DATA PROTECTION

MÁRIO ANTUNES
BALTAZAR RODRIGUES

INTRODUÇÃO À CIBERSEGURANÇA

A INTERNET, OS ASPETOS LEGAIS E A ANÁLISE DIGITAL FORENSE

FCA

Edição
FCA – Editora de Informática
Av. Praia da Vitória, 14 A – 1000-247 Lisboa
Tel: +351 213 511 448
fca@fca.pt
www.fca.pt

Distribuição
Lidel – Edições Técnicas, Lda.
R. D. Estefânia, 183, R/C Dto. – 1049-057 Lisboa
Tel: +351 213 511 448
lidel@lidel.pt
www.lidel.pt

Livraria
Av. Praia da Vitória, 14 – 1000-247 Lisboa
Tel: +351 213 511 448 * Fax: +351 213 522 684
livraria@lidel.pt

ISBN edição impressa: 978-972-722-861-4
1.ª edição impressa: abril 2018

Paginação: Magnetic – Design | Produção editorial
Impressão e acabamento: Tipografia Lousanense, Lda. – Lousã
Depósito Legal n.º 439835/18
Capa: José M. Ferrão – *Look-Ahead*

OS AUTORES

Mário Antunes

Doutorado em Ciência de Computadores e Mestre em Informática, ramo de Sistemas e Redes, pela Universidade do Porto. Licenciado em Engenharia Informática pelo Instituto Politécnico do Porto – Instituto Superior de Engenharia do Porto (IPP – ISEP). Professor Adjunto do Departamento de Engenharia Informática, da Escola Superior de Tecnologia e Gestão (ESTG) do Instituto Politécnico de Leiria (IPLeiria), onde coordena o curso de mestrado em Cibersegurança e Informática Forense. Tem a responsabilidade da lecionação de unidades curriculares nas áreas temáticas de redes de computadores, segurança na Internet, administração de sistemas e serviços de rede e infraestruturas de *cloud* e de *data centers*. É, atualmente, membro efetivo e investigador no *Center for Research in Advanced Computing Systems* (CRACS), uma unidade de investigação do laboratório associado INESC TEC.

Baltazar Rodrigues

Inspetor na Polícia Judiciária (PJ), 28 anos de carreira, nomeadamente na área do combate à criminalidade informática, onde esteve colocado 17 anos, vindo a chefiar em 2005 a equipa de Informática Forense daquela área e, mais tarde, em 2014, o grupo de Perícias Informáticas da PJ. Licenciado em Engenharia Informática pela Universidade Autónoma de Lisboa (UAL), pós-graduado em Direito e Cibersegurança pela Faculdade de Direito da Universidade de Lisboa (FDUL) e, atualmente, mestrando em Guerra de Informação, pela Academia Militar (AM). Professor Adjunto Convidado no curso de mestrado em Cibersegurança e Informática Forense no IPLeiria. Detentor de várias certificações internacionais relevantes na área da análise digital forense, das quais se destacam as seguintes: "Applied NTFS Forensics", "Trainer Development" e "Advanced Windows Forensics" pela University College of Dublin; "Certified Forensic Computer Examiner", pela IACIS; "Cyber-Trainer" pela Universidade de Zagreb; entre outras da INTERPOL, OLAF, FBI e EUROPOL.

ÍNDICE

INTRODUÇÃO

A Internet é uma rede que interliga, à escala global, vários computadores e utilizadores, ultrapassando fronteiras físicas, culturais e ideológicas. É inegável o seu papel dinamizador no quotidiano das empresas, organizações e cidadãos, bem visível nas melhorias obtidas pelo uso das tecnologias de informação e comunicação (TIC) e da Internet num vasto leque de atividades levadas a cabo no ciberespaço, nomeadamente o tratamento e processamento de informação, o fortalecimento de relações comerciais e sociais, a aprendizagem, o entretenimento e, mais recentemente, a *Internet of Things* (IoT) e a Indústria 4.0. A presença digital na Internet, por parte das empresas, organizações e cidadãos, é por isso uma necessidade inquestionável e uma obrigação em prol do desenvolvimento, da competitividade e da inovação.

O aumento crescente e exponencial da Internet, quer na sua abrangência geográfica, quer no número de utilizadores e na multiplicidade de serviços disponibilizados, encetou vários desafios e potenciou o aparecimento de um vasto leque de ameaças no ciberespaço. Destacam-se a proliferação de ataques intrusivos aos dados dos cidadãos e das empresas, do qual resultou o aumento crescente da vigilância às atividades dos utilizadores realizadas na Internet, que se traduziu na correspondente perda de privacidade.

