ISCTE Business School
Instituto Universitário de Lisboa

# MITIGAÇÃO DO MALWARE PARA O DESENVOLVIMENTO EMPRESARIAL EM PORTUGAL

Rui Diogo Duarte Mendes Serra

Tese de Mestrado
em Marketing

*Orientador:*
Prof. Doutor Rui Vinhas da Silva, Prof. Auxiliar,
ISCTE Business School, Departamento de Gestão

Lisboa, Novembro 2011

ISCTE Business School
Instituto Universitário de Lisboa

MITIGAÇÃO DO MALWARE PARA O DESENVOLVIMENTO EMPRESARIAL EM PORTUGAL

**Rui Diogo Duarte Mendes Serra**

# Agradecimentos

Gostaria de expressar a minha gratidão a várias pessoas cujo apoio e ensinamentos me permitiram cumprir com o meu trabalho:

- Rui Vinhas da Silva, Orientador, que partilhou com sabedoria o seu profundo conhecimento em diversas áreas de Economia e Marketing.

- A maioria dos professores e colegas mas, acima de tudo, os meus parceiros de trabalhos no ISCTE. O trabalho deles melhorou o meu.

- Os especialistas e colegas entrevistados para esta tese, cuja opinião, ciência e disponibilidade, engrandeceram o meu trabalho. Em especial à equipa da AnubisNetworks, que conta com algumas das pessoas mais brilhantes nesta área.

- Finalmente, à minha família e à Alexandra: Eu agradeço por tudo.

# Conteúdo

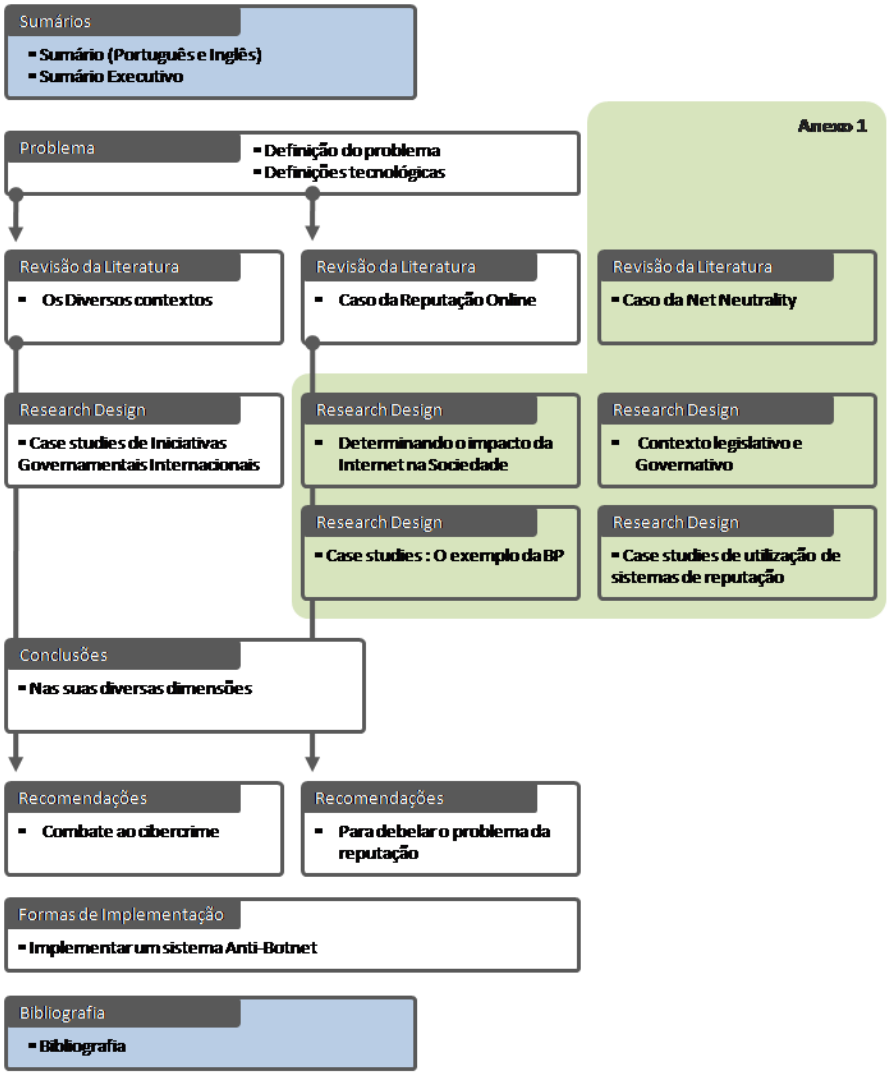
# Índice de Ilustrações



# Índice de Tabelas



# Estrutura do Documento



# *1* Sumário / Summary

## 1.1 Sumário

Num momento em que importa a Portugal capacitar-se, nos seus meios empresarial e industrial, para os desafios árduos que enfrenta, todos os factores diferenciadores contam:

- Dotar as redes e comunicações informáticas de segurança apropriada, ajudando a percepcionar um sentimento de conforto e de conhecimento técnico, que ajudará as empresas estabelecidas em Portugal.
- Debelar o problema do *malware* informático também ajudará prevenindo a fuga de informação e os crimes informáticos.
- A tecnologia de ponta nas grandes empresas de telecomunicações, bancos e outros sectores críticos simbolizam a qualidade e eficiência que se pretende imprimir a Portugal, melhorando a reputação intrínseca a essas empresas e a Portugal (em sentido lato), com os benefícios económicos que resultarão deste factor.

Esta tese, Projecto de Empresa, objectiva estudar os problemas e as oportunidades do combate ao *malware* informático em governos e em quem providencia os acessos à Internet, dos pontos de vista social, e tecnológico, de forma a assegurar a boa reputação online (de rede e social) e segurança destas entidades.

O *case study* do actual momento, os problemas e recomendações, em Portugal e na Europa, visa a transferência de conhecimento para a audiência. E, como corolário, visa argumentar um produto Português, AnubisNetworks *ZombieWall*, como solução que debele alguns dos problemas.

Palavras-chave: *ISPs, anubisnetworks, botnets, reputação online, malware,*

## 1.2 Summary

At a time when it is very important for Portugal to empower itself, in its businesses and industry, for arduous challenges it is facing, all the differentiating factors matter:

- Provide appropriate security measures to computer communications and networks, helping to perceive a sense of comfort and expertise, which certainly will help companies established in Portugal.
- Overcome the problem of computer malware will also help preventing the leakage of information and computer crimes.
    - The high standard technology in large telecommunications companies, banks and other critical areas symbolize the quality and efficiency that is desired for Portugal,

improving the intrinsic reputation fo these companies and Portugal (at large), with the economic benefits that will result from this factor.

This thesis, Corporate Project, aims at studying the problems and opportunities in the fight against computer *malware* by governments and Internet Service Providers, from social and technological point-of-views, so that network and social reputation of these entities can be improved

The case study of the current moment, the problems and recommendations, in Portugal and in Europe, aims at transferring knowledge to the audience. Moreover, as corollary, aims at disclose a Portuguese product, AnubisNetworks *ZombieWall*, as solution to overcome some of the problems.

Keywords: *ISPs, AnubisNetworks, online reputation, botnets, malware.*

# *2* Sumário Executivo

Durante a última década, a Internet transformou-se numa infra-estrutura crítica, com milhões de cidadãos e empresas a depender desta numa base diária.

Durante este mesmo período, as ameaças à segurança na Internet também aumentaram. As mesmas características que tornaram a economia da Internet crescer com tanto sucesso - globalidade, inexistência de controlo, inovação, liberalismo, acessibilidade a todos os sectores socioeconómicos - estão sendo utilizadas por criminosos para a prática de actividades ilegais em grande escala. Os custos globais de tais actividades são de magnitudes de milhões de euros [Bauer, Van Eeten (2008)].

Este é um assunto que, dada a sua extrema importância, abrange muitas vertentes da sociedade: desde, naturalmente, a segurança e engenharias informáticas, passando pelas componentes políticas internacionais até, talvez não tão óbvio, a própria ciência empresarial do Marketing.

Porquê? Por essencialmente dois motivos:

- Primeiro porque existe um canal muito lucrativo (internet), e uma fonte gigantesca de publicidade, de campanhas, de geração de *leads* e de *brand awareness* que dependem grandemente da internet. O mundo digital é o maior e mais importante ecossistema do Marketing, com características muito próprias e cujo manuseamento deve ser tão criterioso quanto apetecível.
- O segundo motivo, inter-relacionado, é que qualquer empresa, para vender precisa de uma boa reputação, enquanto entidade, do seu país, dos seus colaboradores, e até mesmo do sub-mercado onde opera. E não existe sítio onde mais facilmente se destrói e se constrói uma reputação, verdadeira ou falsa, do que a Internet.

O combate ao cibercrime, o impacto que isso tem nas empresas, em especial na reputação das mesmas, e de que modos podem precaver-se é uma temática incrivelmente complexa e abrangente, que facilmente possibilita estudos das mais variadas áreas.

Nesta tese, procura-se simplesmente estabelecer pontos de contactos entre todas as áreas, de um modo superficial (especialmente na parte de tecnologia) permitindo, idealmente, tornar o leitor uma pessoa suficientemente entendida e alertada para que, no seu meio (empresarial, político, e mesmo pessoal) aja em conformidade.

Em corolário, apontar-se-á uma solução que visa debelar este problema. Transformando esta tese, em certa medida, no elemento motivador à implementação da solução.

As soluções que debelam estes problemas (que nunca extingue, obviamente) existem, e requerem simplesmente aplicação, motivação e apoio.

Apoio e motivação deverão surgir quase por obrigação e desígnio nacional, não só pela gravidade do problema, mas também pela necessidade urgente, de Portugal e da União Europeia, de se restabelecerem e fortalecerem no mercado global (para tal suceder, a boa reputação online, e de segurança, são nevrálgicas).

Entre todas as ameaças, as *botnets* são sem dúvida o mais difícil de combater.

*(botnets*, redes de computadores comprometidos com software que, sem conhecimento dos proprietários dos computadores, executam software malicioso (transformando-se em *bots* - autómatos)).

Este software coloca o computador sob o controlo de um atacante remoto, que usa esse *bot* para realizar uma variedade de tarefas ilegais - enviar emails de spam, perturbações na rede, e roubos de identidade e financeiro, entre outros.

As *botnets* são uma ameaça séria. Os números exactos são difíceis de encontrar, mas o que é certo é que milhões de computadores em todo o mundo foram comprometidos (as estimativas divergem entre 1% a 25% de utilizadores online).

Os criminosos realmente lucram com estes esquemas. Sendo também bastantes seguros (transmissões electrónicas que atravessam o mundo), estima-se que os crimes associados a *botnets* se cifrem em valores astronómicos, e a tendência global parece estar a piorar.

Esta tese visa consequentemente mostrar que o combate ao cibercrime, o que os governos, as empresas, e os principais intervenientes fazem, e poderão vir a fazer, tem um impacto profundo (mesmo sendo impossível de determinar) na sociedade e no que se quer na mesma.

Em temos de opções e conclusões, para além de medidas de carácter global, sobressai uma ideia interessante que ganha força, neste âmbito, e que é ter os Internet Service Providers (ISPs) a funcionar como "guardiões", e ajudar a proteger os utilizadores que residem nas suas redes. O raciocínio é que os ISPs podem perceber os padrões de tráfego incomum, e os dados a serem transmitidos, pelos seus clientes subscritores.

O melhor exemplo de combate aos *bots*, e o enfoque nos ISPs, consiste em monitorizar as tentativas de acesso a C&Cs (websites de "comando e controlo" que servem, basicamente, para dar ordens e obter informações (e dados pessoais) por parte dos *bots* residentes).

Se na rede existem computadores a contactar websites de C&Cs e outros websites infectados, então os computadores também estarão infectados. Os ISPs podem, então, notificar o cliente, e até mesmo desligar a conexão até que a infecção seja removida. Uma solução prática, mas os ISPs têm poucos incentivos para sua implementação, especialmente em grande escala. É aqui que deveriam entrar os governos.

A Alemanha “governamentalizou” uma medida deste género, com o apoio de todos os ISPs, e o resultado é um aumento da qualidade da rede, da internet (da reputação, quer dos ISPs quer da Alemanha como um país seguro online) e da vida dos utilizadores, claro (menos cibercrime, menos roubos de identidades e/ ou informações confidenciais).

Além da Alemanha, também a Holanda, a Coreia do Sul e a Austrália implementaram iniciativas do género. E em todo o mundo, muitos ISPs agiram por iniciativa própria e privada neste âmbito. Também em Portugal, pelo menos dois operadores desenvolvem presentemente medidas de mitigação de Botnets (com a colaboração da empresa portuguesa AnubisNetworks), que visam o mesmo princípio. E cujos custos suportam, sem nenhum reconhecimento, apoio, ou mesmo benefício económico, para medidas que promovem o bem comum da segurança.

# *3* Definição do Problema

## 3.1 Enquadramento

Redes de telecomunicações e sistemas de informação são um factor essencial no desenvolvimento económico e social. Talvez mesmo *utilities*, semelhantes à oferta de transportes ou electricidade.

Em simultâneo, a convergência de redes de comunicação, conteúdos, média, serviços e dispositivos cresce exponencialmente, aumentando a dependência da União Europeia (e Portugal) sobre estas redes, infra-estruturas de suporte e tecnologias.

Este factor é facilmente corroborado pela muita informação estatística disponibilizada.

A par deste crescimento também crescem exponencialmente os crimes informáticos, em especial aqueles correlacionados com *malware* (*bots*, spam e vírus).

> *Um estudo realizado pela Symantec, fabricante de software antivírus, estima que os custos dos crimes praticados na Internet ascendam a 114 mil milhões de dólares (80 mil milhões de euros) por ano.*
>
> *Segundo o Norton Cybercrime Report 2011, mais de 430 milhões de adultos em todo o mundo foram vítimas de crimes realizados na internet no ano passado. O mesmo relatório indica, de resto, que os custos do cibercrime superam o mercado de tráfico de marijuana, cocaína e heroína à escala global.*
>
> [Symantec (2011)]

Portugal, enquanto conjunto de empresas, sociedade, e massa humana, terá mais facilidades em evoluir económica e socialmente se estiver dotado de uma infra-estrutura de comunicações tecnológicas mais capaz; em especial se essa capacidade tecnológica se reflectir na reputação (tecnológica e social) percepcionada, do país e das empresas que o compõem.

Capacitar uma infra-estrutura de comunicações tecnológicas, torná-las mais seguras contra os cibercrimes e *malware*, e melhorar a sua reputação, será porventura um dos factores que mais confortará qualquer empresa/ país/ recurso humano, que pretenda interagir económica e/ ou socialmente com Portugal, se atentarmos à importância das comunicações electrónicas no contexto global.

O Problema é, por conseguinte, tentar entender os perigos e como Portugal (e as suas empresas) e, em sentido mais lato, a União Europeia, se podem tornar economicamente mais fortes melhorando a sua infra-estrutura de comunicações tecnológicas, e, em especial, melhorando a sua reputação.

### 3.1.1 Métodos e Objectivos

*Botnets* e *Malware* são as mais sérias ameaças de segurança que a Internet enfrenta hoje, e como outros desafios de segurança cibernética, não podem ser erradicados simplesmente utilizando soluções técnicas.

O problema é, directa ou indirectamente, transversal a toda a sociedade, e a todos os sectores económicos e governativos. Entre estes "stakeholders", o papel de fornecedores de serviços de internet será especialmente recorrente e controverso.

Esta tese é um projecto de empresa que visa esclarecer os seguintes propósitos:

- Quais são as principais ameaças e por que é importante mitigar este problema?
- Quais são as implicações deste problema em termos de:
    - Competitividade
    - Inovação e crescimento tecnológico
    - Segurança tecnológica
    - Contexto Financeiro
    - Contexto Social e Económico
- Qual o impacto das *botnets* e do *malware* na reputação online
- Focalização do problema nos intervenientes (Estado e ISPs) que assumidamente podem mitigar *botnets*, posicionando-os em destaque para:
    - Uma solução, para Portugal, que mitigue este problema?

Esta tese é, na sua essência, uma justaposição e compilação de dados, usando a muita informação existente (especialmente ao nível de organismos como a ENISA, a ANACOM e outros) e suportando os possíveis desenvolvimentos noutras soluções existentes.

Tentando ser imparcial nos seus argumentos, esta tese funciona, contudo, como uma proposta comercial, como um propósito de elucidar uma audiência ou com capacidade decisória, ou de influência.

## 3.2 Definições tecnológicas do Problema

### 3.2.1 Definição de cibercrime (e as suas diversas componentes)

A definição do crime informático corresponde, na essência, a duas variações:

- O crime com um objectivo e penetração direccionados a sistemas informáticos (*Hacking*) com o intuito de obter ou alterar informação, com fins de variada ordem (obtenção de informação confidencial, motivos políticos, motivos sociais, alteração de informação privada, etc.)
- Os crimes não direccionados, expansivos, também perpetrados por cibercriminosos, e que visam a difusão de correio não solicitado, *phishing*, implantação de *botnets* e outras ameaças.

Em termos tecnológicos, todas as componentes de tecnologia que visem crimes informáticos, poderá ser designada por *malware* ou *crimeware* (OstermanResearch [2009]).

As motivações para um ataque poderão ser distinguidas em 5 variantes [Amoroso, E.G. (2011)]:

- *Country-sponsored warfare* - Confronto patrocinado por países (e/ ou entidades com ligações estreitas a governos) - usualmente envolvendo as grandes potencias mundiais e/ou os estados com sistemas de fraca democraticidade - É hoje um dado adquirido que as ofensivas e defesas electrónicas são uma das principais componentes militares. A capacidade de, "à distância" se inutilizar equipamento electrónico, comunicações e defesas, e a capacidade de se capturar ou corromper informação ("intelligence") do adversário são armas de magnitude superior ao armamento bélico tradicional, para mais possibilitando que se esconda a proveniência desses ataques. Um ataque destes tem, por definição, capacidades e motivações muito elevadas. A título de exemplo, é conhecido o treino, pela Coreia do Norte, de um exército de hackers, com o único intuito de perpetrarem ataques, camuflados, contra nações inimigas.
- *Terrorist attacks* - Ataques terroristas - Se considerarmos o tipo de exposição a que um ataque cibernético expõe, se comparado com um ataque terrorista no sentido clássico do termo, é entendível que esta variante é, nos dias que correm, encarada seriamente por alguns grupos terroristas. O impacto é variado, mas os recursos são, acima de tudo, humanos, e menos tecnológicos (no sentido de serem mais acessíveis, se compararmos a aquisição de um servidor com a aquisição de, por exemplo, um lança-granadas).
- *Commercially Motivated attack* - Ataques motivados comercialmente - Serão porventura os ataques mais comuns entre entidades colectivas, se entendermos que um ataque não se restringe a infligir danos visíveis, mas também a recolher informação confidencial e danificar reputação. A motivação é, acima de tudo, obter algum tipo de vantagem comercial.
- *Financially driven criminal attack* - Ataque criminoso de motivação financeira - são os ataques mais comuns, quando perpetrados por indivíduos ou grupos criminosos, e habitualmente correspondem a roubos de identidade, com o intuito de se roubar ou extorquir dinheiro, obtendo credenciais, acedendo a contas bancárias, ou mesmo chantageando os lesados em troca de dinheiro.
- *Hacking* - Uma designação comum que, no seu sentido mais verdadeiro se restringe a delinquência (juvenil, mas também adulta) na internet, com motivações centradas no alcance de reputação própria (nas comunidades de hackers) ou sabotando a reputação de terceiros (por causas políticas, ideológicas e sociais). De todos os ataques, é aquele mais amador e de mais fácil anulação. O âmbito criminal das actividades de *hacking* varia desde actividades não consagradas criminalmente (em alguns países, a venda de cópias pirateadas de software) até crimes com alguma gravidade (danos de propriedade terceira, apropriação indevida de propriedade terceira, divulgação não autorizada de correspondência e informação privada).

