras, Celta Editora.

MARTINS, Marco (2012), "Ciberespaço: Uma nova realidade para a Segurança Nacional", Cibersegurança. Caderno N.º133 IDN, Lisboa, pp.32-49.

PEREIRA, Júlio (2012), Cibersegurança – O Papel do Sistema de Informações da República Portuguesa, Lisboa, Diário de Bordo.

SANTOS, Lino (2011), *Contributos para uma melhor governança da cibersegurança em Portugal*, Lisboa, Tese de Mestrado, Faculdade de Direito da Universidade Nova de Lisboa. Disponível em http://run.unl.pt/bitstream/10362/7341/1/Santos_2011.PDF

SANTOS, Paulo e Bessa, Ricardo e Pimentel, Carlos (2008), ***Cyberwar – O Fenómeno, as Tecnologias e os Atores.***

WOLTON, Dominique (1999), ***E depois da Internet?*** Algés, Difel.