Se, por um lado, a implementação de medidas reativas de segurança na Internet potencia tendencialmente a mitigação das ameaças, por outro a prevenção e a formação pode revelar-se um forte aliado na implementação de medidas pró-ativas e que evitem a execução de tais ameaças.

A motivação para a escrita deste livro é contribuir para a formação contínua dos utilizadores sobre o funcionamento da Internet e sobre as estratégias de prevenção que aí podem ser aplicadas, com vista à minimização dos eventuais riscos que se possam correr no ciberespaço. Para tal, este livro está direcionado para um espectro alargado de leitores, abordando os assuntos através de uma linguagem simples e remetendo para outros livros de referência a comprovação científica e a explicação técnica mais aprofundada de alguns conceitos.

Este livro contempla três áreas distintas que, embora científica e tecnicamente distantes, quando abordadas em conjunto acrescentam valor na compreensão das medidas pró-ativas de segurança que se poderão implementar na Internet e no ciberespaço, designadamente: funcionamento da Internet e dos seus serviços; funcionamento do sistema judiciário português; análise digital forense.

No Capítulo 1, enquadramos o funcionamento da Internet, a sua organização e os seus principais intervenientes. Abordamos os serviços mais relevantes disponibilizados na Internet e o seu funcionamento geral, analisando em detalhe os principais desafios existentes ao nível da cibersegurança. A temática das redes sociais e os desafios específicos ao nível da segurança, relacionados com a sua utilização massificada, são abordados no Capítulo 2.

O Capítulo 3 aborda a organização do sistema judiciário português, as suas entidades e as principais leis associadas aos crimes realizados na Internet e com recurso às tecnologias de informação e comunicação.

No Capítulo 4, damos a conhecer os principais termos relacionados com a gíria do cibercrime, nomeadamente a Lei do Cibercrime (Lei n.º 109/2009). Para cada um dos conceitos abordados descrevemos o provável enquadramento legal dos crimes praticados em cada um dos casos, tendo em conta a legislação em vigor. O articulado legal proposto resulta da vasta experiência de investigação criminal de um dos autores e tem em conta os cenários típicos para os crimes enunciados. Atendendo às variantes existentes para os vários crimes descritos, ressalva-se, pois, a necessidade de interpretar o articulado legal como uma proposta, não sendo (nem podendo ser) uma avaliação rigorosa e jurídica, extensível a todos os cenários concretos.

O Capítulo 5 é inteiramente dedicado a uma introdução à análise digital forense. Aí se introduz o conceito de prova digital, o seu percurso e uma metodologia para o seu tratamento ao longo de processo de investigação criminal. São, igualmente, descritas as funções de um perito forense e elencadas várias aplicações destinadas ao tratamento da prova digital e análise forense.

Uma introdução à recolha de dados em fontes abertas e às técnicas utilizadas para delas extrair "inteligência" (Open Source INTelligence) são apresentadas no Capítulo 6. Além do enquadramento do conceito de fonte aberta, exploram-se várias aplicações que poderão ser utilizadas para daí recolher informação em serviços da Internet, destacando-se os casos de estudo abordados: Facebook e Twitter.

Por fim, no Capítulo 7 fazemos uma incursão a dois tópicos emergentes: a *dark web* e as criptomoedas. No primeiro tópico abordamos o lado oculto e menos

conhecido da *web*, relacionado com a prática recorrente de atividade criminosa com recurso à anonimização dos intervenientes. No segundo tópico fazemos uma introdução às criptomoedas, designadamente à *bitcoin*.

Esperamos que este livro possa contribuir para uma melhor compreensão sobre o funcionamento da Internet e dos seus serviços, com vista a uma atitude pró-ativa na sua utilização diária. Contamos igualmente ter dado um enquadramento sólido sobre os principais desafios atuais da segurança na Internet e da análise digital forense.

Mário Antunes
Baltazar Rodrigues

1

INTERNET, *CLOUD*, IoT E *BIG DATA*

Funcionamento da Internet
Comunicação cliente/servidor
Modelo conceptual TCP/IP
Serviços e protocolos da Internet
Governação da Internet
Espaços de nomes e endereços
Fundamentos de computação na *cloud*
Internet das Coisas (IoT)
Principais ameaças à cibersegurança

INTRODUÇÃO

A Internet interliga, à escala global, um vasto e heterogéneo conjunto de equipamentos que têm em execução aplicações que permitem aos utilizadores a comunicação em rede.

O domínio e a compreensão do funcionamento da Internet, dos seus serviços, dos princípios de comunicação e protocolos, constitui uma mais-valia na identificação de ameaças à cibersegurança e na implementação de correspondentes medidas de mitigação.