### 3.2.2 Definição de *malware*

*Malware* é a denominação genérica para os seguintes tipos de programas e acções destinados a crimes informáticos:

- *Botnet malware* - Um programa utilizado para a coordenação e operação de um ataque automatizado em redes de computadores. Um *bot* (singular de *botnet)* poderá ter "embebido" vários outros tipos de *malware*.
- Vírus - Um programa que visa infectar um computador sem permissão.
- *Worm* - Um tipo de vírus informático, com capacidades de auto-propagação numa rede informática.
- *Trojan*: um programa maligno que se disfarça como uma aplicação benigna quando se instala num computador.
- *Rootkit* - Um conjunto de programas que trabalham para subverter o controlo de um sistema operativo aos operadores legítimos, fazendo alterações em camadas abaixo da camada aplicacional ("abaixo dos programas").
- *Spyware* - Um programa instalado clandestinamente, focado essencialmente em capturar as comunicações e os dados, transmitidos nas interacções de um utilizador com o computador.
- *Backdoor* - Um programa / método concebido para contornar as regras de autenticação e autorização e deste modo obter acesso a uma componente privada de um computador e/ou de uma rede.
- *Downloader* - Um programa que disfarçadamente visa obter e instalar outro software malicioso.
- *Adware* - Um programa que exibe automaticamente ou extrai automaticamente (em download) material publicitário.
- *Ransomware* - Um tipo de código malicioso que criptógrafa os dados que pertencem a um utilizador, exigindo um resgate (financeiro, essencialmente) para o seu restauro.

Outros termos e outras definições haverá. Importa destacar, de todas estas variações, o *malware*, em sentido lato, como todos os programas com funções criminosas, e as *botnets* (redes de *bots*) como programas que se infiltram em muitos computadores com o intuito de os controlarem [CA Technologies (2010)].

### 3.2.3 Definição de *botnets* (e zombies)

Um zombie é um computador, infectado, que toma acções, normalmente prejudiciais, na rede e nos próprios computadores, sem o aparente conhecimento do seu proprietário.

Tal acontece, normalmente, por infecção com *bots* e *botnets*.

Estes *bots* (software (*malware*) inteligente), atacando alvos específicos, ou disseminados casuisticamente em muitos computadores (*botnets* - redes de *bots*) visam vários objectivos, mas mais usualmente, apropriarem-se das contas de email e das palavras-chave dos utilizadores para enviar spam, capturar correspondência ou perpetrarem roubos de identidade.

No primeiro caso, o envio massivo de email permite disseminar automaticamente grandes quantidades de spam com intuitos criminosos, essencialmente para venda de produtos, ou para esquemas de *phishing (ver definição no subcapítulo seguinte)*. Este procedimento origina paralelamente problemas de tráfego na rede, bloqueio das contas e das comunicações do utilizador. Para além dos emails de spam conterem frequentemente vírus que infectam os destinatários.

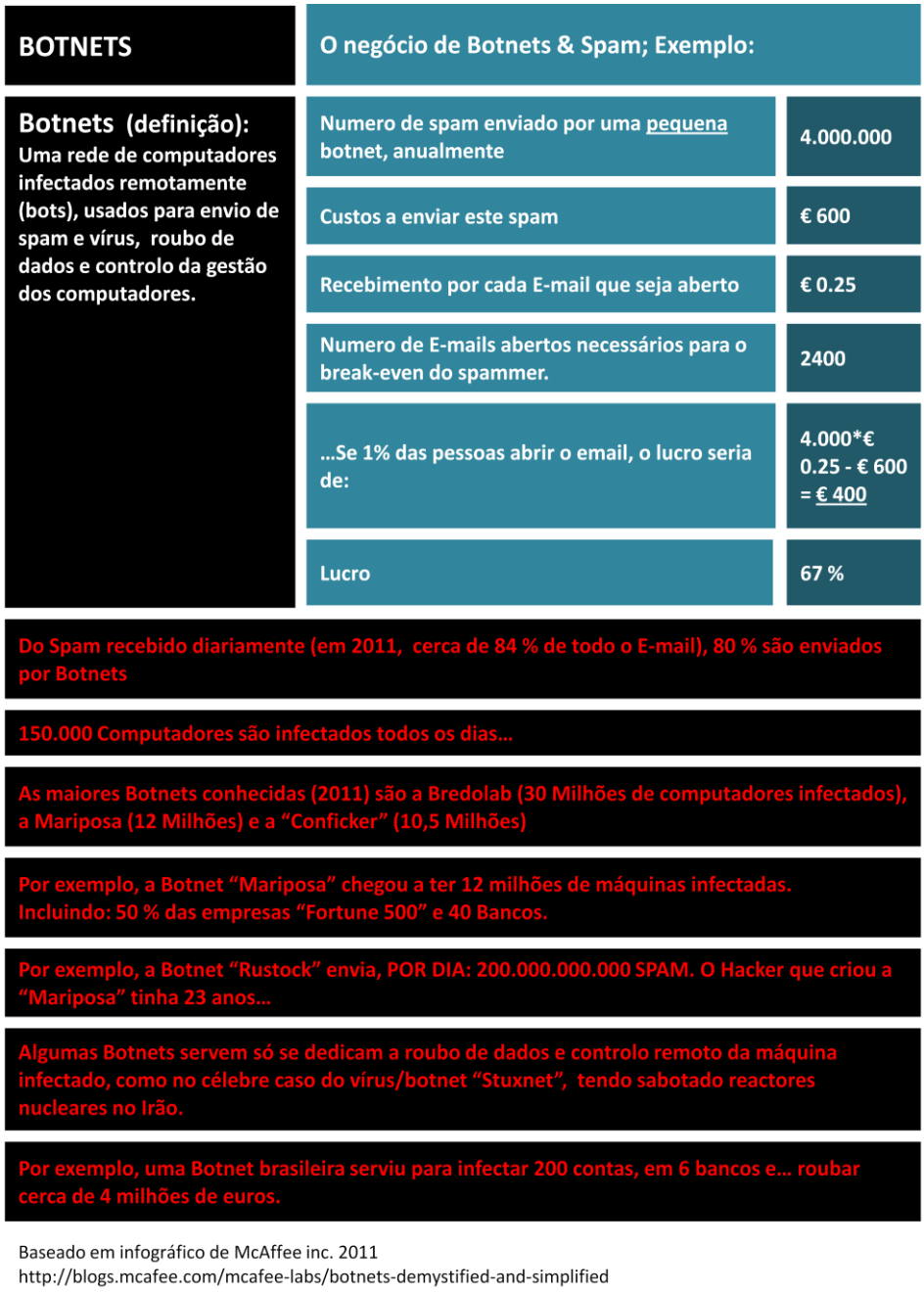



Ilustração 3-1 O negócio de Botnets e spam: exemplo

## A função das botnets

A motivação por detrás de uma *botnet* pouco mudou nos últimos anos. Inter-relacionando a descrição das botnets mais recente [Symantec (2011)] com o oficialmente estabelecido na indústria [ENISA 2011)], podemos encarar as seguintes funções, primárias:

- Ataques *Distributed Denial of Service* (DDoS) – "Inundação" do destino com muitos pedidos ou transferências de dados, até que o serviço fica incontactável e/ou offline: Se considerarmos que o número médio de *bots* dentro de uma *botnet* é 20,000. E que é muito comum um atacante controlar várias *botnets*, um ataque DDoS contra uma

empresa ou governo pode ser devastador. Neste caso particular, as diferentes motivações costumam ser:

- Os ataques contra os concorrentes,
- Os ataques com motivações políticas e ideológicas (como no caso recente contra websites do Governo da Estónia)
- Os ataques contra empresas de segurança e/ou contra empresas que se regem por noções de segurança diferentes (como no caso recente contra as editoras de música, pelos adeptos da distribuição gratuita na internet).

- Fraudes on-line: cada computador infectado por uma *botnet* (um "zombie") envia os dados pessoais aí alojados para um servidor distante (conhecido como um servidor C&C – *Command & Control*). Estes dados podem ser credenciais de acesso (a bancos, a contas de email, etc.), formulários preenchidos, dados de redes sociais, ficheiros de dados armazenados em disco. Estas informações "exploráveis" são depois usadas com propósitos económicos, quer directamente (roubar dinheiro) quer indirectamente (chantagem em troca do retorno dos dados).
  - Ataques *stealth* - Muitas vezes, o computador infectado tem um *backdoor* (um ponto ilegítimo de entrada e saída nas comunicações) permitindo ao atacante utilizar esse computador para fazer outros ataques, normalmente de spam ou *phishing*. As vantagens são que qualquer tentativa de determinar a origem do ataque coincidirá com esse computador infectado, e não com o atacante.
  - Spam - A forma mais comum de utilização de *botnets*: Fazer os computadores infectados como remetentes massivos de email de spam, e de todas as suas variantes, incluindo *Phishing, Whaling (phishing direccionado)*, e afins.
    Este tipo de ataque sub-reptício, uma vez mais, impede de determinar a origem criminosa do sucedido, com outra grande vantagem: Como os emails e os servidores que alojam emails têm uma reputação associada (que lhes permitem, por exemplo, ser aceites em destinos com protecções de segurança), enviar spam através destas entidades funciona como garantia de sucesso na entrega de emails.
  - Redistribuição de código malicioso - Uma característica comum a todas as *botnets* é tentarem reproduzirem-se infectando outras máquinas. As formas de redistribuição deste código malicioso assumem várias formas, desde *Click frauds* (um computador infectado aloja um website, infectando quem clicar em determinado sítio) até à transmissão de vírus pela rede e/ou por email.

| Utilização | Designação |
|---|---|
| Localização e infecção de outros sistemas de informação. | *botnet growth* |
| Roubar informações confidenciais a partir de cada sistema comprometido (*key-logging*, acesso sistema de arquivos, etc.). | Roubo de informação privada e confidencial |
| Executar ataques *Distributed Denial of Service* (todos os *bots* "bombardeiam" um alvo com tráfego, ao mesmo tempo, destruindo frequentemente a ligação e a acessibilidade). | DDoS |
| Hospedar websites de *phishing* (por fraude) e *Mule-websites* com endereços IP rotativos. | *Phishing* e camuflagem |
| Envolver-se em fraude de cliques (Os *bots* "clicam"em *ad-banners* fazendo ganhar dinheiro aos donos dos *bots*) | *Click-Fraud* |

| | |
|---|---|
| *Warez host* (software pirata), pornografia e outros conteúdos ilegais. | Pirataria |
| Espionagem (espiando utilizadores infectados ou interceptando o tráfego da rede). | Espionagem e *Man-in-the-middle* |
| Utilização como um proxy / shell para atacar sistemas maiores informações (remoção de IP trace). | Camuflagem |
| Auto-defesa (eliminando software de anti-*malware*, desactivando as actualizações, etc.). | Auto-defesa |
| Enviar spam (para o lucro, e na distribuição de *malware*). | Envio de spam e propagação de *bots* |

Tabela 3-1 Tipos de utilização para *botnets, (baseado em Amoroso, E.G. [2011])*

As cinco entidades que perfazem um ataque por *botnets* são [Amoroso, E.G. (2011)]:

- O Operador de *botnet* - O indivíduo, grupo ou país que cria a *botnet*, incluindo o modo de "deploy" (integração e activação) e a operação da mesma. Quando as *botnets* têm motivações financeiras, é o operador quem beneficia. É também o elemento de mais difícil detecção, sendo vulgar a imprensa ajuizar, com pouca evidência existente, que determinado ataque teve determinada responsabilidade, simplesmente porque foi determinado (muitas vezes incorrectamente) determinado país de origem (o próprio funcionamento das *botnets* predispõe que computadores infectados controlem outros, tornando difícil aferir uma origem).
- O Controlador de *botnet* - O servidor, ou o conjunto de servidores que controlam as *botnets*, normalmente conhecidos por C&Cs ("Command and Control"). Normalmente também estes servidores foram comprometidos, e muitas vezes sem o saberem. Estão distribuídos desordenadamente por diversas localizações e tem uma reputação (de rede) que os permite comunicar sem serem impedidos. Têm a função de "recrutar" as *botnets*, emitir ordens e receber a informação das *botnets*.
- *Botnets* - Estes são as redes de equipamentos (e utilizadores) desprevenidos, normalmente computadores com ligações de banda larga que, sem saberem, foram infectados por *botnet malware* e que, de esse momento em diante, são distribuidores de spam e vírus, com a própria informação no computador a ser também facilmente distribuída. Existem registos de números superiores a um milhão de máquinas infectadas pela mesma *botnet*, e activas durante períodos de anos.
- *Botnet Software Drop* - Em alguns casos, existem servidores distintos com o propósito de armazenarem o software a ser descarregado de e para as máquinas infectadas. Durante um ciclo de vida de uma *botnet* é comum que os infectados estejam inactivos durante diversos períodos de tempo, e que o software ilícito que os permite serem controlados e fazerem acções seja actualizado ou alterado, de forma a executar diferentes tarefas e/ ou a iludir sistemas de antivírus.
- *Botnet Target* - As *botnets* tem o objectivo, não só de se multiplicarem com vista a obterem mais informação, mas de atacarem um ou mais alvos. Quer sejam milhões de utilizadores a receberem spam, ou um determinado website que se pretende que seja comprometido, fazendo, por exemplo um DDoS (ataque *Distributed Denial of Service*, que inutiliza serviços, sobre dosando os pedidos de ligação para um determinado website).

### 3.2.4 Definição de spam (e *phishing*)

> *São enviados, diariamente, 120 biliões de e-mails contendo spam.*
>
> *[Ironport (2010)]*

A definição legal, constante do artigo 22.º do Decreto-Lei n.º 7/2004, indica:

> *"Considera-se SPAM todas as "mensagens para fins de marketing directo, cuja recepção seja independente de intervenção do destinatário, nomeadamente por via de aparelhos de chamada automática, aparelhos de telecópia ou por correio electrónico". Não constituem comunicação publicitária em rede:*
>
> *Mensagens que se limitem a identificar ou permitir o acesso a um operador económico ou identifiquem objectivamente bens, serviços ou a imagem de um operador, em colectâneas ou listas, particularmente quando não tiverem implicações financeiras, embora se integrem em serviços da sociedade da informação;*
>
> *Mensagens destinadas a promover ideias, princípios, iniciativas ou instituições."*
>
> *[República Portuguesa (2004)]*

O *phishing* é uma vigarice que utiliza SPAM ou mensagens de *pop-up* para ludibriar pessoas no sentido de revelarem números de cartões de crédito, informação de contas bancárias, números de segurança social, palavras-chave e outro tipo de informação confidencial ou sensível. Tipicamente, os "phishers" enviam emails ou *pop-ups* que alegam provir de uma empresa ou organização com a qual a potencial vítima tem negócios - por exemplo, o seu ISP (fornecedor de serviços de Internet), banco, serviços de pagamentos online ou até um organismo governamental. A mensagem costuma dizer que a pessoa necessita de "actualizar" ou "validar" a informação da sua conta. Pode até ameaçar consequências extremamente indesejáveis para o caso de não haver resposta. A mensagem encaminha a vítima para um website que parece um website legítimo de uma organização, mas na realidade não é. O propósito deste website fraudulento é enganá-la no sentido de divulgar informação pessoal que permita aos burlões roubar-lhe a sua identidade e debitar contas ou cometer crimes em seu nome.

### 3.2.5 Definição de ISPs

A definição utilizada, de ISPs (acrónimo para Internet Service Providers - fornecedor de serviços de Internet) é empregada com referência ao seu sentido mais lato, utilizada para melhor desenvoltura do assunto, ou seja: todos os intervenientes (Empresas) que fornecem serviços de acesso e comunicações pela internet, seja na totalidade, seja em componentes específicos (como email) ou mesmo outras variações de telecomunicações (As empresas de telecomunicações, que oferecem *triple-play* são mais que ISPs). No caso Português, os maiores ISPs são a PT (Sapo, Meo, Tmn), a Zon, a Vodafone, a Optimus e a Cabovisão, responsáveis pela quase totalidade da infra-estrutura de telecomunicações nacional.

# *4* Revisão da Literatura: Os diversos contextos da Sociedade

## 4.1 Contexto de Competitividade

A Competitividade que um país pode demonstrar não resulta exclusivamente da política económica dos seus governos, mas também do entendimento cabal dos seus ditames reais, ou seja a capacidade de convencer todos os *stakeholders* de uma economia global do mérito dos nossos bens e serviços (Da Silva [2010]). Dito isto, percepcionarmos, para o exterior, que as qualidades de nosso país incluem a segurança e a reputação na internet, é possível que os conceitos interligados de eficiência e eficácia do país, estendidos a este paradigma, reforcem a capacidade desse mesmo país.

No próprio contexto da importação de produtos portugueses, mesmo que estes ou as empresas que os produzem tenham uma ténue (nenhuma é impossível) relação com a internet e com as comunicações, existe sempre uma relação entre as características do produto e os intangíveis do produto.

Para além desse facto, existem as vantagens associadas ao melhor serviço, para além da qualidade e reputação percepcionadas: Um país evoluirá melhor (economicamente, tecnologicamente) quanto melhor for a capacidade da sua população.

Alcançar o rótulo de tecnologicamente evoluído ainda faz mais sentindo no caso de Portugal, sendo um país com fracas capacidades (o analfabetismo funcional, conforme explicado por Rui Vinhas da Silva (2010) que explica, em parte, o atraso face a outros países, e que basicamente se traduz no desequilíbrio na capacidade de interpretar informação (e que maior fonte de informação existe do que a Internet)).

O caso de Portugal, leia-se a sua deficiente competitividade foi, à luz da actualidade, agravado pelos incumprimentos económicos e financeiros que obrigaram ao auxílio externo. Este factor, indissociável da reputação portuguesa é visível em diversos estudos, que reforçam Portugal, como um mau parceiro para trocas comerciais [Yu, Shun *et al* (2011)], a par de todos os países do sul Europeu. O estudo anteriormente citado, desprestigia Portugal enquanto responsável economicamente, atingindo as suas instituições. Curiosamente, nada de errado se aponta aos cidadãos. Reflectindo sobre estes resultados, facilmente se percebe que providenciar segurança nas transacções económicas e comerciais, e simultaneamente restabelecer as instituições como credíveis (atribuindo-lhes o mérito da tal segurança económica e comercial, por exemplo) é uma medida que, previsivelmente, atenuará qualquer reputação nefasta que Portugal possa ter aos olhos dos compatriotas europeus.

Preposição:

O êxito de uma empresa é fortemente influenciado pelo contexto nacional em que está inserida. E, se determinarmos que a competitividade assenta em quatro factores: As

eficiências Empresarial e Governamental, a performance económica e as infra-estruturas [Cardoso, (2008)], é entendível a importância capital de uma internet segura, logo melhor: infra-estruturas capazes e melhor acesso à grande base de inteligência mundial tornará as empresas mais eficientes e, em principio, com melhor performance económica.

## 4.2 Contexto da inovação e crescimento

Num mundo em que a inovação progride a par da ambição, a meta deverá ser maximizar o crescimento sustentado. A sociedade de inovação deve estar disposta a crescer mais lentamente para garantir que o crescimento em questão é sustentável. Investir na segurança de plataformas será porventura essencial para garantir que para o crescimento em condições, não depende da vulnerabilidade face a maus actores, inimigos e acidentes.

Jonathan Zittrain, [citado por Kauffman (2011)], abordou este ponto com relação à Internet: argumenta ele que a natureza generativa da Internet tem dado origem a problemas de segurança que, se não forem tomadas medidas, ameaçam mover-nos longe de "generatividade", que ele considera talvez a principal virtude da Internet. [Kauffman (2011)].