A evolução da Internet ao longo dos seus quase 50 anos de vida é apreciável[1]. Desde o início de atividade, as tecnologias de informação e comunicação (TIC) têm tido uma evolução considerável, tendo-se atingido elevadas taxas de transmissão e uma grande diversidade de aplicações e serviços. Mais recentemente, a computação na *cloud*[2], a Internet das Coisas (*Internet of Things* – IoT) e a *big data* têm levado a um aumento exponencial e contínuo do volume de dados produzidos, das capacidades de alojamento e processamento na Internet, e ainda da capacidade para analisar e produzir dados e informação em tempo real.

No entanto, o número considerável de equipamentos ligados e a sua heterogeneidade, bem como o número igualmente elevado de utilizadores com acesso à Internet têm-na tornado mais complexa e com necessidades permanentes de vigilância, monitorização e resiliência. Em suma, a Internet tem-se tornado um espaço menos seguro para a comunicação, partilha de dados e trabalho colaborativo.

A **cibersegurança** pode, assim, definir-se como o conjunto de tecnologias, processos e práticas desenhado para proteger as redes, os computadores e outros dispositivos eletrónicos, programas e dados, de potenciais ataques ou ameaças. Conhecer o enquadramento histórico da Internet e o seu funcionamento contribui para uma melhor compreensão da atividade dos computadores e dos programas na Internet. Este conhecimento pode ainda potenciar, em certa medida, a mitigação de problemas relacionados com a cibersegurança.

[1] Em 1969, ainda com a designação de ARPANET.
[2] *Cloud computing* na denominação anglo-saxónica.

Assim, neste capítulo enquadraremos a história e o funcionamento da Internet, os seus principais serviços e as entidades que a governam. O modelo de funcionamento, denominado TCP/IP, é sucintamente abordado e são destacados os conceitos fundamentais de três tópicos emergentes: computação na *cloud*, Internet das Coisas e *big data*. O capítulo termina com a identificação dos principais tópicos relacionados com a segurança da infraestrutura da Internet e com os seus serviços.

1.1 ENQUADRAMENTO HISTÓRICO DA INTERNET

O termo "Internet" resulta da junção de duas palavras inglesas, *interconnected* e *networks*, e designa a infraestrutura de interligação de redes de computadores implantada à escala global.

A construção da Internet, designada inicialmente por ARPANET[3], iniciou-se nos Estados Unidos da América (EUA) no final da década de 60 do século XX, mais concretamente em 1969, com uma forte ligação ao seu Departamento de Defesa (DoD) e às redes utilizadas pelos militares para troca de informação. Na ARPANET começaram por se interligar as universidades da Califórnia (University of California, Los Angeles – UCLA), Utah (University of Utah – UU) e Santa Bárbara (University of California, Santa Barbara – UCSB), bem como o Stanford Research Institute (SRI). A integração de outras instituições nos EUA, a ligação ao Massachusetts Institute of Technology (MIT) e a primeira ligação por satélite à Europa ocorreu nos anos seguintes, ainda na década de 70. Desde então foram-se interligando várias novas redes, maioritariamente nos EUA e na Europa, essencialmente através de ligações dedicadas, assentes na infraestrutura de rede telefónica e recorrendo a ligações por satélite.

A ARPANET foi crescendo de forma rápida e descentralizada, não tendo um ponto central de governação, não pertencendo a uma instituição ou país, nem obedecendo a normas globais de comunicação entre os equipamentos. No entanto, o número de redes já interligadas levou à necessidade, por parte dos operadores e das instituições, de se adotarem normas que todas as instituições pudessem seguir. Essas normas regulariam aspetos relacionados com a identificação das redes e dos seus computadores, tecnologias de acesso utilizadas e, ainda, a forma como os vários operadores estariam interligados, entre outros aspetos. É no primeiro dia do ano de 1983 que se adota o TCP/IP como modelo de comunicação *standard* e a ARPANET passa a designar-se formalmente por Internet.

[3] *Advanced Research Projects Agency NETwork*.

A década de 80 do século XX corresponde a uma fase de expansão da Internet, com o envolvimento crescente dos operadores de telecomunicações, das universidades e centros de investigação, bem como dos governos e das instituições públicas. Assiste-se nesta altura a uma contínua massificação do seu uso e ao aparecimento de várias aplicações e serviços de gestão da rede.

Concretamente em Portugal, a primeira ligação à Internet ocorreu em 1985, entre a Universidade do Minho (UMinho) e a Universidade de Manchester (UOM) no Reino Unido, dando início a um período de implementação da infraestrutura à extensão do território português.