As tecnologias destrutivas são praticamente inseparáveis das inovações socialmente benéficas que dão origem a elas. Nas mãos erradas, um estudo ou um programa sobre como proteger computadores contra vírus envolve necessariamente análise de um vírus, as suas vantagens e defeitos, e tal pode ser usado para criar melhores vírus.

A vulnerabilidade da infra-estrutura mundial de redes de telecomunicações está hoje, quase inteiramente, na mão de maiores ou menores intervenientes, que as usam em seu usufruto, e da restante sociedade global, mas cujos objectivos últimos poderão (e são frequentemente) transviados.

Por exemplo, a tecnologia militar Norte-americana depende em grande parte dos desenvolvimentos comerciais e privados de TI. De acordo com uma estimativa, 95 por cento de transferências de informação militar pelos EUA ocorre em redes "civis" e privadas. [ M. Antolin-Jenkins (2005), citado por Kauffman (2011)].

Estamos portanto num ponto em que a inovação progride aceleradamente e, essencialmente, através de canais desregulamentados, e inerentes a grandes e pequenos intervenientes, essencialmente privados, cuja qualidade da segurança não é inteiramente percebida, mas cuja responsabilidade, em caso de extravio, roubo de dados e patentes, etc., é muito limitada.

Em analogia, poderemos culpar a NASA pela queda de um foguetão se mais ninguém faz, se ninguém faz melhor? E se o cidadão comum não sabe como eles fazem? O mesmo se passa neste momento com o mundo da inovação no espaço da Internet. Existe uma dependência de toda a sociedade na qualidade e segurança que poucos intervenientes sabem e conseguem providenciar (confiamos nos resultados do motor de busca da Google, confiamos na segurança do *IPhone* e confiamos na ligação de internet da Vodafone). E todos os intervenientes são privados, com objectivos privados que, como tal, investirão na segurança só até ao ponto em que não transbordem casos para a opinião pública que manchem a sua reputação.

E mesmo quando existem casos de redes comprometidas, ou fugas de informação, escondem-se atrás do facto (verdadeiro, por sinal) de que pode acontecer a todos, e que o cibercrime é tremendamente evoluído.

Hipótese:

Quem são os principais *stakeholders* que podem contribuir para debelar este problema? Porventura os ISPs e os Governos? E poderão/ deverão ser responsabilizados?

### 4.2.1 Contexto Tecnológico

O contexto tecnológico que enquadra o problema, é simples na sua equação:

- As telecomunicações, telefónicas, moveis, e de internet são nucleares para todas as empresas. Assumir-se-á que sem a tecnologia, uma esmagadora parte das indústrias e serviços não existiriam ou definhariam à luz dos tempos modernos.
- As tecnologias informáticas e da comunicação são dotadas de uma complexidade extrema. O domínio destas tecnologias está reservado a um pequeno número de corporações. Estas corporações são responsáveis pelo fornecimento e gestão da tecnologia às restantes empresas e aos cidadãos (ao mundo inteiro).
- Outras empresas, dada a natureza das suas actividades, são altamente dependentes de serviços de internet e comunicações de qualidade e segurança.
- As comunicações, em especial as que lidam directamente com protocolos de internet, são passíveis de serem utilizadas para outros fins que não os legítimos. Consideremos a utilização legítima de internet como aquela que visa a inter-transmissão de dados, a descoberta e partilha de informação, a utilização de ferramentas e serviços informáticos, a transacção económica e financeira de bens e serviços.
- Os crimes informáticos (cibercrimes) e as variadas actividades mais ou menos ilícitas que os suportam (*malware*, tráfego de tecnologia e outros) usurpam propriedades de empresas e cidadãos (propriedade intelectual, económica, reputação) e, colateralmente, desequilibram os mercados criando e cimentando uma economia paralela de milhões de euros.

Preposição:

Assumiremos, com base nos pontos anteriores, a importância das tecnologias e comunicações informáticas. Assumiremos também que existe um impacto muito importante causado pela quebra de segurança nestas tecnologias.

## 4.3 Contexto financeiro

Para se ter uma noção melhor da dimensão do problema, seria interessante medir os efeitos do *malware* na vida social. A União Internacional de Telecomunicações (ITU) publicou um relatório abrangente nesta matéria. O relatório mede os efeitos de bem-estar total, face ao *malware*, considerando tanto os seus custos e suas receitas.

Uma versão resumida dos intervenientes e impacto apresenta-se de seguida:

| *Players* | Tipos de Impacto |
|---|---|
| **Custos** | |
| Utilizadores / Negócio (directos) | *Click fraud*<br>Fraude Financeira (extorsão, roubo)<br>Outras (Chantagem e resgates, perda de documentos relativos a trocas comerciais)<br>Pagamentos de compensação a Clientes |
| Utilizadores / Negócio (indirecto) | Custo das medidas preventivas (software, hardware, treino e educação)<br>Perda de produtividade (tempo a ler spam, utilização de outros meios de comunicação menos eficazes)<br>Perda de confiança do consumidor<br>Perda de reputação<br>Desperdício de recursos computacionais (ex. Largura de banda, tráfego, etc.) |
| Utilizadores individuais (directo) | Fraudes financeiras (incluindo fraudes de cartão de crédito)<br>Roubos de identidade e de dados financeiros<br>Adulteração de dados, estragos na reputação, personificação ilícita do utilizador, com impacto financeiro, económico e social<br>Custos com software de segurança, computadores |
| Sociedade (indirecto) | Mercado e transacções paralelas<br>Custos de segurança nacional<br>Custos na segurança, justiça<br>Custos de oportunidade de negócios na internet<br>Temor de segurança, desprestigiando os negócios e os intervenientes<br>Perda de qualidade de vida<br>Perda de proveitos do comércio online<br>Ataques na Infra-estrutura da Internet |
| **Proveitos** | |
| Providers de Segurança | Venda de produtos de segurança, software, serviços profissionais |
| Sociedade | Acesso a pirataria |
| Cibercriminosos | Ganhos financeiros (fraude, roubo, extorsão)<br>Ganhos financeiros de intermediários (aluguer de *bots*, ferramentas de *Hacking*, emails, identidades, etc.) |

Tabela 4-1 Impactos Financeiros do *malware [ITU (2009)]*

Preposição:

O Impacto económico é muito abrangente e com um potencial de causar danos graves. Em sentido lato, toda a sociedade é impactada, do lado dos custos.

## 4.4 Contexto Social e Económico

O que torna a Internet diferente é que esta propicia, muito facilmente, variadas formas de comunicação e de criatividade humanas.

As inovações mais importantes de comunicação estão indelevelmente associadas à Internet (email, a rede mundial, multimédia), quer directa, quer indirectamente, através da facilidade de colaboração e acesso a informação que esta possibilita.

Neste contexto, é possível argumentar que a Internet seja mais um fenómeno social do que tecnológico, pois suplementa as comunicações tradicionais e fornece novas formas de comunicação (por exemplo as comunidades online). Tais desenvolvimentos engendraram a dimensão sociocultural da Internet. E é precisamente esta dimensão sociocultural que contém as questões mais controversas no campo da Governação da Internet: desde políticas de conteúdo até direito ao anonimato e transacções virtuais, todas estas questões reflectem de modo muito particular as diferenças nacionais, religiosas e culturais hoje prevalecentes.

> *A U. S. Federal Trade Commission (FTC) – Consumer Network Data Book, registou mais de 1,3 milhões de reclamações dos consumidores para o ano de 2009. As queixas relacionadas com fraudes correspondem a 54% do total, estimando-se lesões no consumidor em mais de 1,7 Biliões de dólares (US). Destas 40% são fraudes relacionadas com cartões de crédito.*
>
> *Além disso, a FTC explica que em 70% dos casos, a fraude ocorre através de Internet e e-mail.*
>
> *[FTC (2009)]*

## Incentivos para a sociedade

| Incentivos no combate aos Botnets | | ISPS | Empresas | Governos |
|---|---|---|---|---|
| Peer pressure, interna e concorrencial | Vantagens sociais e económicas (directas e indirectas) | +++ | ++ | +++ |
| Manter *Brand Image* | | +++ | + | ++ |
| Pressão institucional: *Normas e valores internos* | | ? | ? | ++/+++ |
| Pressão institucional: *Leis e Regulamentos* | | +++ | ? | +++ |
| Custos de suporte a clientes e Abuse Management | Vantagens técnicas e financeiras (directas) | +++ | ++ | |
| Custos com soluções de segurança | | +++ | ++ | |
| Custos com expansão da intra-estrutura | | +++ | ++ | |

**Descrição**

**Em termos sociais, os Governos sentem a pressão dos seus valores (os valores de segurança dos cidadãos variam, em especial nos governos de base conservadora ou progressista. No que concerne a pressão de regulamentar, é muito elevada para os Governos, e elevada para os ISPs**

**A imagem corporativa, em especial se avaliada no mercado concorrencial, dos ISPs é muito importante quando correlacionada com a segurança. As empresas veem a sua imagem, em termos de segurança, associada aos países a que pertencem. Os países, por sua vez, concatenam estas duas entidades.**

**Em termos de vantagens técnicas, por motivos óbvios, a dimensão e a especialização das empresas é directamente proporcional aos custos que tentam minimizar**

Adaptação livre de Theoretical Framework ; Botnet Mitigation and the Role of ISPs (Asghari [2010])

Ilustração 4-1 Incentivos aos ISPs, relacionando com outras empresas e governos

### 4.4.1 Brand Management (e Reputação)

Em nenhum outro momento da história as sociedades globais estiveram tão próximas. As comunicações são globais, a informação é obtida em tempo real, e cada empresa tem presença na internet, directa e indirectamente, fruto da troca de informação, formal e/ou informal, que os milhares de fóruns e canais noticiosos permitem.

A gestão das marcas joga-se neste terreno vasto e perigoso.

A gestão da reputação online das marcas é um factor muito importante em organizações com um posicionamento, de marketing e/ou vendas. Se pensarmos no investimento que estas organizações fazem sobre este aspecto da sua reputação da marca, quer seja imiscuindo-se em blogs e fórums, quer seja veiculando adequadamente informações generosas sobre acções beneméritas, sustentabilidade e outros factos louváveis, e se admitirmos que a internet é um excepcional canal multicultural, universal, com uma capacidade avassaladora na produção de conteúdos e geração de ideias, perceberemos facilmente que qualquer tentativa de gestão de reputação, pelos meios tradicionais do marketing, terá um efeito reduzido ou mesmo contraproducente, se for deliberadamente ou inocentemente alterado. Significando isto que se uma organização não se proteger adequadamente dos detractores, incautos e criminosos, os mesmos (ou outros) canais que usa para se fortalecer, terão efeitos prejudiciais nefastos.

São inúmeros os casos de fugas de informação confidencial (vide inúmeros casos no site da empresa Wikileaks), rumores infundamentados com impactos graves na valorização das empresas (vide o caso do blog Engadget que, numa tarde, fez a Apple desvalorizar 3%, por causa de um email anónimo que furtivamente veio de um domínio da Apple), e muitos outros casos com impactos incríveis. A internet é volumosa, na velocidade e distribuição de informação e, para além de sofisticados sistemas de monitorização da reputação, as organizações devem focar-se no desvio e manipulação das mesmas [Beal, Strauss (2007)].

### 4.4.2 Globalização

Em contexto de Globalização, as Empresas são, em essência, transnacionais, desejando operar, com uma facilidade aproximada, em diversos países do mundo. Isto é obtido pela facilidade de comunicação (física e digital) e informação. É também obtido pela abertura das diversas economias mundiais a exportação e importação, sem dúvida o factor que mais impacta o equilíbrio (ou desequilíbrio) entre os diversos países.

Entre as diversas facetas da Globalização, estão:

- A utilização de recursos internacionais, nomeadamente em Outsourcing.
- A instalação física em diversos países, com os devidos benefícios (fiscais, sociais, de reputação) quer para as empresas "instaladoras", quer para os países que as albergam.
- A prospecção desses mercados com compras e vendas de produtos e serviços, sendo que o canal primordial para tal é a internet [Click, Duening (2005)].
- Todos os países têm vantagens e desvantagens para se imporem no mercado global.

Com base no mencionado anteriormente, vamos assumir que um país ter uma boa infra-estrutura e infoestrutura de comunicações e de internet é um factor considerável para um bom posicionamento enquanto país exportador e importador, de bens, serviços e recursos humanos.

### 4.4.3 A geografia e a Internet

Uma das suposições iniciais sobre a Internet era de que esta, dado o seu carácter global, iria transpor quaisquer fronteiras nacionais provocando a erosão do conceito de soberania.

Na sua célebre "Declaração de Independência do Ciberespaço", John Perry Barlow enviou a seguinte mensagem a todos os governos: "Vocês não são bem-vindos entre nós. Não exercem nenhuma soberania sobre o lugar onde nos reunimos... Vocês não têm o direito moral de nos impor regras e nem possuem quaisquer meios de coação que devêssemos temer de verdade... O ciberespaço não está dentro das vossas fronteiras."

Esta declaração é um exemplo do "tecno-optimismo" predominante, típico de meados dos anos 1990. Desde a declaração de Barlow, houve muitos desenvolvimentos, inclusive de programas de localização geográfica mais sofisticados.

Hoje, ainda é difícil identificar exactamente quem está atrás de um computador, mas é bastante simples identificar através de que ISP é que se acedeu à internet. Além disso, as leis nacionais mais recentes de muitos países, em especial no mundo ocidental, exigem que os ISPs identifiquem os seus utilizadores e que forneçam a informação necessária sobre eles às autoridades, sempre que estes tenham comportamentos criminosos.

Quanto mais a rede estiver ancorada na geografia, menos peculiar será a Governação da Internet. Por exemplo, com a possibilidade de localizar geograficamente os utilizadores a as transacções da Internet, a complexa questão da jurisdição sobre a Internet pode ser mais facilmente resolvida através das leis já existentes.

Uma prioridade seria dar assistência aos países em desenvolvimento a fim de viabilizar a sua participação significativa no processo de Governação da Internet.

Dispõe-se que a internet é verdadeiramente global e que os ISPs são os melhor posicionados para localizarem cada objecto (utilizador, website, rede, etc.).

### 4.4.4 Outsourcing

As tendências modernas de economias em escala que propagam a necessidade da focalização em qualidade (na óptica do consumidor), inovação e serviço, as "deseconomias" de complexidade, como refere Alvin Toffler, acabam por desembocar em estruturas corporativas onde os órgãos centrais assumem um papel de coordenação, havendo lugar á subcontratação (porque mais que ter as competências, importa ter-lhes acesso) [Cardoso (2008)].

O objectivo da empresa passa a ser o desenvolvimento, localizado, e adequado a necessidades que poderão ser temporariamente restritos ou restritivos. Neste caso, apresentar Portugal como um país plenamente adequado a que corporações estrangeiras façam evoluir as suas estruturas secundárias (sucursais, aproveitando acima de tudo as qualificações humanas e o "ambiente") será um factor diferenciador positivo e importante. Pensemos que recursos humanos mais informados (com melhor internet) contribuirão para isso e pensemos que um "ambiente" tecnológico mais seguro decerto também contribuirá para isso. Sendo que é aqui que entra a segurança e a qualidade dos sistemas de comunicações e internet.

<u>Assumpções:</u>

- Assumiremos, fruto dos parágrafos anteriores, que qualquer acontecimento com uma empresa tem capacidades excepcionais para se propagar na Internet como informação.
- Assumiremos também que, dada a natureza extremamente social e desregulada de todos os espaços que compõem a internet, a informação de e sobre determinada empresa, pode facilmente ser desviada, conotada, tornada ambígua.
- Noutro contexto assumiremos também que a internet se tenta auto-regular através da reputação das várias entidades, usando essa reputação para aferir o contacto e os privilégios dessas entidades dentro do ecossistema.
- Por fim assumiremos que o mundo deixou de estar tão dependente da localização física, sendo comum a deslocalização, as *ventures* e o outsourcing, desde que garantidas as comunicações.

## 4.5 Contexto Governativo e Legislativo

De forma a corroborar o problema exposto, faz-se notar a aprovação, pelo Conselho de Ministros de Portugal, em 21 de Julho de 2011, de uma proposta de lei que visa transpor para Portugal as recentes directivas comunitárias das comunicações electrónicas.

Esta transposição surgiu apenas dois dias depois da Comissão Europeia ter avançado com um processo de infracção contra Portugal pelo incumprimento nesta área, o que demonstra adequadamente a preocupação que este assunto sustenta.

A proposta de lei é mais abrangente e visa acima de tudo regular o sector de telecomunicações. Não obstante este facto, reconhece os seguintes eixos principais:

> - *O reforço de uma regulação independente e de uma acção reguladora que promova a inovação e o investimento;*
> - *O reconhecimento da gestão eficiente do espectro como vector fundamental de promoção de bem-estar e de desenvolvimento económico;*
> - *A consolidação do mercado interno, entre outros, através da criação do Organismo de Reguladores Europeus das Comunicações Electrónicas;*
> - *O fortalecimento da protecção dos consumidores de serviços de comunicações electrónicas, incluindo os utilizadores com deficiência;*
> - *E a promoção de comunicações seguras através do reforço da segurança e integridade das redes".*
>
> *Conselho de Ministros, República Portuguesa*

Podendo ser observado como a segurança, o bem-estar dos consumidores, a colaboração inter-comunitária e a percepção de que sustenta um progresso económico são os factores críticos que medeiam as preocupações governamentais, tanto Portuguesas como Europeias.

Portugal foi um dos últimos países da zona Euro a adoptar legislação conveniente. Outros países, nomeadamente a Alemanha e os EUA há muito que destinaram grande preocupação, e grandes investimentos, com a segurança online.

### 4.5.1 Direitos de Propriedade Intelectual

Os direitos de propriedade intelectual habilitam qualquer pessoa a desfrutar da protecção dos interesses morais e materiais resultantes de sua produção científica, literária ou artística.

Este direito é contrabalançado pelo direito de todos de participar livremente na vida cultural e de partilhar os avanços científicos.

Estabelecer um equilíbrio entre estas duas reivindicações é um dos maiores desafios da Governação da Internet.

Uma das características essenciais da Internet é que novos conhecimentos e informações são produzidas através da interacção mundial dos utilizadores.Conhecimentos consideráveis foram gerados através de intercâmbios em listas de correio, grupos de discussão e blogs. Em muitos casos, nenhum mecanismo internacional está disponível para proteger esses conhecimentos.

Deixado num vácuo legal, o conhecimento pode ser transformado em mercadoria e comercializado por particulares. Este viveiro de conhecimentos comuns, uma base importante de criatividade, corre assim o risco de ser esvaziado. Quanto mais a Internet for comercializada, menos espontâneos se tornarão seus intercâmbios. Isto pode levar a uma redução da interactividade criativa.

O conceito de bem público global visa promover soluções que também protegeriam o conhecimento comum da Internet para as gerações futuras.

### 4.5.2 "Ilegal offline – ilegal online"

Esta noção traz a discussão sobre o dilema entre mundo "real" e mundo "ciber". As regras existentes reais podem e devem ser implementadas na Internet (isto é frequentemente salientado no âmbito da União Europeia).

A Decisão-Quadro do Conselho da Europa sobre Combate ao Racismo e à Xenofobia indica explicitamente "o que é ilegal *offline* é ilegal *online*". Um dos argumentos da abordagem "ciber" da regulamentação da Internet é que a quantidade (volume de comunicação, número de mensagens) engendra uma diferença qualitativa. Segundo este ponto de vista, o problema dos discursos de ódio não é que nenhuma legislação tenha sido promulgada sobre estes, mas sim que seu volume e disseminação na Internet os tornam um tipo diferente de problema legal. Mais indivíduos são expostos e é difícil impor a observância das leis existentes. Consequentemente, a diferença que a Internet suscita relaciona-se principalmente com problemas de execução legal, não as regras ou leis.

### 4.5.3 Ciber vs. Mundo Real

O conceito de Bem Público Global pode ser vinculado a muitos aspectos da Governação da Internet. Os vínculos mais directos respeitam o acesso à infra-estrutura da Internet, da protecção ao conhecimento desenvolvido, da protecção das normas ou *standards* técnicos, e do acesso à educação online.

A infra-estrutura da Internet é predominantemente gerida por empresas privadas. Um dos desafios actuais é a harmonização da propriedade privada da Internet com a sua condição de bem público global.

Leis nacionais prevêem a possibilidade de restrições à propriedade privada se estas restrições forem motivadas por determinadas exigências públicas, inclusive prover direitos iguais a todos os utilizadores e evitar interferir nos conteúdos transportados.

Significa isto que, por exemplo, a implementação de leis que garantam a liberdade de opinião e de expressão, devem ser postas no contexto do estabelecimento de um equilíbrio adequado entre as duas necessidades.

Este regime ambíguo abre muitas possibilidades de interpretações diferentes das normas e, em última análise, de diferentes implementações.

A aplicação da lei online ainda não se compara à aplicação da lei tradicional (offline). E possivelmente nunca a equivalerá [Fertik, Thompson (2010)]. São milhares de criminosos, sem fronteiras geográficas, suportados por organizações com muito potencial nefasto (porque vislumbram a óptima relação proveito *versus* exposição) e inclusive por governos.

Talvez só mesmo o "diligentelismo" (vigilância, cooperação (entre cibernautas e mesmo empresas de segurança), utilizadores) [Fertik, Thompson (2010)], e as iniciativas de governos (democráticos) conseguirão restabelecer alguma ordem.

### 4.5.4 Proteger a Internet como bem público global

Algumas soluções baseadas no conceito da Internet como bem público global podem ser desenvolvidas a partir dos conceitos económicos e legais existentes.

Assim, por exemplo, a teoria económica propõe o apurado conceito de "bem público", que foi estendido ao âmbito internacional como "bem público global". O bem público tem duas propriedades que são cruciais: consumo não concorrencial e carácter não exclusivo. A primeira supõe que o consumo de um indivíduo não se dê em detrimento do consumo por outro; a segunda, que seja difícil, senão impossível, excluir um indivíduo de ter acesso a algo que lhe seja potencialmente benéfico.

Muitos concordam que o modelo para o desenvolvimento futuro da Internet vai depender do estabelecimento de um equilíbrio apropriado entre os interesses privados e o interesse público.

## 4.6 Perceber como o Problema abrange os ISPs

### 4.6.1 Contexto histórico

Os dados de Internet podem viajar através de uma gama diversificada de suportes: fios telefónicos, cabos de fibra óptica, satélites, microondas e conexões sem fio. Mesmo a rede eléctrica básica pode ser usada para retransmitir tráfego de Internet. O rápido crescimento da Internet desencadeou um aumento considerável da capacidade e abrangência de telecomunicações. Estima-se que, de 1998 para cá, a capacidade de telecomunicação tenha

crescido quinhentas vezes, devido a uma combinação de inovações tecnológicas e investimentos em novas instalações de telecomunicação [Bauer, Van Eeten (2008)].

Como a camada das telecomunicações suporta o tráfego da Internet, qualquer regulamentação nova vinculada à área das telecomunicações também terá impacto, inevitavelmente, na Internet. A infra-estrutura de telecomunicações é regulamentada tanto no nível nacional como internacional por uma variedade de organizações públicas e privadas.

Tradicionalmente, as telecomunicações internacionais eram coordenadas pela União Internacional de Telecomunicações (UIT), que desenvolveu regras elaboradas cobrindo a relação entre operadores nacionais, atribuição de gamas de rádio e gestão de posicionamento de satélites.

Eventualmente, a abordagem liberal prevaleceu sobre os monopólios das telecomunicações. O processo de liberalização foi formalizado internacionalmente em 1998, através do Acordo sobre Serviços Básicos de Telecomunicações (BTA) da Organização Mundial do Comércio (OMC), em cujos termos mais de cem países deram início a um processo de liberalização caracterizado pela privatização dos monopólios nacionais de telecomunicação, a introdução da competição e o estabelecimento de agências reguladoras nacionais.

A OMC moveu-se gradualmente para o centro do regime internacional de telecomunicações, tradicionalmente governado pela UIT. Contudo, os papéis da OMC e da UIT são totalmente distintos. A UIT define padrões técnicos detalhados, regulamentos internacionais específicos da área das telecomunicações, e também dá assistência a países em desenvolvimento. A OMC provê um quadro de regras gerais de mercado.

Depois da liberalização, o quase monopólio da UIT, como principal instituição definidora de padrões para as telecomunicações, foi erodido por outros órgãos e organizações profissionais, como a Instituto Europeu de Padronização das Telecomunicações (ETSI), que desenvolveu padrões GSM, e o Instituto de Engenheiros Electricistas e Electrónicos (IEEE), que desenvolveu o TCP/IP e outros protocolos relativos à Internet.

A liberalização dos mercados nacionais de telecomunicação deu às grandes companhias de telecomunicações, como AT&T, Cable and Wireless, France Telecom, Sprint e WorldCom, a oportunidade de estender globalmente a sua cobertura de mercado. Como a maior parte do tráfego é suportado pelas infra-estruturas de telecomunicações dessas companhias, elas têm grande influência nos processos da Governação da Internet.

### 4.6.2 Os ISPs

Dos intervenientes no processo, os ISPs são provavelmente os melhores posicionados para suportar os utilizadores, detectando e "desinfectando" as redes e computadores infectados. Afinal, e em última instância, os ISPs são quem providencia o acesso tecnológico à internet. Esta responsabilidade é clara e o cenário natural seria que os ISPs, com o seu *know-how* técnico, e com o distintivo de guardiões dos portões de acesso ao mundo virtual assumissem a gestão deste assunto.

Existem, não obstante, algumas variáveis que poderão inviabilizar este cenário:

- Os ISPs operam em mercados altamente competitivos e de constante evolução. Os custos com sistemas de segurança são elevados, implicam manutenção muito exigente e o reforço do investimento ocorre normalmente em espaços temporais muito curtos, devido à evolução natural da tecnologia (e dos problemas de segurança).

- Um utilizador de um ISP é, acima de tudo, um cliente, que paga pelo serviço e espera qualidade condizente, quer com o preço, quer com os standards normais de mercado. Ao detectar que um cliente está infectado com uma *botnet*, o ISP não terá outra solução senão tentar impedir que o *botnet* se propague e/ou ataque. Algumas vezes isso significará cortar ou abrandar a ligação do cliente, total ou parcialmente. Existem implicações legais, mas especialmente contratuais e de qualidade de serviço, quando se faz isto a um utilizador. Até por este aspecto, seria importante uma corroboração estatal, uma autorização (ou melhor uma legislação), que sustentasse estas acções de mitigação, sem prejudicar o ISP.
- Outra variável, directamente relacionada com a anterior é o chamado problema de "Killing the Messenger", ou seja, se um ISP activamente avisa um cliente que este está infectado, o cliente reclama contra o ISP, por desconhecimento tecnológico e/ou porque esperava uma qualidade de serviço que tivesse evitado que tal sucedesse. Ou porque poderá sentir que a sua privacidade foi violada (O ISP, para detectar um utilizador infectado teve, sem outra opção, que monitorizar o tráfego deste). Normalmente esta situação é complicada de gerir do ponto de vista legal e não é fora do comum alguns ISPs evitarem estes sistemas ou, se os tiverem, evitarem avisar o cliente.

Estes tipos de problemas reprimem naturalmente um ISP nas suas intenções.

Acima de tudo, e mais que eventuais questões financeiras, as questões relacionadas com a sociedade e os seus legalismos tradicionais (o dever de fornecer um serviço a cliente; o dever de respeitar a privacidade do cliente) esbatem nos "não-legalismos" do mercado pouco regulamentado da Internet (Não existe nenhuma lei mundial que advogue o dever das entidade privadas se esforçarem por mitigar o cibercrime).

Existem outros problemas, de natureza técnica, que também dificultam o combate ao *malware*, em especial a sua variante mais letal, as *botnets* (que servem como porta-aviões para lançar todos os outros tipos de *malware*):

Eis um exemplo:

Os ISPs possuem gamas de endereços IPs. Estas gamas/ redes, por serem limitadas, também para evitar outros problemas de segurança e ainda para distribuir a reputação das redes IPs o mais equitativamente possível, são atribuídas provisoriamente e alternadamente aos clientes. Este factor, inultrapassável pelo menos nos próximos tempos, implica que existem dificuldades em descobrir, quando se monitoriza uma rede, quem foi, de facto o cliente humano a que corresponde determinado endereço. Mesmo tendo os *timestamps* (os períodos de tempo em que se detectou a infecção) e verificando os mesmos com a atribuição do IP. Isto sucede porque nem sempre é possível recuperar a informação no meio de milhões de dados de registo (de "log") que ocorrem em curtos espaços de tempo.

Este e outros problemas técnicos, para além dos problemas mencionados anteriormente, são a causa de muitos ISPs e Operadores negligenciarem o seu dever de informarem os clientes no caso de infecção. Limitam-se a guardar os dados de actividade por seis meses, conforme a legislação vigente (Directiva 2006/24/EC).

**Porque é que os ISPs estão no centro do Furacão**

Para além do óbvio facto que os ISPs e Operadores são responsáveis pelas telecomunicações da quase totalidade dos cidadãos e empresas, existem factores acrescidos que potenciam que os criminosos usufruam da capacidade dos ISPs:

Os utilizadores alternam os seus IPs e tal permite que a reputação desses IPs habitualmente seja imaculada. Dessa forma, infectar um cliente subscritor de uma ligação de comunicações de um ISP (seja móvel, Banda larga ou outra) garante, com alguma razoabilidade, que o *botnet* poderá comunicar livremente. Num cenário em que o criminoso utilizasse uma comunicação privada, facilmente, algures na internet, algum sistema de segurança detectaria uma actividade criminosa (por exemplo o envio massivo de spam) e catalogaria a rede numa das muitas listas de Reputação (públicas e privadas, da qual "submetem e bebem informação" muitos sistemas de segurança).

As listas de reputação são, como referido ao longo deste documento, uma peça fundamental, não só no combate à insegurança das comunicações, mas também na própria gestão da actividade de todos os intervenientes: os ISPs precisam de ter boa reputação (para que os clientes comuniquem livremente) e os cibercriminosos usufruem dessa boa reputação, para fazer proliferar as suas comunicações (criminosas) livremente.

**Por que é que os spammers usam ISPs de email?**

Nota: Na definição, anteriormente assumida, de que os ISP são mencionados no seu sentido mais lato, ou seja, Internet Service Providers, Telcos, Carriers e basicamente todo o tipo de empresas que fornecem total ou parcialmente, serviços de telecomunicações e acesso à internet, convém agora destacar um tipo de operação, comum a estas empresas: a função de ESPs (Email Service Providers) cujo caso particular reflecte fielmente a natureza global do problema.

Um cibercriminoso/ spammer que se dedique ao envio de spam, utilizando *botnets*, poderia porventura criar um servidor de SMTP (o protocolo do correio electrónico) ao invés de usufruir das infra-estruturas das empresas ligadas ao fornecimento de serviços de email.

Uma vez mais, a Reputação surge como o motivo principal, neste caso a variados níveis:

Um ISP alberga, na sua estrutura um número variável de organizações, entre as quais ESPs que utilizam a rede para enviar emails. (como exemplo, a Google - Gmail - envia o email do Utilizador X através….do serviço de comunicações que o Utilizador X estiver a usar). Como o email utiliza um protocolo e porto de acesso diferentes, o ISP consegue detectar o serviço em causa como sendo de envio de email (e não de comunicação móvel ou utilização do protocolo http ("de websites"), por exemplo).

É muito comum que um ISP destine determinada largura de banda (restringida) para o envio de email (para o porto 25 de SMTP, normalmente) e para outras comunicações especiais nesse porto. Por outro lado, para um cliente ESP, já terá de conceder um serviço de qualidade (que o *spammer* aproveita) [Bauer, Van Eeten (2008)].

Um *spammer* terá decerto os seus endereços (de IP, de DNS, etc.) listados numa qualquer lista de reputação, impedindo-o de, em muitos casos, conseguir entregar o spam. Mas um ESP, pela dimensão, tem outros privilégios, e outra reputação (normalmente medíocre, fruto de muitos utilizadores "bons" e muitos utilizadores "maus", mas suficiente para a maioria das situações). Em princípio, apesar de por vezes com alguns atrasos (deliberados pelos ISPs, em alguns casos), dificilmente algum destinatário rejeitará um email vindo do Hotmail ou do Yahoo, por falta de reputação adequada.

A importância das listas de reputação, para o caso particular do email atingiu uma tal dimensão elevada que é legítima a probabilidade de, num futuro próximo, não estar bem cotado e/ou identificado implica a presunção automática de culpa da entidade em questão.

A vantagem, mencionada anteriormente, do ESP ter uma maior largura de banda disponível, possibilita que um email de spam seja enviado para vários destinatários em simultâneo, multiplicando o alcance do (eventual) dano.

Outro factor prende-se com a colocação de um nível intermédio, dificultando por definição, a capacidade do ISP monitorizar e detectar o *spammer*, tendo para isso que interferir no espaço do ESP.

O outro factor para a utilização dos ESPs é ainda mais tecnológico: A robustez dos sistemas e da infra-estrutura, a redundância (uns equipamentos substituem outros quando falham, mantendo o sistema funcional) e os mecanismos de controlo, em especial na verificação que os endereços de destino existem, minimiza o desperdício no envio de email (de spam, *Phishing, Whaling*, etc.). Considerando que normalmente, na comunicação, o spam só é detectado pelo volume anormal que produz, isto é uma vantagem.

Esta lógica tecnológica é, de certo modo, um pouco contrastante. Se um ESP tem obviamente mais recursos que um utilizador singular, para o envio de spam, também teremos que considerar que normalmente estes serviços ou são gratuitos ou são oferecidos como gratuitos em "bundles" de serviços pagos (exemplos do Gmail, Sapo, MSN, etc.). Tal significa que o investimento em segurança pode ser descurado em detrimento do investimento em comunicação. Em especial no mundo altamente competitivo dos serviços de internet, em que todos procuram uma notoriedade que os permita angariar clientes, ignorando (por vezes propositadamente) se estes pretendem dedicar-se a ilícitos, não é fora do comum que alguns ESPs se predisponham abertamente a albergar os *spammers*, por ganância ou má gestão.

Duas importantes ilações poderão ser extraídas dos parágrafos anteriores:

- A colaboração ao longo da cadeia de fornecimento de serviços é um factor primordial para que se impeça a proliferação das actividades criminosas.
- A monitorização de diferentes protocolos e a aplicação de listas de reputação são necessários para alcançar os *spammers*. Ao SMTP devem aliar protocolos de internet, como IP/DNS que permitam monitorizar os ESPs.

**A situação actual nos ISPs**

Em geral, os ISPs levam a sério o desafio de segurança nas telecomunicações.

É um desafio de gestão em curso, que tem ramificações importantes para a retenção de clientes, e isso impõe custos para o prestador. É, em traços gerais, um processo de negócio que actualmente tem uma eficácia aceitável.

Uma das conclusões mais importantes é que pouco mudou ao longo dos últimos anos. A maioria das medidas é aplicada em proporções semelhantes de fornecedores para o que foi observado em 2007. Mesmo a utilização de mecanismos de autenticação de remetente permanece aproximadamente o mesmo [ENISA (2009)].

> *Aos olhos dos ISPs, ao longo dos últimos anos, as ameaças têm assumido duas formas proeminentes: o spam que chega aos clientes (que por sua vez contém ou desencadeia outro tipo de malware) e os acessos livres a websites de internet contaminados.*
>
> *[Damballa (2008)]*

Perante estes factores, a maioria dos ISPs já implementaram ou têm planos para implementar novas medidas, tais como listas negras, *Web firewalls (*filtragem no acesso a websites), *greylisting* (um método para perceber se o remetente de email é spam), DKIM (uma gestão criptográfica da entrega de mensagens), e gestão de porta 25 (alterar os portos de entrega dos mails).

Assim, e embora os níveis de propagação de ameaças, com destaque para o spam, se tenham mantido ou aumentado, graças a estas variadas medidas, os ISPs são frequentemente capazes de ajustar ou actualizar as suas medidas para garantir que eles permanecem eficazes.

Esses resultados, sugerem que a prevenção de spam atingiu uma espécie de equilíbrio, em que esforços substanciais são necessários para gerir spam, mas os desafios e as contra medidas são geralmente bem compreendidas. As contra medidas são eficazes, quando geridas e actualizadas correctamente, tão pouco grandes mudanças parecem ser necessárias.

Existe contudo uma opinião generalizada, entre os ISPs, que a prevenção de *malware* e spam não é apenas uma questão de proteger os clientes de *spammers* externos. É premente a necessidade de uma abordagem coordenada contra o spam e o *malware*, e uma parte fundamental depende dos próprios fornecedores que obviamente têm *spammers* e criminosos entre os seus próprios clientes [Asghari (2010)].

### 4.6.3 Medidas actualmente nos ISPs

**Anti-Spam**

Quanto à detecção, quase todos os fornecedores de sistemas de segurança revelam que a maneira mais comum de fazer isso é por filtragem do tráfego, aplicando regras e heurísticas para determinar se o email é spam ou legítimo. Medidas mais pró-activas, não tão amplamente utilizadas, incluem a monitorização de picos de tráfego, bem como análises em tempo real de anomalias de tráfego ou métodos de detecção baseados em assinaturas.

Para a prevenção de spam, as listas negras eram a medida mais comummente usada para impedir o envio de spam, bem como limitar altos volumes de correio de saída (*Outbound rate limit*). Outras medidas incluem a execução de antivírus de saída e gestão ou bloqueio da porta de acesso 25 (a porta frequentemente utilizada para email).

Uma filtragem efectiva possui efectivamente gestão de listas negras, filtragem de conteúdo e autenticação de remetente.

Na autenticação do remetente, SMTP AUTH é o método de autenticação do remetente dominante, com SMTP TLS e SPF também utilizados. Mas métodos de Autenticação por DKIM têm aumentado significativamente (*ndr*: isto são tudo métodos técnicos para tentar verificar a origem de uma comunicação).

Depois de detecção de spam, a maioria dos fornecedores adopta uma abordagem colaborativa: tendem a entrar em contacto com o provedor dos serviços (ISP), e só bloquear conexões SMTP, ou endereços IP, se o ISP não resolver o problema.

**A gestão de reputação**

As listas negras e as bases de dados de reputação são das medidas mais comuns. As fontes dessas bases de dados variam. Muitos dos fornecedores usam as suas próprias bases de dados, compiladas através dos sistemas de Anti-Spam, mas um número superior utilizará bases de dados de reputação específicas, comerciais ou *opensource*.

"Confiabilidade" de listas negras: Como as listas negras ("blacklists", na designação universal) são tão importantes no bloqueio de spam, o seu grau de confiabilidade é crucial. No entanto, é muito comum, entre todos os maiores fornecedores, afirmarem que tiveram os seus servidores adicionados à lista negra (ou retidos incorrectamente. Após estas ocorrências, verificaram que é geralmente difícil ter o problema resolvido, pois é preciso comprovar a legitimidade das redes).

**A detecção de *botnets***

> *Um cálculo preciso da quantidade de actividade bot é dificultada pela sua natureza em todo o mundo, no entanto, entre 1.000 e 2.000 diferentes servidores activos de Comando e Controlo (C&C) são conhecidos (instalados e a funcionar todos os dias); cada C&C tem uma média de 20.000 computadores infectados (bots): alguns servidores C&C podem gerir apenas poucos computadores infectados (~ 10), mas os grandes podem gerir milhares de bots (~ 300.000).*
>
> *[Damballa (2008)]*

Baseado em estudos anteriores, sabemos que os ISPs enfrentam dois conjuntos de custos no que diz respeito aos assinantes infectados. Eles têm incentivos para tomar alguma acção contra *bots* (para evitar os custos de estarem em listas negras, perdendo reciprocidade, etc.), mas não querem tomar acções a mais (para evitar custos de chamadas de clientes, a responsabilidade legal, etc.).