A Fundação para a Computação Científica Nacional (FCCN) inicia a sua atividade em 1992, ficando responsável pela gestão dos nomes que utilizam o sufixo ".pt" e pela atribuição dos endereços e identificadores às instituições públicas e privadas em Portugal.

Na década de 90, já com um elevado grau de globalização da Internet através da interligação de redes de vários países em diferentes continentes, assiste-se ao aparecimento de um dos principais serviços da Internet: o ***World Wide Web*** (WWW), ou simplesmente a ***web***. Genericamente, este serviço consiste na possibilidade de aceder a conteúdos através de uma aplicação gráfica específica, um *browser*, tirando partido das potencialidades de uma linguagem de marcação (*Hypertext Markup Language* – HTML) para "navegação" entre vários documentos.

Nas últimas duas décadas, a Internet não tem parado de crescer. Embora a sua globalização seja evidente e tenha permitido uma taxa de abrangência à escala mundial, é ainda possível encontrar zonas do globo que, por razões de ordem política ou outras, não dispõem de acesso à Internet[4]. Por outro lado, as tecnologias de comunicação sofreram um enorme avanço, tendo permitido um aumento muito grande nas taxas e capacidades de transmissão na Internet. Ou seja, transmite-se atualmente mais rápido e acede-se a uma maior quantidade de informação.

O crescimento acelerado do número de utilizadores, a quantidade de operadores envolvidos à escala global e a miríade de tecnologias de informação e comunicação que estão envolvidas fazem da Internet um caso de sucesso de partilha colaborativa de informação com impacto positivo no progresso das sociedades. Tal facto está bem refletido nos conceitos mais recentes que têm sido implementados na Internet, como sejam a computação na *cloud*, a abrangência da Internet a todos os dispositivos e "coisas" que se encontram ligadas entre si

[4] http://www.internetsociety.org/map/global-internet-report/

e à Internet, e ainda a necessidade de processar e gerir enormes volumes de dados através de soluções de *big data*. Por exemplo, o recurso a sensores para recolha de dados do ambiente envolvente e a sua publicação imediata na *cloud*, revela bem a realidade da Internet atual. Mantém os pilares com que foi criada, como sejam o acesso livre e descentralizado à informação, mas o âmbito atual é claramente mais abrangente, comportando não apenas computadores, mas também todos os dispositivos eletrónicos com ligação à Internet através de qualquer meio físico.

1.2 DESENHO DA INFRAESTRUTURA

A Internet é uma infraestrutura física onde assenta a comunicação entre as várias redes que dela fazem parte, quer sejam domésticas ou empresariais. Cada uma dessas redes é constituída por vários equipamentos terminais, como computadores pessoais (*personal computer* – PC), computadores portáteis e servidores, que estão interligados através de ***switches*** e acedem à Internet através de um equipamento de interligação, designado por ***router***. Estes asseguram o encaminhamento dos dados enviados pelos equipamentos terminais para a Internet e, à semelhança dos restantes, fazem parte da infraestrutura de comunicações, são ligados por cablagem maioritariamente de fibra ótica e cobre e encontram-se fisicamente alojados em edifícios dedicados, designados por ***datacenters***.

A inclusão de uma nova rede na Internet é um processo adaptativo e transparente para os utilizadores e equipamentos que dela fazem parte. Genericamente, cada nova rede na Internet é anunciada automaticamente, através de um processo de divulgação hierárquica, a todos os equipamentos de interligação da Internet, que ficarão a ter conhecimento da sua existência e das melhores rotas para lhe encaminhar os dados. Tomemos como exemplo o que acontece quando um cliente residencial estabelece com um operador de telecomunicações um contrato de ligação à Internet. Após a instalação, os equipamentos existentes em casa passam a ter acesso à rede local através do meio físico disponível (normalmente *wireless*), que, por sua vez, acede à Internet usando a tecnologia de acesso contratada e disponibilizada pelo operador (por exemplo, ADSL ou 4G).

2 REDES SOCIAIS

Definição de rede social
Funcionamento
Classificação
Noção de pegada digital
Principais ameaças
Medidas preventivas

INTRODUÇÃO

As redes sociais, como o Facebook ou Twitter, são atualmente as aplicações com maior contribuição para a pegada digital dos utilizadores na Internet. Além das ameaças intrínsecas ao funcionamento da Internet e da *web*, é possível encontrar desafios emergentes específicos, relacionados com a segurança e privacidade dos dados e dos utilizadores das redes sociais.