Para equilibrar estes custos, a maioria dos ISPs decidir tomar medidas apenas contra os *bots* mais agressivos em suas redes. Isto implica que os ISPs divergem sobre o grau de vigilância contra *bots* - com base em pontos fortes e pontos fracos dos seus diversos incentivos.

Um estudo científico (Asghari, [2010]) antecipou um conjunto hipóteses empíricas e estatisticamente testadas. A análise dos dados foi realizada em duas etapas: um teste individual de hipótese, complementado por uma análise de regressão multivariada. O conjunto de dados final contém 741 casos, representando quatro anos de observações para o desempenho de segurança de 200 Fornecedores. Estes são os principais ISPs que operam em 40 países do alargamento da OCDE. As principais conclusões dos testes de hipótese são as seguintes:

- Os resultados fornecem evidências convincentes de que os ISPs são, na verdade o ponto focal na mitigação de *botnets*: cerca de 200 Fornecedores de internet respondem por 80% das infecções *bot* nesses países, e por outras palavras, o grosso do problema está concentrado dentro de um pequeno número de agentes económicos.
- Os ISPs diferem significativamente em relação ao nível de" actividade *botnet*" que ocorre nas suas redes.
- Outra constatação importante é que a contagem de assinantes está negativamente associado aos níveis de actividade *botnet*. Isto contradiz a crença comum de que os maiores ISPs têm pior desempenho em termos de segurança.
- Curiosamente, os Fornecedores de cabo têm uma performance melhor do que os Fornecedores de DSL - em média, infecções por *bot* 10% menores. (Algumas razões para isso poderiam ser o uso dos sistemas existentes de monitorização de tráfego em redes, devido à infra-estrutura de banda larga partilhada. Alternativamente, poderia ser devido à possibilidade de imporem políticas mais rígidas de rede, visto que eles normalmente têm uma grande base de assinantes residenciais).

- Outros resultados incluem descobrir que a taxa de pirataria está positivamente associada aos níveis de actividade *botnet*.

Ao pesquisar as implicações políticas dessas descobertas, e entre os factores investigados, o mais promissor é que a regulamentação específica parece ser eficaz; e o facto de que os maiores ISPs e Fornecedores de cabo têm níveis mais baixos de actividade *botnet* (quando correlacionados com o tamanho destes).

No entanto, as questões críticas que precisam de ser respondidas é se no contexto mais amplo da situação da cibersegurança os ISPs devem ser feitos parcialmente responsáveis por atenuar os efeitos das *botnets* – sim, os cibercriminosos estão nas suas redes, mas não, os ISPs não são polícias e não terão "jurisdição" para impedir crimes. E se não forem os ISPs a ser responsabilizados quem deveria ser, visto que ninguém possui a capacidade (a infra-estrutura) para debelar o problema.

Tecnicamente, *Botnets* podem ser detectadas, e existe uma variedade de abordagens:

Ao nível dos ISPs, alguns produtos permitem analisar consultas DNS para detectar se um computador foi infectado por códigos maliciosos. Embora esta abordagem pareça ser válida, a verdade é que pode ser muito útil mas não é a solução derradeira: Analisando o tráfego DNS para detectar computadores zombie que estão tentando conectar-se ao seu C&C só é útil se o C&C já for conhecido (da mesma forma que as assinaturas de intrusão baseadas em software de detecção ou de anti-vírus também precisam de ter um registo de que o tráfego é conhecido por ser mau), mas:

- Análise de tráfego DNS não detecta C&C desconhecidos.
- Alguns C&C conectam-se directamente a um IP em vez do nome de domínio.
- Alguns C&C são hospedados em computadores comprometidos com um nome de domínio autêntico, e tido como "bom".

Então, a fim de detectar tráfego *botnet*, de forma semelhante aos anti-vírus ou aos sistemas de detecção e de intrusão, os ISPs têm necessidade de combinar vários métodos baseados em listas de reputação, heurísticas e outros, como por exemplo, um método baseado em fluxos (por exemplo, os humanos não conseguem enviar 10 mails por segundo, e se um computador o estiver a fazer, tem um *bot* a fazê-lo pelo utilizador) [Bauer, Van Eeten (2008)].

Ao nível da rede também é possível fazer algo: como muitos *worms* tentam infectar computadores próximos, numa rede local (LAN), um *honeypot* local (um sistema de computadores que funciona como uma armadilha para os atacantes) pode ajudar na detecção precoce de qualquer software malicioso que está tentando infectar todos os computadores de uma organização. Neste âmbito, administradores locais desempenham um papel chave, uma vez que podem detectar uma infecção e tomar a acção apropriada

Ao nível do computador: existem algumas dicas de como o código malicioso é executado num computador:

- Estranhos nomes de processo.
- A ligação lenta à Internet (o computador pode estar a servir para o envio de spam ou participar num Ataque DDoS).
- Comportamento estranho do browser (alterar a home page, novas janelas que aparecem, etc.).
- Software Anti-vírus que parece não estar em execução.

- Nomes de pastas estranhos e programa adicionados misteriosamente à lista de programas que têm permissão para acesso Internet.
- Alterações na pasta *hosts* do computador.
- Pastas estranhas nos programas de inicialização.
- Objectos novos (*plugins* e *add-ons)*, acrescentados aos browsers, ou a outros programas.
- Conexões de rede desconhecidas, estabelecidas no computador.

Não obstante a lista supra mencionada, as *botnets* mais avançadas conseguem estar activas sem que nenhum dos sinais se produza. E para além desse facto, com a quantidade diferente de sistemas operativos, programas, browsers, e especialmente utilizadores (no grau de conhecimento e/ou nos cuidados de manutenção dos seus computadores), a abordagem "endpoint" (ao nível do utilizador) é bastante ineficiente [Pivotal Veracity (2009)].

Conclusão

Existem medidas, a ser implementadas em diversos ISPs, ou pelo menos conhecidas no meio, que debelam com maior ou menor sucesso alguns dos problemas. É do conhecimento comum que soluções instaladas na rede, ao invés de no endpoint (nos computadores clientes), podem produzir maior impacto.

Alguns países e iniciativas privadas já deram os primeiros passos face a esta situação, conforme é comprovado adiante neste documento.

## 4.7 Perceber como o problema pode ser explorado por Portugal

O sentimento de segurança na internet, é passível de ser estendido a outros vectores importantes de uma sociedade que se quer competitiva em todos os âmbitos possíveis, em especial os que lidam com a percepção que um cidadão cria acerca de um país, a sua capacidade, os benefícios que poderá extrair, o quão seguro se sentiria nesse país, e o quão fácil seria integrar-se e ambientar-se socialmente, inter-relacionáveis.

S e encararmos que os mercados mais sofisticados (aqueles com a melhor reputação) acabam por funcionar como mercados aspiracionais, marcando as tendências (Da Silva [2010]) e estipulando o que é *hot* e o que é *not*, um cenário hipotético onde Portugal se posicionasse na linha da frente em termos de segurança e reputação de internet, seria também um cenário onde Portugal seria apreciado pela sua capacidade técnica podendo estabelecer paradigmas de qualidade aos quais associaria as suas empresas e os seus produtos. E, como ironia do destino, que melhor canal de informação para propagar as qualidades dos produtos do que a internet, precisamente o ecossistema onde Portugal seria um dos países que mais assertivamente distribuiria a informação (sendo que aqui se deve interpretar que este asserto se refere a eliminação de impurezas, desinformação de carácter ilícito, spam, etc.) e não uma tentativa de sufocar a liberdade de expressão na internet.

A segurança de Portugal (ou como Portugal é um país seguro) pode, assim, ser entendida num espectro mais alargado: Portugal é, da Europa, um dos poucos países considerados pacíficos, benevolentes, e muito estáveis. Tentando emular o pensamento comum da sociedade:

- Portugal carece das ideologias extremistas (e respectivos incidentes, como os atentados de Oslo, em Julho 2011, ou os tiroteios de Helsínquia, em Junho de 2011) dos países Escandinavos. Estes problemas, naturalmente que afectarão a estabilidade social do país, para além de estarem algumas vezes relacionados com temas como a xenofobia e o repúdio a estrangeiros.
- Portugal carece dos problemas com independentistas internos, como a Irlanda ou a Espanha. Uma vez mais, estes problemas indiciam instabilidade social.
- Os problemas de imigração dos italianos e franceses são menos relevantes em Portugal. Estes problemas, obviamente, incutam dificuldades para os trabalhadores estrangeiros nesses países.
- Existe uma noção de corrupção abundante nos países dos Balcãs. Claramente estes indicadores inibem empreendimentos externos de procurarem estes países, pois decerto que antevêem impedimentos em termos de mercados livres e imparciais.
- A adulteração democrática percepcionada na Rússia, noutros países da ex-cortina de ferro, e países com uma base comunista muito forte (China, Coreia). Uma vez mais, a falta de rigor e transparência inibe o empreendimento externo legítimo.

Conclusão

Portugal é percepcionado, em suma, como um pacato país, estável e estabilizado há muitos anos.

Decerto não será a preocupação "top-of-mind" dos investidores estrangeiros, mas a ponderação que alguns tomam, em especial em indústrias mais sensíveis ao ambiente social, como sejam Bancos e Seguradoras, Indústrias tecnológicas, e outras, implica que a segurança poderá ser um factor diferenciador na altura de decidir o país a investir ou onde procurar outsourcing.

Um governo deverá ter, como prioridade, a segurança à maior extensão possível. Ainda que no caso português, a legislação e a sociedade tornem Portugal uma nação muito rígida ("tight power"), mas ainda assim HNO positiva (Human Nature Orientation – Negative) – onde as leis assumem que as pessoas obedecerão às mesmas, este factor repete-se em todos os países da Europa [Hennessey et al *(2011*)].

# *5* Revisão da Literatura: A Reputação online

## 5.1 O Problema da Reputação

A Reputação permite aos utilizadores e aos serviços criar uma expectativa de comportamento baseadas em juízos, muitas vezes tomando como referência os juízos de terceira parte. Existe obviamente um benefício significativo, dos pontos de vista económico e social em ser capaz de se confiar em pessoas (e em comunicações) que não se conhece directamente.

A Reputação electrónica é um benefício tão valioso como a reputação tradicional, na medida em que todo o tipo de comunicações assentam em listas /acumulações de reputação, próprias ou de terceiros, que costumam ser escrupulosamente tidas em consideração na hora de, por exemplo, aceitar uma ligação de rede, um email, ou um post do Facebook [Wilson (2009)].

As mais recentes aplicações na internet são todas baseadas em reputação, quer para gestão de risco, quer mesmo para determinar a veracidade da informação transmitida. E nesse sentido, a reputação torna-se extremamente valiosa. E, naturalmente, adulterar ou arruinar determinada reputação, quer de pessoas singulares, quer de pessoas colectivas (até mesmo governos) tem impactos significativos, essencialmente no mundo virtual mas que, pelo impacto da velocíssima transferência de informação na sociedade moderna, extravasa normalmente para o mundo real.

Sempre que se "vai" à internet, encontra-se conteúdo escrito por cidadãos comuns, anónimos (o que a indústria chama de User Created Content). E é esta dinâmica que baseou a génese da Web 2.0 (outro jargão, que significa, entre outras coisas, a democracia, a liberdade e a facilidade com que qualquer utilizador pode criar, comentar, e interferir, na internet). Mas, tal como na vida real, um universo excepcionalmente grande e prodigioso, fundado na desregulamentação, eventualmente necessitará de regulamentação.

Poderá ser pouco democrático moderar fóruns e bloquear conteúdos (uma realidade cada vez mais evidente na Web 2.0) [Fertik, Thompson (2010)]. Mas o conteúdo ofensivo e os ataques à reputação são uma realidade que vai para além de uma qualquer luta de galos. Trata-se da reputação, às vezes de um cidadão, muitas vezes de uma empresa ou um partido político. E disponível para "todo o mundo assistir e tomar partido".

### 5.1.1 "Reputation Hijacking"

O termo *Reputation Hijacking* (sequestro de reputação) continua a obter notoriedade, pelas piores razões, nas diversas comunidades, especialmente de segurança Anti-*malware* e na imprensa.

É um termo destinado a descrever quando um *spammer* utiliza outros recursos, com melhor reputação, para as suas actividades ilícitas. Normalmente os visados são os grandes

Fornecedores de email. A ideia por detrás deste esquema é que ao fazer isso, eles estão "sequestrando" a reputação de IPs do provedor de email em vez de arriscar a própria reputação de IPs que, com actividade contínua e/ou dependendo da proveniência (normalmente países com fraca reputação online, como a Rússia ou a Índia) se tende a degradar, impedindo-os de penetrar nos sistemas que usam RBLs (listas de reputação) para filtrar (ou pelo menos condicionar) o tráfego.

Desde muito cedo que os *spammers* perceberam que poderiam ter servidores dedicados - e que trabalhassem por algum tempo – utilizando outros servidores que não os seus, porque cedo a comunidade de segurança detectava padrões de actividades. A partir desse momento, os *spammers* sentiram a necessidade de se mover para novos IPs, constantemente, antes que os anteriores fossem "blacklisted". Na verdade, foi esta situação que levou ao surgimento das *botnets*: ter computadores de cidadãos comuns a lançar o spam. Quando o tal cidadão comum fica com a reputação afectada, é só passar ao próximo cidadão comum (isto não é problema, visto que as *botnets* são tentaculares, e com a capacidade de infectar simultaneamente milhares de computadores).

### 5.1.2 Manipulação de Search engines

A Gestão da Reputação Online (ORM) funciona de uma maneira bastante simples: influenciar o fluxo de dados e notícias na internet de modo a acentuar os pontos positivos e dando a impressão de aprovações massiva; e por outro lado, desvalorizando os pontos negativos, e dando a impressão que os opinantes são um pequeno grupo com interesses obscuros.

Embora possam efectivamente salvar reputações, algumas das técnicas utilizadas são controversas e balançam na fronteira da legalidade.

Uma reputação na internet é gerida cuidadosamente com o objectivo de promover a imagem desejada do cliente. Este processo abrange as páginas de resultado dos Search Engines (SERP), sites de notícias, blogs, redes sociais, streaming de media e relações públicas em sites.

A gestão dos comentários online tornou-se cada vez mais importante para empresas e profissionais: uma pesquisa de 2009 conduzida pela Opinion Research Corporation concluiu que *"(...) 84 por cento dos americanos dizem que as avaliações de clientes na internet têm uma influência decisiva sobre a sua decisão de comprar um produto ou serviço".*
As empresas que utilizam ORM geralmente empregam uma estratégia similar: pesquisando on-line tudo e qualquer coisa sobre o cliente, apresentando essa informação ao cliente, para posteriormente determinarem o que deve ser suprimido, alterado ou enfatizado.

Na fase de limpeza, os gestores de ORM removem o nome do cliente nas buscas de pessoas e empresas, removem itens (como os arquivos enviados), encerrando de contas, e mesmo entrando em contacto com responsáveis de sites e canais noticiosos, ameaçando com litígios.

A segunda fase concentra-se em criar e moldar uma presença online desejada para o cliente. Uma técnica particularmente usada é o Search Engine Games (um termo que descreve a manipulação dos algoritmos de um motor de busca, a fim de obter posições ideais SERP), algo similar a Search Engine Optimization (SEO). Há uma série de técnicas de SEO legítimas

tais como a optimização das páginas de internet, a utilização de Pay Per Click (PPC), ou apenas ter conteúdo realmente popular.

Depois haverá outras técnicas, como "influenciar" opinantes especialmente famosos, ou atacar judicialmente sites e empresas com poder na reputação.

Como exemplo, a famosa empresa de listas de reputação Spamhaus sofre anualmente muitas litigações, por terceiras partes, por colocar websites como mau reputados nas suas listas (que são usadas por muitos ISPs, Bancos e afins); estes processos costumam ser infrutíferos, mas enquanto duram, a má reputação fica suspensa, o que é suficiente para a notícia desvanecer, ou para o website continuar a produzir conteúdo impróprio ou ilegal.

### 5.1.3 Como a desintermediação afecta a reputação

Comentários de clientes satisfeitos e insatisfeitos aparecem em milhões de websites. Pesquisas sobre "revisões de produtos por consumidores" produzem no Google mais de 73 milhões de resultados. E alguns sites solicitam especificamente queixas e comentários negativos, como por exemplo, o Pissed Consumer [Kabay, M.E (2011)].

Websites que alimentam comentários não confirmados sobre pessoas, produtos e empresas, poderão causar falsidades. Ainda que acreditemos que o poder das multidões tendencialmente apontará para as respostas certas, também não será menos verdade que muitas pessoas utilizam estes meios, muitas vezes anónimos, para publicar opiniões essencialmente negativas, e pouco polidas. Também existirão pessoas muito influenciadoras e outras muito influenciáveis. E no final, certamente existem indivíduos, que denigrem uma empresa para fazer vingar outra, ou denigrem uma pessoa, por vingança, para extorsão, e muitas outras actividades criminosas.

Como poderão as vítimas de campanhas de difamação superar a publicidade negativa? O Digital Millennium Copyright Act (DMCA) aplica severas multas por violações de direitos de autor, mas esbarram frequentemente quando o assunto é calúnia. Torna-se muito dispendioso quando, para se remover material calunioso, é preciso recorrer a acções judiciais. Para mais quando em muitos websites, os gestores destes recusam assumir responsabilidades pelos comentários que aí são efectuados.

Poderíamos ainda perguntar como os consumidores conseguem evitar a manipulação por especialistas de informações (positivas ou negativas) na internet, no âmbito de SEO?

Se uma organização assumir a responsabilidade pelo conteúdo de seu website, a vítima pode exigir a remoção de material calunioso, e se esse pedido for recusado, processar os proprietários ou outros responsáveis por perdas e danos (mas tal é muito incomum).

Estes são exemplos de como a desintermediação, ou a falta de responsabilidade sobre informação que, tem pertença, se torna um problema grave, nos termos quer da reputação online, quer mesmo dos cibercrimes.

Organizações que não exercem qualquer controlo sobre conteúdo que vive nos seus websites e/ou nas suas redes, organizações que declinam explicitamente responsabilidades, não serão mais que portadores ou distribuidores de informação, não deixando mais ninguém para resolver o problema senão comentadores que assinam com o nome verdadeiro, ou criminosos que divulgam a sua autoria num qualquer website de pirataria e/ou vírus (muito improvável).

Cada vez mais se levantam vozes a favor da teoria "Kill the Messenger", atacando os ISPs, os donos dos fóruns, e até mesmo os países, por se manterem absolutamente neutrais, no que concerne ilícitos de terceiros, nas suas propriedades.

### 5.1.4 Características de um sistema electrónico visando a reputação

As principais características de sistemas electrónicos de reputação, compreendidos como relacionados com segurança trazem inúmeros benefícios no âmbito de aplicações e serviços electrónicos.

As quatro variantes mais comuns, em termos de aplicações são: redes sociais, mercados online, redes P2P (Peer-to-peer), o Anti-Spam, e a Web-of-trust (sistemas de autenticação com chave pública). Reside nestes pontos as maiores vulnerabilidades à reputação.

A reputação, nos sistemas acima mencionados é medida tal e qual a reputação entre cidadãos, no mundo "real": consiste na opinião agregada que pessoas, no geral, têm sobre alguém ou a respeito de algo, ou quanta admiração alguém ou alguma coisa recebe, e isto com base no comportamento ou carácter passados. A reputação incorpora uma expectativa sobre um comportamento baseado em informações ou observações do historial de determinada pessoa ou sistema.

**Confiança e reputação**

Confiança e reputação estão fortemente relacionadas pois a reputação permite confiar. Confiança normalmente existe a um nível pessoal, onde a opinião pessoal pesa mais do que a opinião dos outros, ao passo que a reputação expressa a opinião colectiva, conduzindo a confiança ou desconfiança, que emerge como o resultado de opiniões de membros de uma determinada comunidade.

Deste modo, para esta reputação fortemente sedimenta sobre uma componente de "contexto social" é muito importante analisar implicações de segurança. A reputação é um mecanismo para convivência. É um mecanismo de psicologia social que é usado como uma entrada para uma heurística que determinará uma decisão sobre "confiabilidade", um indicador escalável para avaliar relação risco / transacção dentro de uma comunidade alargada.

Existe de facto um benefício económico significativo em ser capaz de se confiar em pessoas que não se conhece pessoalmente (estranhos). As opiniões que usamos para construir a confiança em estranhos muitas vezes provêm de outros estranhos. Felizmente que os contactos online, sendo mais numerosos, mais distribuídos e com maior frequência (do que contactos *offline*) têm também um carácter de desprendimento e anonimato, significando isto tudo que a maioria das pessoas, quando fornece determinado feedback, fá-lo honestamente. E, de qualquer modo, os principais sistemas de reputação resultam de métricas e agregação de variáveis que são compiladas mecanicamente, reduzindo a subjectividade humana (rankings e estatísticas, como por exemplo o número de vírus detectado por um sistema, provenientes de Portugal).

Quanto à reputação induzida por humanos, há evidências que sugerem que, sob certas circunstâncias, a tomada de decisão de grupo pode chegar a surpreendentemente bons resultados.

Tudo isto resulta num importante mecanismo de gestão e avaliação, usado por sistemas empresariais, para fornecer uma importante ajuda na tomada de decisão sobre se se deve confiar em algo ou alguém, e isto de uma forma que é semelhante à forma como interagimos na sociedade.

**A reputação como gestão de risco**

A Reputação é normalmente considerada como pertencente à segurança "leve" ("Soft security"). E por esse facto é advogado o uso de controlos sociais para criar e proteger os sistemas abertos, que não dependem de autoridades globais, mas que dependem dos participantes interagindo entre si. Embora a segurança rígida ("Hard security") (por exemplo, autenticação com base em criptografia) não permita que invasores penetrem em sistemas, excepto se estes contornarem o sistema, uma abordagem de "soft security", usando reputação, tem uma capacidade muito mais preventiva, pois monitoriza e restringe invasores com base em comportamentos passados (suspeitos).

Mais: A reputação tendencialmente incentiva o bom comportamento (Sendo a boa reputação muito valiosa, um utilizador fará, geralmente, por comportar-se bem). Por outro lado a má reputação é anunciada entre sistemas e um mau comportamento em determinado local (um website, por exemplo) facilmente implica o bloqueio no acesso a outros locais.

Afectar seriamente a reputação de uma organização requer, muitas vezes, muito mais que o lançamento de um boato falso (existem muitos na internet, no entanto). O nível cultural neste meio é relativamente elevado e é requerida muita consistência. E é neste ponto que a (gestão da) reputação online adquire a sua importância mais crítica: a informação que afecta a reputação é muitas vezes obtida por malware (que entra nos sistemas e rouba informação) por extorsão (trocas de informação) e, se se tratar de rumores falsos, por actividades de personificação (como penetrar na conta de email de alguém e enviar um email em seu nome) [Fertik, Thompson (2010)].

## 5.2 Objectivos e modelos dos Sistemas de Reputação

Existem vários sistemas baseados em reputação disponíveis. E os principais objectivos / motivos para sistemas de reputação serem usados numa rede de entidades que interagem umas com as outras são:

- Fornecer informações para ajudar a avaliar se uma entidade é confiável ("trust evaluation").
- Incentivar as entidades a comportarem-se de forma confiável.
- Desencorajar interacções suspeitas entre entidades.
- Auxiliar na procura de novos conhecimentos e recursos consultando entidades confiáveis como fontes ("e-Discovery").

Reputação é uma opinião formada sobre a base de informações agregadas. Este informação agregada geralmente inclui as história da entidade (comportamento passado) que é relatado devido a:

- Conhecimento directo: a opinião directa do entidade avaliadora, quando disponível, por exemplo formada a partir de operações anteriores, ou de observações directas de certos factores.
- Conhecimento indirecto: as opiniões que os outros formulam sobre a determinada entidade.

A reputação é dependente do contexto: por exemplo, alguém com uma boa reputação para vender laptops pode ter uma má reputação vendendo automóveis. Resumindo: a reputação precisa de ser confinada ao perfil /contexto ao qual é aplicada (o vendedor de laptops versus o vendedor de carros). No entanto, as semelhanças entre os contextos /perfis podem ser explorados para aferir a sensibilidade da reputação quando reutilizada em contextos similares.

A matéria-prima fundamental que baseia uma reputação é um conjunto de votos ou opiniões sobre os atributos da entidade (É mesmo ele? Ele é um vendedor de confiança? É X do chave pública de Y? Como correu a transacção económica? Quanta largura de banda consumiu esta entidade?).

Estas aferições são então combinadas usando mais ou menos algoritmos sofisticados para produzir uma pontuação agregada de reputação. As formas como os votos são combinados para calcular a pontuação total (o algoritmo de métricas) são tipicamente diferentes de acordo com a aplicação. A métrica escolhida pode ser simples (por exemplo, a média de concatenação, ou somatório das pontuações individuais) ou complexas (por exemplo, podem ser usadas ponderações).

Quanto mais complexa a métrica, o mais difícil pode ser para um utilizador do sistema entender o real significado da pontuação de reputação. Para além do mais, a métrica em si pode ser um ponto de falha do sistema, uma vez que pode estar sujeita a ataques.

O sistema de incentivos / punição é uma importante componente para um sistema baseado em reputação. Incentivos e recompensas incentivam uma entidade a comportar-se de maneira confiável, a fim de adquirir, manter ou aumentar a sua reputação ao invés de beneficiar de um castigo apropriado, (baixar a reputação de uma pessoa proibindo-a de frequentar uma comunidade) é necessário para desencorajar o mau comportamento, e/ou encorajar a reabilitação.

Para manter uma reputação resistente a ataques, em geral, o valor da punição tem que ser maior do que o ganho potencial de se tentar contornar o sistema.

### 5.2.1 Modelos de avaliação da reputação

São consagrados três principais modelos de avaliação de reputação: subjectivos, objectivos e híbridos.

**Sistemas de reputação subjectiva**

- Sistemas da reputação subjectiva baseiam-se principalmente nas informações fornecidas dentro de uma comunidade controlada de utilizadores - e onde a

comunidade tem finalidades bem definidas, como a venda bens, a partilha de conteúdo, de conhecimento ou de opiniões -.

- O prestador de serviços à comunidade desempenha um papel fundamental na gestão da reputação do sistema, e tanto o prestador como o próprio sistema de reputação têm uma reputação associadas.
- Os utilizadores, na sua interacção, categorizam outros utilizadores por meio de medidas subjectivos, normalmente de carácter psicológico.
- Interacções, cumprimentos e educação, aspirações, promessas e acordos são, habitualmente os mecanismos de comunicação que permitem aferir determinada opinião. São obviamente muito falíveis, havendo, no entanto, consensos alargados em situações mais óbvias. Por exemplo, alguém que num fórum esgrime argumentos de forma rude, será catalogado por um conjunto alargado de utilizadores como tal, podendo, em virtude disso, ser negado de aceder a determinados conteúdos.
- Noutro exemplo, um utilizador pode considerar um email interessante que outros consideram spam, e ele pode até mesmo mudar de ideias no decorrer do dia

**Sistemas de reputação objectiva**

- A reputação do prestador de serviços ou a reputação do sistema requer evidência factual da sua qualidade (e rankings de comparação entre outros serviços), com base em métricas bem definidas e critérios repetíveis. O indivíduo pode aplicar algum tipo de análise subjectiva a determinados dados para obter a sua avaliação pessoal da reputação (e partilhar com outros utilizadores), mas se esses dados forem sustentados por métricas e por sistemas de avaliação credíveis, restará então o senso comum para uma correcta avaliação do sistema e/ou dos utilizadores.
- Por exemplo relatórios, análise baseada em métricas e critérios científicos, a taxa de bit rate de um servidor de *streaming* de vídeo, entre outros, são componentes que, em especial se existir uma amostra de comparação, servem para categorizar a avaliação de um website. Por exemplo a taxa de *uptime* de um website, em comparação com outros, é uma métrica que afere eficientemente a qualidade do serviço.

**Sistemas de reputação híbridos**

- Sistemas de reputação híbridos são uma combinação de sistemas objectivos e subjectivos.
- Normalmente, estes sistemas são baseados em sistemas de reputação objectiva, onde os resultados factuais são interpretados com base em valores subjectivos, pessoais ou motivacionais.
- Como exemplo, supomos que um produto chinês obteve uma óptima votação numa comunidade virtual, mas que devido à nacionalidade do mesmo, as pessoas tendem a desvalorizar, dada a dimensão da população do país de origem.

### 5.2.2 Principais modelos de estrutura de Sistemas baseados em reputação

Sistemas de reputação normalmente apresentam um dos dois principais modelos de estrutura (sendo que um compromisso entre estes dois modelos também é possível):

**Modelo centralizado**

- No modelo centralizado uma autoridade central recolhe pontos de reputação (de outras entidades e usando outras fontes, tais como a sua própria observação), e normalmente processa-os para formar uma pontuação de reputação agregada para uma determinada entidade.
- Posteriormente, redistribui esta reputação para ser utilizada por outras entidades.
- Comércio on-line e comunidades de mercado podem usar este modelo. Mas este modelo assume especial importância na gestão da rede por parte dos ISPs. Listas de reputação de IPs, ou utilizadores servem para activar os sistemas de Antivírus e de anti-spam.
- Mercados on-line (como o eBay ou a Amazon) estão entre os exemplos mais conhecidos de aplicações que fazem uso de reputação de sistemas centralizada, neste caso híbrida, sobre os vendedores.

**Modelo descentralizado**

- No modelo descentralizado as entidades participantes da comunidade divulgam, partilham e contribuem com informações, sem a necessidade de um repositório central.
- Este modelo é mais adequado para redes que são descentralizadas por natureza, tais como *peer-to-peer* e sistemas autónomos.
- Valores diferentes para a confiança surgem de diferentes fontes de reputação.
- Estes modelos são muito habituais em fóruns e em blogs.

## 5.3 Ameaças à Reputação

### 5.3.1 PseudoSpoofing

No ataque de *pseudospoofing*, o atacante cria várias identidades (sibilas) e explora-as, a fim de manipular uma pontuação de reputação. Por exemplo, múltiplas identidades podem ser usadas para fornecer reputação positiva a uma designada identidade, cuja reputação aumenta de forma mentirosa.

Ao montar um ataque de *pseudospoofing* (também conhecido como “Sybil attack”), o atacante inscreve-se em múltiplas contas, que podem ser usadas, ou para atribuir reputação umas às outras, ou para distribuir a actividade criminosa ( um milhão de contas a lançar um email é mais difícil de detectar do que uma conta a lançar um milhão de emails, pois não se detecta o comportamento robótico).

Enquanto em ambientes centralizados, uma correspondência one-to-one entre entidades pode ser assegurada pela autoridade central, o ataque de *pseudospooffing* é bastante eficaz em ambientes descentralizados, pois inúmeras contas com inúmeras interacções são muito difíceis de correlacionar, em especial se existirem deficiências na forma como as entidades permitem feedback.

As contra medidas existentes contra este tipo de ataque, visam tornar o ataque inútil. Pode-se por exemplo criar um 'preço' ou "Taxa de entrada" na criação de contas, ou, mais comum, criar desafios só resolúveis por humanos, como por exemplo a existência de uma operação que envolva algum tempo, um *Captcha* (introduzir texto escondido numa imagem, para

atestar que é mesmo um humano a digitar), uma operação de vários passos (exemplo: irá receber um email com a confirmação e o link para activar a conta), ou mesmo a resolução de um quebra-cabeças.

Para diminuir a probabilidade das pontuações adulteradas, enviadas em massa, é possível pedir um feedback à reputação dada, ou uma descrição mais aprofundada.

### 5.3.2 Representação, Roubo de reputação e Spoofing

Uma entidade adquire ilicitamente a identidade de outra entidade e, consequentemente rouba a reputação.

Poderá existir um duplo objectivo por parte do atacante: beneficiar da boa reputação roubada e/ou difamar a reputação adquirida. No caso do anti-spam, por exemplo, um invasor pode representar um utilizador legítimo por falsificação de seu endereço de email, conseguindo entregar com sucesso spam e /ou fazendo falsas recomendações e /ou mesmo enviando mensagens erróneas no nome do anterior (e verdadeiro) dono da identidade (*Spoofing*).

Entidades com grande reputação são mais propensas a ser vítimas de um ataque de Representação.

A responsabilidade de mitigar este problema recai sobre o sistema subjacente, que precisa de mecanismos para proteger a infra-estrutura de identidade.

### 5.3.3 Bootstrap

A "questão bootstrap 'está relacionada com o valor inicial dado à reputação de um recém-chegado que ainda não construiu qualquer reputação. A escolha deste valor de entrada não é trivial: Uma opção de design pode ser o prémio de confiança para o recém-chegado, até que ele se comporte mal, no entanto isso pode incentivar a que entidades criminosas tentem a mudança de identidade regularmente (a abertura do caminho para o ataque de *pseudospoofing* e de Representação)

Outra opção é fazer o recém-chegado ter de trabalhar para construir a sua reputação. Tal aumentaria o seu desejo de preservar a sua identidade e reputação, no entanto ele seria inicialmente penalizado e poderia desencorajar. Isto é o que tem sido chamado de "o custo social de pseudónimos ".

Outra proposta é o compromisso de deixar que pares estabelecidos no sistema possam emprestar parte de sua reputação a um recém-chegado.

O “recomendador” coloca a sua reputação em risco em virtude de “ser fiador” do recém-chegado. Para que tal funcione, deverá ser recompensado/ prejudicado em consonância com o comportamento de recém-chegado.

### 5.3.4 Extorsão

A ameaça de extorsão é realizado em ataques coordenados destinados a chantagear um

Individuo, com objectivos de prejudicar a sua reputação, reabilitar uma reputação anteriormente "manchada" de forma a obter um lucro ilícito ou outros motivos mal-intencionados.

Por exemplo, a negação de reputação (ver abaixo) pode impedir a vítima de, por exemplo entrar numa rede, ou fazer uma transacção bancária. A vítima é, então, chantageada, a fim de limpar a sua reputação.

Noutros casos, quando um utilizador deixa uma pontuação negativa sobre um sistema, o administrador ou moderador do sistema poderá forçar este utilizador a reconsiderar, usufruindo da sua condição de administrador ou moderador, para expulsar o utilizador.

Uma variante de extorsão consiste no contrário: envolver-se com um vendedor com alta reputação (e que por isso vende muito) e depois chantageá-lo com a ameaça de deixá-lo com um feedback negativo.

Por medo de retaliação, os utilizadores tendem a não expressar feedback negativo. Por exemplo, existem relatos que apontam como o feedback sobre os vendedores do eBay é irrealisticamente positivo, em especial não havendo uma alta correlação entre o comprador e o vendedor.

Há uma gama completa de danos potenciais que essa ameaça pode causar: danos emocionais para indivíduos vulneráveis ("cyberbullying"); um aumento nas actividades criminosas; danos à reputação, perda de receita para as identidades gestoras; perda de confiança nos julgamentos de reputação julgamentos e "spill-over" para eventos do mundo físico (por exemplo, a revelação dos dados privados relativos ao contrato comercial, ou a organização de bullying físico). As vulnerabilidades que esta ameaça pode explorar incluem a falta de gestão formal / e a falta de garantia de mecanismos para a reputação.

### 5.3.5 Denial of reputation

Negação de reputação consiste numa campanha concertada para prejudicar a reputação de uma entidade, a fim de isolar a vítima - efectivamente realizando uma, muitas vezes com a intenção de extorquir. A Negação de reputação é realizada habitualmente por falsas denúncias sobre a vítima. (Por *mouthing*, *pseudospoofing*, conluio, etc.) ou roubando a identidade da vítima e forçando que a sua reputação seja corrompida.

Então, a vítima é chantageada (extorsão), para ter a sua reputação limpa.

### 5.3.6 Badmouth

Badmouth, como o nome indica, é uma variação que consiste numa conspiração, entre utilizadores, para adulterar uma pontuação de reputação. Em escrutínio, um número de utilizadores concordam (por conluio, ou usando *pseudospoofing*) dar feedback positivo a uma entidade, para fazê-la rapidamente ganhar uma boa reputação ou, analogamente, os utilizadores conspiram para dar um feedback negativo sobre a vítima, para diminuir ou destruir sua reputação, ou para perpetuar a negação de reputação. Geralmente estes ataques são condicionados na sua eficácia devido a razões estatísticas [Fertik, Thompson (2010)].

Conluio significa que vários utilizadores conspiram (Conluio) para influenciar a classificação de dada a reputação.

Os utilizadores em conluio, podem ser coniventes para certificar uma chave pública.

### 5.3.7 Repúdio de Dados e Repúdio da transacção

Uma entidade pode negar que uma transacção aconteceu, ou a existência de dados os quais foi responsável.

Embora seja mais fácil de implementar uma verificação para apurar a transacção em sistemas centralizados, em sistemas descentralizados este problema é mais aparente.

A Replicação de dados para múltiplas entidades é uma técnica de mitigação adoptada, habitualmente, em redes P2P (Peer-to-peer, de partilha de ficheiros). O mais comum é serem solicitadas ou auto-geradas e expedidas provas de transacção.

### 5.3.8 Recomendação de Desonestidade

O problema de reputação relatado é fortemente dependente de "confiabilidade" no fornecimento de reputação. Por exemplo, um membro já existente recomenda alguém que não é confiável e o novo membro então prossegue com a sua actividade ilícita. Estas acções são reforçadas por conluios para chantagem. Exemplo: vinte utilizadores recomendam um utilizador fantasma e a única coisa que lhes acontece é uma pequena quebra na sua reputação.

### 5.3.9 Ameaças de Privacidade para Eleitores e Proprietários de Reputação

Dar uma opinião honesta sobre um tema delicado exige que a privacidade seja garantida ao utilizador/eleitor.

A situação é semelhante ao e-voto (voto electrónico), onde o proprietário reputação tem um forte incentivo para tentar influenciar o resultado, tanto através da ameaça directa aos eleitores como por outros meios de influência injusta.

Se a privacidade dos eleitores não for garantida, há um risco de distorcer os votos devido ao medo, e outras ameaças (por exemplo, extorsão ou retaliação, principalmente quando o feedback negativo é a acção que despoleta).

Da mesma forma, há ameaças contra a privacidade dos proprietários ou gestores da reputação. Esta ameaça à privacidade está presente, por exemplo, no mercado on-line, onde o proprietário do sistema coordena e permite ou proíbe a geração de utilizadores e composição de perfis.

### 5.3.10 Risco de comportamento em rebanho e Penalização de Inovadores e opiniões controversas

Opiniões inovadoras que desafiam o status quo são fundamentais para o progresso da sociedade. No entanto, propor algo novo, muitas vezes resulta em ser criticado pela grande maioria que desconsidera uma opinião como aceitável. Este "medo de rejeição" pode resultar numa abstenção de comentar.

Fornecendo mais anonimato aos eleitores podem ajudar a mitigar esta ameaça.