O domínio dos conceitos fundamentais sobre o funcionamento das redes sociais contribuirá positivamente para a compreensão dos desafios existentes ao nível da cibersegurança, bem como para as ações preventivas e reativas que se possam tomar no sentido de os contornar.

O aparecimento da *web* assenta em dois objetivos visionários para a época que, em certa medida, se confundem com os da criação da própria Internet:

- Permitir a comunicação e a partilha de informação entre todos os utilizadores;
- Tornar a informação facilmente acessível a todos os utilizadores, independentemente da localização.

Ao longo do tempo assistimos ao aparecimento de vários serviços e aplicações que concretizam, total ou parcialmente, estes objetivos. Como exemplo, podemos referir o aparecimento dos *Bulletin Board Systems* (BBS), do serviço de *email* e dos protocolos para partilha remota de ficheiros entre computadores, como o *File Transfer Protocol* (FTP).

O serviço *web* fomentou em larga medida a produção de conteúdos e a sua partilha. Alguns exemplos incluem as aplicações que tiraram partido da participação em massa da comunidade da Internet na produção de conteúdos, através de estratégias de *crowd sourcing*, que potenciou o aparecimento de *blogs* e serviços de enciclopédia como a Wikipedia[1].

É neste contexto que surge, já no século XXI, o fenómeno de ***social media***. Intimamente relacionado com o aparecimento das redes sociais, potenciou em larga

[1] www.wikipedia.org

escala a produção de conteúdos pelos utilizadores e a concretização dos objetivos inicialmente traçados aquando da criação da Internet. Os utilizadores passaram a criar, comentar e partilhar conteúdos, expressar emoções sobre esses mesmos conteúdos, moldar tendências e criar opiniões, assumindo a necessidade de terem presença digital na Internet e tornando-se verdadeiros produtores de informação.

Em termos técnicos, as redes sociais constituem um bom exemplo de aplicações da *web* que podem ser utilizadas por diferentes equipamentos e cujos dados são alojados e processados na *cloud*. É ainda com recurso a aplicações de *big data* que se torna possível analisar o gigantesco volume de dados produzido e assim identificar, entre outros aspetos, associações entre utilizadores e tendências.

O facto das redes sociais serem em grande número e cada uma conter um número elevado (nalguns casos, extraordinariamente elevado) de utilizadores e seguidores, produz um efeito de escala ao volume de dados gerado e alojado na *cloud*. Tal implica que as redes sociais sejam diretamente afetadas pelos constrangimentos e ameaças à segurança dos dados, descritos no Capítulo 1.

Neste capítulo definimos sucintamente o conceito de rede social e apresentamos uma proposta de classificação das mais comuns, por tipo de utilização. É descrito o funcionamento e organização de uma rede social, enquadrando os aspetos técnicos mais importantes. Damos particular destaque, no final do capítulo, à identificação das principais ameaças associadas ao funcionamento das redes sociais, deixando uma lista de recomendações e tópicos de reflexão sobre a segurança neste tipo de aplicações.

2.1 DEFINIÇÃO DE REDE SOCIAL

Genericamente, as redes de contactos sociais têm como principal objetivo o estabelecimento e fortalecimento de "relações sociais" entre indivíduos com interesses e atividades semelhantes. O aparecimento das redes sociais virtuais permitiu transportar para a Internet as funcionalidades de uma rede social física. Ou seja, os intervenientes passaram a estabelecer relações virtuais com outros utilizadores da rede social com os quais tenham afinidade (por exemplo, conhecimento pessoal) ou interesses comuns (por exemplo, o desenvolvimento de atividades na mesma área profissional).

As aplicações de redes sociais, como o Facebook ou o Twitter, têm por objetivo gerir as ligações existentes entre os utilizadores e os grupos que daí surgem. Para

cada utilizador estas aplicações armazenam um vasto conjunto de informação, como os seus dados de identificação, as suas ligações e todos os documentos (por exemplo, mensagens e conteúdos multimédia) que produziu. Esta informação é guardada por ordem cronológica, sendo possível, em cada momento, obter a **pegada digital** produzida por cada utilizador na rede social.

São diversas as motivações para a utilização das redes sociais por parte de empresas ou particulares. Quanto a estes últimos, ressalta-se a necessidade de terem presença digital e uma rede de "amigos virtuais" com quem possam partilhar informações sobre os seus interesses, responder a comentários de outros utilizadores, comentar conteúdos multimédia publicados e falar, verbalmente ou através de mensagens. Já as empresas têm como principal motivação a promoção dos seus serviços ou produtos junto do maior número de potenciais clientes que usem a rede social em causa. Por exemplo, as empresas ligadas à área de marketing começaram a olhar para as redes sociais como uma excelente oportunidade de publicitar os produtos e serviços dos seus clientes, através da utilização de estratégias de **marketing digital** nas redes sociais.