Outra possível medida preventiva é permitir que o cálculo de pontos de reputação personalizado por meio de métricas de confiança local, de modo que um utilizador possa ter conversas de âmbito local sem que isso afecte a reputação global. Ou seja, alguém propõe algo que não é actualmente aceite pela comunidade inteira), mas esse alguém pode conseguir ter um nível muito elevado de reputação junto de um restrito número de utilizadores (seu círculo de confiança). E , apesar da disparidade dos votos, o sistema interpreta as tendências comuns, diluindo a quebra da reputação [Wilson (2011)].

### 5.3.11 Efeito Minority Vocal

Em determinado ambientes sociais, quanto maior a reputação de alguém, mais importância tem a sua votação sobre outras entidades. E, se se considerar que os votos com capacidade disruptiva só podem ser obtidos a partir de pessoas com reputações fortes, a reputação pode ser distorcida pelo facto de que aqueles com opiniões moderadas têm votos de pouca influência.

Isto leva a imprecisões na reputação.

### 5.3.12 Comportamento discriminatório

Uma entidade pode envolver-se em comportamentos discriminatórios em relação aos outros. Por exemplo, nos sistemas de reputação de segunda ordem (ou seja, aqueles em que pesa o grau de "confiabilidade" de outras entidades), uma entidade pode optar por cooperar exclusivamente com os parceiros que têm uma reputação elevada (e cujas avaliações sejam positivas e influentes), conseguindo uma reputação falaciosamente elevada, e simultaneamente adoptando discriminações. Por exemplo, um utilizador pode transaccionar legitimamente com determinados websites de elevada reputação que lhe garantam uma boa reputação, propagada para outros websites onde irá conduzir actividades ilícitas.

### 5.3.13 Ameaças a Ratings

Há toda uma gama de ameaças às avaliações que medeiam uma reputação no que concerne as métricas utilizadas pelo sistema para calcular a classificação de reputação agregada de a pontuação única dada ao recomendando.

Estas ameaças incluem, entre outros:

- Ameaças contra o armazenamento seguro de classificações de reputação. Num sistema centralizado, o repositório central é o ponto único de falha. Num sistema descentralizado, os dados de reputação são replicados em diferentes pontos da rede. As medidas de segurança devem acompanhar estes locais, para além de assegurar que as redes básicas (de acesso, de aplicação) não são também comprometidas.
- Ameaças contra a distribuição segura de avaliações (transporte seguro), incluindo a modificação e reprodução de reputação, perda de mensagens acidentais (por exemplo, através de ataques a redes subjacentes),
- Ameaças à confidencialidade / privacidade de pontuação e ameaças contra a privacidade dos eleitores.

- Ameaças à linearidade de avaliações, por exemplo, determinando como uma combinação linear de ratings podem estar sujeita a ataques indetectáveis. Em alguns casos, algoritmos não-lineares são utilizados para a classificação, sendo o cálculo complexo e seu resultado imprevisível, se bem explorado.
  A pontuação da reputação pode originar diversos ataques, e é em geral importante um bom design da pontuação.
  Ameaças à Robustez do bom ou mau comportamento esporádico, potenciando o risco de sobrecarga num nó com uma boa reputação

### 5.3.14 Ameaças a DNS e SMTP

O DNS foi um dos primeiros protocolos criados para a Internet, quando ainda ninguém previa a dimensão que esta viria a ter. A infra-estrutura hierárquica e distribuída do DNS e o seu modo de funcionamento foram pensados para tornar este serviço resistente e ágil.

Por outro lado, o protocolo não previu, na sua génese, a possibilidade de manuseamento das respostas DNS de forma a impedir o aproveitamento malicioso da sua função. Este facto torna-se perigoso porque a quase totalidade das aplicações que usam o DNS como ferramenta de suporte confiam na autenticidade e veracidade da resposta obtida.

Finalmente, por possuir uma estrutura de gestão altamente distribuída, onde participam, literalmente, milhares de entidades e indivíduos, o DNS é vulnerável, em vários dos seus componentes, a situações de aproveitamento ilícito.

Neste contexto, é natural que o DNS seja um alvo de eleição para ataques de negação de serviço ou seja utilizado como ferramenta de suporte a todo o tipo de actividade maliciosa, tais como ataques de amplificação, *DNS cache poisoning*, *fast-flux* ou outros.

Importa referir que o DNS pode ser explorado de várias formas para, directa ou indirectamente, potenciar um ataque informático:

**Ataques em Topologia ou Distribuídos (DDoS)**

Um ataque de negação de serviço, como o próprio nome indica, visa interferir e causar uma disfunção no bom funcionamento de um serviço. No caso do serviço de DNS, o vector de ataque mais utilizado consiste no envio de um número elevado de perguntas recursivas, a um ou mais servidores de DNS, provocando desta forma um esgotamento de recursos como a largura de banda disponível, espaço de memória ou capacidade de processamento no servidor. Como consequência deste esgotamento de recursos obtêm-se a degradação do serviço DNS ou mesmo o seu total colapso. A inexistência de um servidor DNS operacional implica a indisponibilidade de todas as aplicações e serviços dele dependente.

Os ataques podem tentar explorar relações de confiança entre os membros da comunidade. O ataque pode ser direccionado para um determinado alvo que, se quebrado (por exemplo, por DDoS), teria o efeito máximo (como a enfraquecer ou matar a comunidade).

O atacante pode investigar também entidades que têm as maiores classificações de reputação e atacá-los, visto que as suas recomendações têm o maior impacto.

Para além destes ataques à raiz da hierarquia de DNS, existem vários casos de ataques dirigidos a esta ou aquela entidade. O caso mais famoso e mediático teve como principal interveniente Michael “Mafiaboy” Calce, um canadiano de apenas quinze anos, que em Fevereiro de 2000, desencadeou inúmeros ataques de negação de serviço contra os sistemas da Amazon, Ebay, Yahoo!, CNN e Dell.

**Envenenamento da cache**

Os servidores de *cache* são usados para acelerar o funcionamento global do serviço DNS.

De uma forma genérica, qualquer resposta a perguntas DNS é armazenada no servidor de *cache* e as posteriores consultas ao mesmo nome DNS são respondidas directamente pelo servidor de *cache* com a informação entretanto armazenada. Um conjunto de fragilidades conhecidas no protocolo DNS ou em implementações deste, assim como o forte crescimento da largura de banda disponível, permite que um indivíduo motivado possa, com uma grande probabilidade de sucesso, injectar informação errónea (RR falsos) num qualquer servidor de *cache*.

Para isso, basta que o atacante envie, ao servidor de *cache* alvo, o maior número de respostas falsas que a sua ligação à Internet permite. A resposta falsa – composta por um RR indicando um endereço IP sob o seu controlo – é aceite e armazenada no servidor de *cache* se coincidir com a pergunta recursiva, num determinado conjunto de elementos. Parte desses elementos são conhecidos do atacante, nomeadamente a pergunta DNS ou o endereço IP do servidor DNS do qual é esperada a resposta. A outra parte tem que ser adivinhada pelo atacante. Possuindo uma boa ligação à Internet, através da qual possam ser enviadas milhares de respostas falsas por segundo, o atacante tem uma elevada probabilidade de acertar, antes que a resposta verdadeira chegue ao servidor de *cache*, com a componente por si desconhecida.

Esta técnica é normalmente usada como método preparatório para outro tipo de ataques. Uma vez consumado o envenenamento, o atacante usa o seu servidor *web* (o endereço IP indicado na resposta falsa) para efectuar, entre outros, ataques de *phishing* ou disseminar *malware*.

**Sequestro de zona**

O sequestro de uma zona DNS faz-se atacando directamente ou utilizando credenciais para o serviço em linha de gestão de delegação de zonas, obtidas ilicitamente, serviço este prestado pelo *registry* ou pelo *registar* do domínio. Os ataques ao serviço de gestão exploram vulnerabilidades nos sistemas e aplicações usadas nesta função. O atacante pode igualmente obter, utilizando técnicas de engenharia social, credenciais válidas para acesso ao serviço de gestão (utilizando por exemplo a informação pública recolhida previamente).

Uma vez dentro do serviço em linha, o atacante pode alterar os endereços IP dos servidores primários e secundários para o domínio alvo, redireccionando-os para servidores sob sua administração. Controlando a zona DNS, o atacante pode efectuar um conjunto de actividades maliciosas tais como distribuição de *malware*, *phishing* ou envio de spam.

# 6 Research Design: *Case studies* de Iniciativas Governamentais Internacionais

## 6.1 O que está a ser feito actualmente

*Botnets* são redes de computadores comuns, silenciosamente, sequestradas por organizações criminosas. Estas são a arma dos cibercriminosos para atentados graves ameaçando a economia da Europa e a privacidade dos seus cidadãos – as *botnets* e o *malware* - compreendem o spam, a extorsão, a negação de serviço, roubo de identidade e exploração por motivos políticos, entre muitos outros perigos.

A perda total global anual é estimada em mais de 7.000 milhões euros, só na Europa [ENISA (2010)].

**O que está a ser feito?**

Existem várias iniciativas promissoras, no âmbito europeu, e implementadas a nível nacional, incluindo, por exemplo:

- *Bot*-Frei: uma parceria dos ISPs alemães e o Estado, que detecta e notifica os clientes infectados e fornece assistência de desinfecção, incluindo uma linha de apoio.
- O tratado anti-*botnet* Holandês: uma parceria de 14 ISPs holandeses e a Telecom Regulatory Authority (OPTA), abrangendo 98% do mercado holandês.
- O programa dinamarquês MoU - um quadro de cooperação entre ISPs e o CERT.
- O estudo e respectivo esforço adjacente, suecos, sobre *botnets* na Suécia.

A nível europeu, a ENISA publicou recentemente os resultados de uma ampla consulta a todos os sectores envolvidos na luta contra o *botnets*. Tal tem sido encaminhado no âmbito da Parceria Público Privada Europeia para a Resiliência (EP3R), que neste momento, planeia uma iniciativa europeia para combater *botnets* com base em iniciativas nacionais da UE e com o objectivo de reforçar a cooperação entre os ISPs Europeus, as autoridades nacionais e os parceiros relevantes.

O grupo de trabalho da OCDE sobre Segurança da Informação e Privacidade (WPISP) está actualmente a analisar o papel dos Fornecedores no combate *botnets*. Vários documentos suportam que a luta contra *botnets* é uma das prioridades da UE.

### 6.1.1 Quais são as opções para os governos europeus?

As *Botnets* têm muitas semelhanças com epidemias de saúde, que requerem um esforço conjunto e concertado. A Europa explora a oportunidade que consiste em aproveitar as iniciativas de sucesso já em funcionamento nos diversos países europeus com o objectivo de:

- Estimular o compromisso dos principais intervenientes nacionais (ISPs, os produtores de software, empresas de segurança, as autoridades públicas, etc.) para unir forças para erradicar a *botnets*, em particular, através da Parceria Público Privada Europeia para a Resiliência (EP3R) e das Autoridades nacionais de telecomunicações.
- Fornecer um quadro político abrangente, incluindo incentivos adequados, legislação de apoio e meios técnicos adequados para que os ISPs, os utilizadores finais, pesquisadores e produtores de software sejam capazes de desenvolver e implementar medidas eficazes de defesa.

## 6.2 O caso da Alemanha

A Iniciativa Anti-*botnet* Alemã foi despoletada pela associação alemã do sector de Internet (ECO) em 08 de Dezembro de 2009, sendo uma iniciativa da indústria privada destinada a apoiar os cidadãos na protecção dos seus sistemas de TI. O objectivo da iniciativa é garantir que os clientes cujos computadores pessoais se tornaram parte de uma *botnet* sem que eles estejam conscientes, sejam informados pelos seus Fornecedores de telecomunicações e, ao mesmo tempo, lhes seja dado apoio competente na remoção do *malware*. O Governo alemão Federal acolheu e apoiou a iniciativa como um exemplo de sucesso da responsabilidade assumida pelo sector privado para fortalecer toda a sociedade.

**Breve descrição**

O conceito é a construção de um centro de apoio central da Alemanha que consiste num website de ajuda ao utilizador com suporte por email e telefónico. Com a ajuda deste *helpdesk*, os utilizadores de Internet cujos PCs foram "alienados" por *malware* e fazem parte de uma *botnet*, quando tal foi confirmado pelo seu acesso à Internet, poderão ter o apoio necessário para se "desinfectarem".

Os Fornecedores podem desinfectar os computadores dos clientes, utilizando as ferramentas oferecidas on-line e obtendo o apoio de um assistente de *helpdesk*.

O objectivo do projecto aqui descrito é o de estabelecer processos para permitir que os utilizadores finais afectados consigam não só deixar de infectar a rede (e os restantes utilizadores) como "limparem-se" destas ameaças, protegendo os seus dados.

A Iniciativa Anti-*botnet* Alemã:

1. Identifica os clientes com PCs infectados
2. Informa os clientes
3. Oferece apoio na forma de o centro de suporte

*Spamtraps* e *honeypots* são utilizados para encontrar PCs infectados. Para essa finalidade, apenas ataques de PCs infectados são avaliados. Em nenhum caso se faz uma avaliação do tráfego de Internet através de métodos de inspecção de pacotes ou procedimentos similares

(que violam leis de privacidade alemãs). Por outras palavras, o comportamento do utilizador não é registado ou avaliado.

Após o primeiro ano de operações do centro de apoio, o ganho esperado de segurança revê-se num número consideravelmente menor de PCs infectados na Alemanha em comparação com o status quo anterior. O objectivo principal é remover a Alemanha do ranking dos dez maiores países de onde se originam as actividades *botnet*, o que melhorará a segurança dos cidadãos e das empresas, o nível de reputação dos sistemas e do próprio país.

### 6.2.1 Fluxo do processo

- Os Fornecedores operam *honeypots* e *spamtraps*. Somente os Fornecedores podem identificar os seus clientes, relacionando o endereço IP com um ponto específico no tempo.
- Os Fornecedores informam os clientes particulares com base num processo determinado pelos mesmos. Numa primeira fase, os clientes são informados de que foram infectados com software "mal-intencionado". Os clientes são encaminhados para o website da Central de Ajuda, onde instruções de desinfecção estão disponíveis.
- Se o cliente não for bem sucedido, pode entrar em contacto com um Provedor. O Provedor decide então se o cliente precisa de ser encaminhado para o call center para obter mais ajuda com a remoção do *malware*. Neste caso, o Provedor atribui ao cliente um pseudónimo juntamente com informações codificadas sobre a infecção.
- O processo é passível de resumo da seguinte forma:
    - Os utilizadores afectados são inicialmente informados pelos seus ISPs para fazerem download de ferramentas adequadas e seguir instruções no website do Projecto.
    - Se o utilizador não conseguir resolver o problema "por conta própria", é encaminhado, sob pseudónimo, a obter ajuda por telefone do *helpdesk* geral do Projecto.
    - Se os passos anteriores não resolverem, o utilizador é encaminhado para um especialista de nível de suporte 2 (especialista em segurança). Para além de sugerir o que fazer, é obrigatória uma actualização do estado do processo por via informática, para resoluções futuras de outros clientes.
    - Se os passos anteriores não resolverem o problema, o utilizador é aconselhado a deslocar-se fisicamente ou a um centro técnico do provedor, ou a uma loja informática, dependendo da opção (livre) do provedor e dos seus recursos. Saliente-te que um programa de *vouchers* para reparação de máquinas infectadas funciona em paralelo com este projecto, garantindo ao utilizador custos mais baixos na intervenção física à máquina infectada.

**Cobertura do projecto**

No lado dos ISPs, todos os maiores Fornecedores de internet alemães participam ou diligenciaram para participar neste Projecto. ISPs como 1 & 1 (incluindo Freenet), QSC, Netcologne, KabelBW, DeutscheTelekom, Vodafone, Hansenet, Telefonica, UnityMedia, Kabel Deutschland e Versatel foram incluídos ou demonstraram vontade de participar.

Juntos, os ISPs mencionados têm mais de 23 milhões de clientes DSL e cobrem quase completamente o mercado alemão de fornecimento de Banda Larga.

### 6.2.2 Aspectos jurídicos e desafios

Devido ao sistema de suporte implementado neste Projecto, os ISPs operam de modo a que nenhuns dados confidenciais dos utilizadores sejam partilhados (ou seja, os dados ficam concentrados na base de dados central, que serve de apoio a todo o Projecto).

Caso seja necessário, em casos excepcionais, e por motivos de gestão, incluir algum tipo de informação pessoal, tal é efectuado dentro de critérios muito específicos, e, em relação a esta abordagem, está prevista a solicitação prévia de uma declaração para o efeito, ao Comissariado Federal para a Protecção.

**Projecto e financiamento**

A duração do projecto é de 18 meses, com um máximo de 6 meses para o planeamento e construção e 12 meses para estabelecimento das operações de *helpdesk*. O orçamento inicial e financiamento para o Projecto é de 2 Milhões de euros, fornecidos pelo governo alemão (Ministério Federal do Interior).

O Escritório Federal de Segurança da Informação (BSI) oferece aos seus conhecimentos técnicos para apoiar a Eco (o organismo que resultou da agregação do governo e dos ISPs) e cuidar da estratégia e implementação da iniciativa, para além de ser consultora na concessão do financiamento.

No final deste período, a Eco irá garantir a continuidade do Projecto, através do esforço privado dos ISPs.

Em Setembro de 2011, o Projecto encontrava-se na fase final, de avaliação da iniciativa, de avaliação e os resultados estavam a ser muito promissores.

### 6.2.3 Feedback da iniciativa

Em conversa informal, via email, em Setembro de 2011, com Sven Karge, Head of Content Department da Eco, foi obtido o seguinte feedback:

- ″ Entre o início do projecto em meados de Setembro de 2010 e o final de Agosto (2011), tivemos mais de 1,2 milhões de visitantes no site do projecto e mais de 700 mil downloads e activações da ferramenta de limpeza central (DE-Cleaner). “

- ″ Aprendemos que menos de 1% dos utilizadores finais precisaram de mais informações de apoio, via telefone ou via email, significando que mais de 99% pôde desinfectar os seus computadores apenas com a ajuda dada no site. “

- ″ Recebemos informação de que mais de 50% dos utilizadores finais estão dispostos a cooperar numa base voluntária e de verificação para contribuir para esta iniciativa.”

- ″ A Alemanha, em relatórios mundiais sobre actividades maliciosas, estava, em 2010 na posição global número 3. Menos de um ano depois baixámos para 7.”

- ″ Em relatórios sobre origem de Zombies de Spam, estávamos (a Alemanha) em número 3 nos principais rankings mundiais, como o relatório da Symantec. Agora estamos na

posição 22! A própria Symantec compara esta iniciativa ao desmantelamento do Botnet Rustock."

″ Em relatórios de origem das infecções por Botnets, a Alemanha estava em 2º lugar mundial. Agora somos oitavos. "

## 6.3 Outros casos

### 6.3.1 Holanda

Em Julho de 2009, 14 ISPs holandeses concordaram em se unir na luta contra *botnets*.

Estes ISPs representam quase todas as conexões de Internet para consumidores domésticos e empresariais, na Holanda, sendo responsáveis por 98% do mercado.

Esta aliança foi fomentada pela Telecom Regulatory Authority (OPTA).

O acordo resultante da aliança não apresenta disposições sobre a forma de mitigação mas abordagens definidas incluem o intercâmbio de informações sobre os sistemas infectados e melhores práticas entre os ISPs participantes, um serviço de notificação ao cliente e, como medida de protecção, a construção de uma lista de reputação comum que implicará restrições no acesso a *hosts* identificados como maliciosos.

A Infra-Estrutura Nacional contra o Cibercrime (NICC) é um programa holandês, fundado em 2006, com foco em melhorar a resiliência da infra-estrutura crítica contra ameaças provenientes de crimes cibernéticos. Embora a função da NICC não seja combater o crime directamente, suporta as partes envolvidas nos seus esforços para melhorar a segurança dos processos de TI relacionados com o trabalho. A iniciativa serve como um elo entre as partes, disponibilizados recursos e informação, bem como para gerir informações de incidentes, vulnerabilidades e boas práticas ocorridas. A comunicação é organizada num ambiente de interacção público-privada, e a partilha de dados só acontece dependendo do nível exigido de confidencialidade.