No entanto, em ambos os casos é evidente a necessidade de ter presença digital, com maior ou menor grau de exposição junto da rede social, mas sempre com interesse e motivação em pertencer à ***social media***.

2.1.1 Terminologia

Com as redes sociais surgiram alguns termos novos que podem ter designações diferentes consoante a aplicação.

Genericamente, cada utilizador começa por registar-se numa rede social e tornar-se seu **membro**, associando um **perfil**. A partir desse momento passa a ter uma **página** e a sua informação (por exemplo, nome, fotografia, contacto, localidade) passa a estar acessível aos restantes membros, que lhe podem fazer um **pedido de amizade** ou de **ligação**. A lista de **amigos** (ou de ligações) de cada utilizador vai assim crescendo à medida que este vai aceitando os pedidos que lhe são feitos.

Os conteúdos produzidos por um utilizador designam-se por ***posts***, que podem ser posteriormente comentados ou reencaminhados para outros utilizadores. Cada utilizador recebe continuamente uma lista atualizada de *posts* de todos os membros da sua rede, ordenados cronologicamente, designada por ***feed***. Em algumas

aplicações, os utilizadores podem ainda identificar nos seus *posts* os seus **amigos** (ou **ligações**), ou ainda sugerir a adição de novos, que são amigos de amigos comuns.

A variedade dos interesses dos utilizadores pode ser muito grande e, nesse caso, a rede social pode permitir a criação de **grupos** ou **canais**. O objetivo é agrupar de forma consentida os utilizadores com interesses comuns num determinado tema.

Dependendo da rede social, podemos encontrar, pelo menos, uma das seguintes formas de relacionamento dos utilizadores:

- **Amizade** – trata-se do relacionamento tradicional e bilateral estabelecido através do envio de um pedido de amizade. Neste caso, a informação partilhada por cada um dos utilizadores fica acessível no *feed* do outro e vice-versa;
- **Seguidor** – um utilizador pode optar por seguir outro unilateralmente, tornando-se assim o seu seguidor (*follower*);
- **Fã** – muito usado no relacionamento entre os utilizadores e a página de uma marca ou empresa. Neste caso, o utilizador subscreve o acesso aos conteúdos publicados pela empresa através do seu *feed*. No entanto, a empresa não recebe no seu *feed* os conteúdos publicados pelos seus subscritores.

Os conceitos de "amigo" e "seguidor" numa rede social são similares, mas com algumas diferenças operacionais significativas. Assim:

- Seguir um utilizador numa rede social (por exemplo Twitter ou Facebook) não implica o envio (e aceitação) de um pedido de amizade. Ou seja, não é necessária aprovação de um utilizador para que possa ser seguido;
- Enquanto os seguidores visualizam os *posts* e outros conteúdos produzidos pelo utilizador seguido, o contrário não se verifica. Ou seja, trata-se de um relacionamento unilateral em que o utilizador seguido não recebe no seu *feed* os conteúdos produzidos pelos seus seguidores.

Algumas redes sociais adotaram uma terminologia própria para alguns dos conceitos descritos anteriormente. Por exemplo, no caso do Twitter, os *posts* são designados por ***tweets***, têm no máximo 140 carateres (em fase de aumento para 280 carateres) e são classificados por uma ou mais palavras precedidas pelo símbolo "#", as quais se designam por ***hashtag***. A replublicação de um *post* ou o seu encaminhamento designa-se por ***retweet***.

3 SISTEMA JUDICIÁRIO PORTUGUÊS

Organização do sistema judiciário
Organização dos tribunais
Hierarquia das leis
Ministério Público
Gabinete do Cibercrime
Órgãos de Polícia Criminal
Lei do Cibercrime (Lei n.º 109/2009)
Formalização da queixa
Fases do processo penal

INTRODUÇÃO

O aumento considerável de transações que passaram a ser realizadas na Internet acelerou o aparecimento de novas oportunidades para o crime e para a realização de ações ilícitas. Nesse sentido, os sistemas judiciários tiveram de ajustar as suas leis à tipologia de crimes que surgiu com a Internet.

Para o cidadão comum, o conhecimento sobre as leis relacionadas com este tipo de criminalidade significa mais cidadania, mais conhecimento e, em certa medida, mais prevenção e segurança na utilização da Internet e dos seus serviços.

É razoável pensar que a utilização da Internet, como meio globalmente utilizado para a partilha da informação e conetividade de todos os seus utilizadores, não deveria, à partida, levar ao aparecimento de crimes e atividades ilícitas. As inúmeras vantagens, que a Internet e os seus serviços trouxeram para a melhoria da qualidade de vida dos seus utilizadores, deveriam necessariamente ser potenciadas em prol de um desígnio muito abrangente: o do bem comum e desenvolvimento global dos países. E, em boa medida, olhando para os quase 50 anos da Internet, é possível afirmar que esse desígnio foi alcançado, tendo provocado um enorme avanço no desenvolvimento dos países e da Humanidade em geral.

Contudo, como em tantas outras áreas, o que é bom e tem enormes vantagens, também revela o seu lado obscuro. O espírito aberto e descentralizado com que a Internet foi crescendo e acolhendo todas as pessoas e instituições, não lhes impondo qualquer "direito de admissão", permitiu que nela fossem entrando os mais diversos tipos de utilizadores e com as mais variadas motivações. Desde logo, os que passaram a utilizar a Internet como meio para agilizarem e melhorarem a forma como realizavam as suas atividades profissionais, mas também os que viram na Internet um mundo de oportunidades para praticar o mais variado conjunto de crimes. E são várias as atividades ilícitas que são praticadas na Internet, das quais damos conta ao longo desta obra.

É assim neste contexto que, ao longo do tempo e à medida que os crimes praticados na Internet se iam desenvolvendo, os governos, sistema judiciário e polícias

se foram organizando para esta nova realidade. Alteraram-se procedimentos, criaram-se novas leis e apertaram-se as regras de "admissão" dos utilizadores, com o objetivo de diminuir a atividade criminosa na Internet. Este jogo entre o "bem" e o "mal" no que diz respeito à utilização da Internet não tem aparentemente um fim à vista. Com efeito, à medida que se vão produzindo novas e mais apertadas regras para a eliminação de uma atividade ilícita, são logo descobertas pelos criminosos vias alternativas para dar continuidade a essa mesma prática.

Nesse sentido, torna-se importante que o cidadão comum tenha um conhecimento geral sobre o funcionamento das instituições, das principais leis e dos procedimentos que fazem parte do **sistema judiciário português**, com especial enfoque para os que lidam diretamente com a **criminalidade informática**, vulgarmente designada por **cibercriminalidade**. Tal atitude dá ao cidadão comum uma perceção clara sobre os limites que vão sendo estabelecidos à utilização lícita e legal da Internet, identificando simultaneamente as práticas ilegais que constituem um crime passível de investigação e sancionável pelos tribunais.

É esse o intuito deste capítulo, onde abordamos o sistema judiciário português e os seus principais atores, através de uma linguagem simplificada e sem entrar em aspetos técnicos do Direito. Iniciamos com a explicação sobre a organização do sistema judiciário português e da hierarquia com que as leis são aplicadas. De seguida, detalhamos o funcionamento do Ministério Público (MP), dando especial relevância ao seu gabinete de cibercrime e à cooperação com os Órgãos de Polícia Criminal (OPC), em particular com a Polícia Judiciária (PJ). É analisada de seguida a Lei do Cibercrime (Lei n.º 109/2009) e outras leis relevantes para este tipo de crimes. Este capítulo conclui com a descrição das várias fases do processo penal.

3.1 ORGANIZAÇÃO DO SISTEMA JUDICIÁRIO

O sistema judiciário é composto por um vasto conjunto de instituições, sendo algumas delas constitucionalmente designadas por **órgãos** e às quais estão atribuídos **poderes**. A organização global destas instituições é hierárquica e algumas delas ocupam os níveis superiores, sendo, por isso, designadas por **soberanas**.

Nesta secção enquadramos os principais órgãos e os respetivos poderes, com destaque para os tribunais que constituem a face mais visível para os cidadãos.

3.1.1 Órgãos de soberania e poderes

O Estado português é uma República constitucional e assenta em quatro órgãos de soberania: o Presidente da República, a Assembleia da República, o Governo e os Tribunais.

A Figura 3.1 ilustra a organização hierárquica dos vários órgãos e os respetivos poderes que lhes estão consignados pela Constituição da República Portuguesa (CRP). O Presidente da República tem o **poder moderador** e a função de fiscalizar a atividade do Governo. A Assembleia da República tem o **poder legislativo** e compete-lhe legislar os vários projetos de lei que aí são discutidos. O Governo tem o **poder executivo** e a sua missão principal é cumprir o programa que definiu para a legislatura. Pode ainda apresentar projetos de lei ou legislar autonomamente através de Decretos-Lei (DL). Por fim, os tribunais representam o **poder judicial**, tendo como missão defender os direitos e interesses dos cidadãos e a garantia da legalidade democrática.

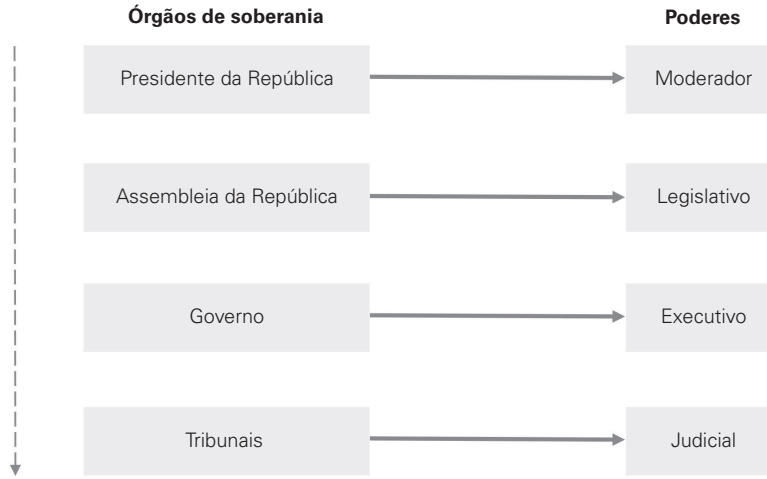

Figura 3.1 • Órgãos de soberania e poderes

3.1.2 Tribunais

Os tribunais representam o órgão de soberania com competência para administrar a justiça em nome do povo (Artigo 202.º da CRP), têm um funcionamento independente e apenas estão sujeitos à lei (Artigo 203.º da CRP).

DATA PROTECTION

O aumento crescente e exponencial da Internet, quer ao nível geográfico, quer no número de utilizadores e serviços disponibilizados, lançou vários desafios e potenciou o aparecimento de um vasto conjunto de ameaças no ciberespaço. Se, por um lado, a implementação de medidas reativas de segurança na Internet conduz tendencialmente à diminuição de ameaças, por outro lado, a prevenção e a formação contínua dos utilizadores podem revelar-se um forte aliado na implementação de medidas pró-ativas e que evitem a execução de tais ameaças.

Este livro, escrito numa linguagem muito clara e simples, procura contribuir para a melhoria do conhecimento dos utilizadores quanto ao funcionamento da Internet e às estratégias de prevenção que aí podem ser aplicadas, com vista à redução dos riscos que possam correr.

Destinado aos profissionais que pretendam adquirir conhecimentos introdutórios e competência na área da investigação da criminalidade informática e análise digital forense, aos estudantes de Informática, de Direito e de outras áreas relacionadas, e também ao público em geral, este livro apresenta-se como uma preciosa fonte de informação sobre os variados temas de interesse no âmbito da segurança na Internet.

TEMAS:

- **Funcionamento da Internet e dos seus principais serviços**
- **Redes sociais e aspetos relacionados com a segurança dos utilizadores**
- **Sistema judiciário português e Lei n.º 109/2009**
- **Formalização da queixa e fases do processo penal**
- **Gíria do cibercrime**
- **Noção de prova digital e metodologia de análise digital forense**
- **Relatório de análise digital forense**
- **Técnicas de OSINT**
- **Recolha de informação em fontes abertas**
- ***Dark web*, *dark net* e *deep web***
- **Rede TOR**
- **Criptomoedas e *bitcoin***

Os temas fundamentais da cibersegurança, num texto acessível a todos! Com informação essencial sobre o funcionamento da Internet, os aspetos legais, a análise digital forense e as estratégias de prevenção, com vista à redução dos riscos no ciberespaço.

MÁRIO ANTUNES

Professor Adjunto do Departamento de Engenharia Informática, da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria (IPLeiria), onde coordena o curso de mestrado em Cibersegurança e Informática Forense. Membro efetivo e investigador no *Center for Research in Advanced Computing Systems* (CRACS), integrado no laboratório associado INESC TEC.

BALTAZAR RODRIGUES

Inspetor na Polícia Judiciária (PJ), 28 anos de carreira, nomeadamente na área do combate à criminalidade informática. Professor Adjunto Convidado no curso de mestrado em Cibersegurança e Informática Forense no IPLeiria. Detentor de certificações internacionais relevantes em análise digital forense.

ISBN 978-972-722-861-4

9 789727 228614

FCA

GRUPO LIDEL

www.fca.pt