Para além da actividade normal da NICC, temas importantes de interesse para as partes em todos os sectores estão organizados em grupos de trabalho, como o "Safe Internet Banking", que compreende os bancos, ISPs e fornecedores de segurança.

Paralelamente, e como resultado, o governo é tido como um parceiro e um destinatário de informação sobre os processos de segurança.

### 6.3.2 Austrália

Em 2005, o Australian Communications and Media Authority (ACMA) começou o Australian Internet Security Initiative (AISI) com a intenção de reduzir o número de computadores infectados conectados à Internet.

Esta iniciativa está ligada com o Código de Boas Práticas da Indústria da Internet, que descreve uma directriz para a implementação de acções participando Fornecedores de Serviços da Internet em cooperação com o CERT da Austrália. O programa é voluntário, mas

foi bem recebido. No presente ano, o número de ISPs participantes aumentou de 6 (em 2005) para 100.

A ideia principal deste AISI é aumentar a consciência da situação dos *malwares* em geral, conduzindo centralmente uma organização de dados e identificação remota de dispositivos infectados e notificando os Fornecedores de rede responsável, outros Service Providers ou mesmo outros administradores de TI.

A AISI envia relatórios diários para as partes participantes e serve de "umbrella" ao projecto, providenciando detalhes aos Fornecedores de rede, detalhes de implementação de outras acções tomadas (a partir de encaminhamento de informações sobre a infecção), e dando conselhos sobre como remover o *malware*, para restringir a conectividade da Internet do sistema infectado, e como proteger o proprietário de outros e maiores danos.

Além disso, todos os incidentes que originem suspeitas de uma actividade criminal são comunicados aos órgãos governamentais responsáveis.

### 6.3.3 Japão

Os esforços japoneses na luta contra *botnets* estão concentrados no National Cyber Clean Center (CCC), e começaram em 2006. Uma cúpula, reunindo o Ministério Japonês de Assuntos Internos e Comunicações, e os Ministérios da Economia, Indústria, e Comércio, lideram e organizam as actividades. Várias instituições e empresas de vários grupos de interessados trabalham em conjunto, incluindo mais de 70 ISPs japoneses, responsáveis pelos serviços relativos a cerca de 90% de todos os utilizadores da Internet.

Os participantes são divididos em três grupos internos:

- O Centro de Informação Telecom Sharing and Analysis (ISAC) Japão, é responsável pelas contra medidas de operações e técnicas contra as *botnets*.
- JP-CERT, é responsável pelo grupo de análise e extracção de dados do programa.
- A Agência de Promoção de Tecnologia da Informação (IPA), trabalha na sensibilização do utilizador e é responsável pela prevenção de infecções.

O procedimento geral é comparável à abordagem da Austrália, na medida em que o CCC centraliza e redistribui informações sobre infecções detectadas nos ISPs participantes. Também é mais orientada para infecções nos utilizadores finais, com notificações "customizados", informações especializadas de desinfecção, e ferramentas para a remoção distribuídos entre os cidadãos.

### 6.3.4 Coreia do Sul

Como uma taxa de ataques DDoS significativa contra o seu país e relatórios indicando altas taxas de infecção entre os computadores da Coreia do Sul, a Agência de Segurança Coreana para a Internet (KISA) e o CERT Coreano (KRCERT) lançou uma extensa campanha contra as *botnets*. A abordagem consiste em três partes:

- Máquinas remotamente infectadas são detectadas por vários meios. Isto inclui servidores de DNS especializados, que monitorizam consultas e conexões suspeitas.

Outros dados provêm de análise de *malware* e relatórios dos Sistemas de Detecção de Intrusão.

- O KRCERT realiza extensa monitorização e mitigação de *botnets* usando um serviço de gestão centralizada DNS. Desta forma, nomes de domínio que foram confirmadas como tendo fins maliciosos podem ser facilmente eliminados ou juntados a listas de reputação.
- Para complementar os esforços de mitigação, a cooperação entre KRCERT, ISPs e fornecedores de segurança de TI procura notificar os utilizadores finais acerca das infecções, fornecendo-lhes também ferramentas de remoção para limpar os seus sistemas.

Além desses esforços, a Coreia do Sul criou o *E Call-Center 118*, uma "hotline" de emergência para lidar com incidentes de Internet. Os agentes de call center são treinados para dar conselhos sobre a remoção de *malware*, para identificar emails de spam, e para responder a questões sobre privacidade da internet e tecnologia em geral.

# 7 Conclusões

## 7.1 Contexto

Considerando que um sistema de telecomunicações (tanto infra-estruturas como serviços) representa um desafio de segurança que é em grande parte, e em escala, semelhante ao desafio da evolução tecnológica da sociedade, as mesmas motivações técnicas, organizacionais e humanas devem ser observadas na tentativa de enfrentar esse desafio.

Proteger as informações é proteger os proprietários das mesmas e como tal, a cibersegurança deve ser vista de uma perspectiva global, e com impacto em todos os sectores da sociedade: um país inseguro não fomenta o próprio desenvolvimento, e muito menos o investimento no mesmo. A inovação ressente-se, bem como a educação. Em casos críticos, os cidadãos perdem confiança nos sistemas tecnológicos de, por exemplo, os bancos ou a DG de Finanças.

Aos olhos estrangeiros, telecomunicações inseguras são telecomunicações fracas e obsoletas, assim como a probabilidade de o país e as empresas que o compõem serem competitivas e apelativas.

Um sistema que facilite o cibercrime resultará em problemas. Primeiro para os cidadãos, que serão, com mais frequência, roubados, denegridos ou chantageados, depois para as empresas, que presenciarão fugas de informação e desinformação no mundo global de informação, depois para o país, que é a súmula destas entidades.

Em proximidade, e directamente afectada e afectante dos perigos da segurança online, está o caso particular da segurança da reputação online, e em todas as suas inerências: desde o ponto de vista conceptual, como impedir que alguém personifique ou roube informação de outrem, para divulgar, extorquir ou tirar vantagem (espionagem industrial), até ao aspecto inerente aos serviços, que se regem por listas de reputação (todos os ISPs do mundo, provavelmente) (imagine-se uma empresa de comércio online cujo website era constantemente interdito a clientes de todo o mundo, por ter má reputação de rede).

Em suma, medidas deverão ser tomadas, entre a iniciativa privada e pública, entre os tecnologicamente avançados ISPs e as empresas e cidadãos a quem prestam serviços, e a quem abrem as comunicações, móveis, de internet, de email, etc.

Conclusão:

Se as actividades baseadas no processamento de informações estão a crescer diminuindo a exclusão digital (e social), tal exigirá:

- Informação confiável e segura nas infra-estruturas (com acessibilidade garantida, disponibilidade, “confiabilidade” e continuidade dos serviços).
- Políticas para criar confiança.

- Enquadramento jurídico adequado e com autoridades (jurídicas e policiais) versadas e objectivadas em novas tecnologias, capazes de cooperar com os seus homólogos de outros países.
- Gestão de segurança efectiva, e transversal a todos os organismos da sociedade;
- Ferramentas de segurança que fomentem a confiança nas aplicações e serviços oferecidos (transacções comerciais e financeiras, saúde, governo, votos electrónicos, etc.) e em procedimentos de salvaguarda dos direitos humanos, especialmente a privacidade dos dados pessoais.

O objectivo da segurança cibernética é ajudar a proteger os activos e recursos da organização. Estes recursos são organizacionais, humanos, financeiros, técnicos e de informação, permitindo à organização prosseguir a sua missão.

O objectivo final é garantir que nenhum dano duradouro é perpetrado contra a organização.

Ou seja, a segurança consiste em reduzir a probabilidade de que uma ameaça se materialize. Similarmente, o objective da segurança deve ser reactive, limitando o dano resultante ou o mau funcionamento e garantindo que, após um incidente de segurança, as operações normais possam ser restauradas dentro de um prazo aceitável e com um custo aceitável.

### 7.1.1 Conclusões com enfoque em Portugal

Quando se pensa em medidas que possam tornar Portugal, e o seu tecido empresarial mais competitivos, vislumbram-se um conjunto de situações e objectivos que se melhorados tornarão Portugal mais fortalecido, quer nas suas exportações, mas também nas condições com que importa produtos e serviços, nas condições que ajudam trabalhadores expatriados a decidirem instalar-se no país, e, acima de tudo, condições que fazem empresas estrangeiras quererem implantar uma sucursal, e/ou fazer negócios com o nosso país. Todas as condições que poderemos imaginar oferecer são sintetizadas numa única expressão: A reputação que Portugal tem aos olhos globais.

Alguns compostos que formam a reputação de um país, para o efeito supra mencionado, são bastante óbvios: A burocracia para os estrangeiros, o nível de corrupção, a vida em comunidade, os direitos dos trabalhadores, a produtividade, quais os problemas de xenofobia e discriminação existentes, etc.

Existe, nestes parâmetros todos, um parâmetro, muitas vezes negligenciado, mas que tem um impacto considerável na reputação de um país: A qualidade e a segurança das comunicações electrónicas, designadamente o acesso à internet.

O que pode, à primeira vista, parecer uma componente meramente técnica, e relativamente nivelada no âmbito dos países ocidentais é, em especial quando negativa, um factor muito considerável para as empresas, em especial aquelas com necessidades relacionadas com a internet (que serão praticamente todas, numa sociedade moderna). Ninguém arrisca transacções ou a implementação de um website num país com problemas de conexão, *hacking* de websites, *downtime de internet* ou proliferação de *botnets*. As comunicações electrónicas são simplesmente fundamentais no mundo empresarial moderno. E por isto mesmo, quanto melhor a reputação das comunicações electrónicas desse país, melhor este parecerá aos olhos do investimento estrangeiro.

## 7.2 Assimilando a Segurança como componente da sociedade moderna

Inevitavelmente, com o tema da Segurança, segue o tema das liberdades individuais.

Para o efeito deste documento, não deveremos contudo pensar nos espíritos rebeldes e conservadores que juntos ou separados desbravam, diariamente, o nebuloso mundo da internet, uma componente vital da sociedade moderna, mas que só recentemente tem sido regulada, ou pelo menos balizada (episódios como o acesso a conteúdos pirateados e a informação confidencial, ou ainda as opiniões lesivas, anónimas que não encontram oposição judicial na internet contam centenas de casos que todos conhecemos).

Para este documento importa ponderar a segurança na internet como o debelar de ilegalidades, facilmente rotuladas como tal, e válidas tanto no mundo da internet como no mundo real. Roubos de identidade, envio de correspondência não solicitada, penetração de infra-estruturas privadas com o intuito de apropriação de material confidencial e/ou danos e destruição de propriedade privada são temas que não deverão deixar margens de dúvidas no que concerne a necessidade de forçar algum tipo de segurança para que crimes não sucedam. Na verdade, a expressão e o usufruto das liberdades necessita de seguranças básicas que tornem estas liberdades possíveis [Amoroso, E.G. (2011)].

Postulado:

A segurança, no seu sentido mais lato, é nevrálgica para manter as comunicações.

Assimilando que computadores e redes mantêm infra-estruturas críticas, basilares da sociedade moderna, podemos determinar que o risco de ter cibercriminosos a infligir danos nessas mesmas infra-estruturas causaria danos com potencial de contágio enorme. Como exemplos, imagine-se o nível de confiança que um cidadão depositaria no seu banco conhecendo relatos de outros bancos que tivessem sido comprometidos? Como confiaria um cidadão nas suas infra-estruturas de energia se conhecesse sabotagens noutros estados, como o ataque aos sistemas nucleares no Irão (Julho de 2010)?

Postulado:

As infra-estruturas de redes, computadores e comunicações são críticas no mundo moderno, e crimes contra as mesmas significam danos com potencial de contágio, em especial na confiança depositada em entidades similares àquelas que foram comprometidas.

Ao analisar a evolução do cibercrime e *botnets*, em particular, é possível prever como irão evoluir os ataques de *malware.*

A motivação por trás dos ataques irá aumentar ainda mais. Enfrentamos economicamente e politicamente os ataques motivados, e ataques com o intuito de obter publicidade.

A qualidade e simplicidade das ferramentas disponíveis e kits de desenvolvimento para ataques continuará a aumentar, de modo que cada vez mais atacantes não-especialistas serão passíveis de causar danos graves.

Conceitos de comando e controlo de infra-estruturas utilizadas para *botnets* irão adoptar tecnologias emergentes, a fim de atingir níveis mais elevados de fraude e resiliência. Isto envolve protocolos de rede e padrões Web, bem como as novas tendências em sistemas de comunicação em tempo real ou redes sociais para transmitir e disfarçar o tráfego malicioso.

Conclusão:

O cibercrime tornou-se um negócio rentável e indefinições e diferenças ao nível da mitigação, em termos globais facilita a propagação da actividade. Isto significa que mesmo *botnets* não muito complexos vão durar por longos períodos e estar disponíveis para ataques e fraudes.

Com a proliferação de smartphones já apareceram os primeiros *bots* para smartphones – isto é um exemplo de como a evolução das tecnologias só adiciona outras dimensões à ameaça global de *botnets*.

## 7.3 Os ISPs e os Governos como actores-chave

Alguns serviços são providenciados por governos. Mas muitos são providenciados por grupos comerciais, como ISPs ou bancos. Poderemos assumir então que existe uma interdependência entre os sectores públicos e privados num estado. Mais: considerando as empresas globais a operar internacionalmente, com destaque para os sectores tecnológico, bancário, e de energia, seria tácito admitir que existe uma interdependência a nível global para providenciar estas infra-estruturas de redes e computadores e, em adjacência, para providenciar a segurança necessária que proteja os cidadãos (e as empresas, e os próprios países) [Amoroso, E.G. (2011)]. Esta total interdependência é comummente chamada de “flat world” [Friedman, T. (2007)].

Postulado:

Nas telecomunicações, a interdependência entre sectores públicos e privados, locais a globais, implica uma colaboração que melhor debele o problema da segurança.

Aplicando o célebre ditado popular português, - “Casa roubada, trancas na porta” -, e escalando-o para uma mentalidade, transnacional, de menosprezo pelo investimento em segurança, quando ainda não existem ameaças corroborantes que justifiquem, conseguem-se descobrir casos onde a segurança é, com veleidade, descurada. Os custos (pessoal, equipamento, monitorização) são elevados, e é comum que muitas empresas (especialmente do sector privado) negligenciem a segurança das suas infra-estruturas. Não obstante os factores sociológico e económico, o desconhecimento acerca de tecnologias extremamente complexas e, especialmente de actividades criminosas não tradicionais será porventura a principal causa para a deficiente preparação de algumas empresas e cidadãos, em especial as

empresas e cidadãos cujo "core business" ou conhecimento académico, profissional e/ ou social não está relacionado com a área informática.

Se entendermos o papel do estado enquanto protector das liberdades individuais e colectivas das entidades (pessoas e empresas) que o compõem (quando estes pressupõem actuações dentro da legalidade, claro) e se ao papel do estado adicionarmos o papel das empresas cuja *raison d'etre* (e responsabilidade) é fornecer as comunicações e as infra-estruturas para as mesmas ao resto do país (Empresas de telecomunicações, ISPs, SPs, Carriers, etc.), para além de, por motivos óbvios, deterem um conhecimento aprofundado sobre as tecnologias e os perigos em questão, poderemos diferenciar a responsabilidade de todas as entidades que compõem uma sociedade moderna, colocando, nos lugares cimeiros, o Estado e os ISPs, seguidos de perto de outras entidades, colectivas, cujo âmbito envolve lidarem com informação vital para a sociedade (Bancos, hospitais, serviços de defesa).

Conclusão:

O Estado e os ISPs possuem especial relevo e responsabilidade em proteger os cidadãos contra a insegurança nas telecomunicações.

A fim de assegurar que é economicamente viável para os ISPs operar serviços de apoio à desinfecção das máquinas dos utilizadores finais, os seus esforços devem ser apoiados através de Parcerias Público-Privadas, reflectindo, por exemplo, a Iniciativa Anti-*botnet* Alemã ou a Parceria Público Privada Europeia, EP3R.

Caso estas iniciativas de desinfecção nacionais se revelem eficazes, esta prática deveria ser alargada à UE como um todo.

## 7.4 Conclusões de gestão corporativa

### 7.4.1 Gestão dinâmica

Aproximando a segurança através de um processo de gestão dinâmico e contínuo, afecto a múltiplas posições da organização, é a melhor via para lidar com a natureza dinâmica do risco e as necessidades em evolução, isto através da contínua adaptação e melhoria das suas soluções.

A qualidade da gestão de segurança irá determinar o nível de segurança oferecido. A política de segurança cibernética deve ser definida ao nível da gestão de topo. Existem estratégias de segurança, políticas, procedimentos e soluções, que deverão contudo ser personalizadas, pelo facto de que existem organizações com necessidades de segurança particulares, que precisam de ser atendidos em momentos determindados [Kroes (2011)].

Para um exemplo do contexto dinâmico em que a gestão da segurança deve funcionar, considere-se o processo de detecção de vulnerabilidades de segurança em software. Isto é feito por meio de actualizações periódicas de segurança (actualizações de antivírus, etc.). Boletins de informação, mais ou menos personalizados, tornam possível a manter-se informado sobre as vulnerabilidades que foram detectadas e como intervir adequadamente e aceleradamente. Se um nível mínimo de segurança for mantido, e possível debelar em tempo útil questões que surjam.

É também imperativo alocar recursos suficientes para implementar uma gestão dinâmica que actualize continuamente as soluções de segurança e, assim, manter um nível consistente de segurança, face á evolução da… insegurança.

A dimensão dinâmica de segurança representa um desafio crucial não só para os fornecedores de ferramentas de segurança e editores de software, mas também para os administradores dos sistemas de segurança nas organizações, que raramente têm o tempo necessário para incorporar todos os mecanismos que estão disponíveis. Torna-se portanto eficaz, que se fomente a partilha de ferramentas e o recurso (controlado) a especialistas externos.

Os normativos vigentes, bem como indivíduos e organizações especializados, podem representar grandes fontes quer de informação útil e auxílio, quer de incentivo (aplicar uma norma ISO de segurança, por exemplo) para a organização.

### 7.4.2 Outsourcing e dependências

Prestadores de serviços que oferecem filtros anti-vírus e anti-spam efectivamente assumem uma parte da gestão de segurança para os "stakeholders" de determinada organização. Esta tendência implica uma mudança e redistribuição de papéis no que concerne as responsabilidades em matéria de segurança. Sendo a segurança cada vez mais transferida para o prestador de serviços ou fornecedor técnico, existe a necessidade de, por um lado, vincular legalmente e contratualmente esse prestador de serviços, por eventuais insucessos, como assegurar que esse prestador tem capacidade, legitimidade e, acima de tudo rectidão, para as tarefas de segurança.

Esta mudança não resolve, contudo, os problemas da segurança, mas apenas transfere para o prestador de serviços a implementação, tornando-o responsável não só pela disponibilidade e desempenho do serviço, mas também para a gestão e manutenção de um certo nível de segurança. É consequentemente necessário assegurar que o ISP prestador de serviços realmente acrescenta valor (e segurança), e que existe uma constante e bidireccional comunicação entre os organismos internos de uma empresa e os prestadores de serviços.

A questão da delegação da totalidade ou parte da missão de segurança não é puramente técnica. É de natureza estratégica e legal, e levanta a questão fundamental da dependência de fornecedores. [Click, Duening (2005)].

Reforça-se por isso a necessidade de encontrar um contexto legal que sirva ambas as partes e, em resultado, os clientes.

### 7.4.3 Comportamento Preventivo das organizações

A prevenção de segurança é, por definição, pró-activa. E envolve factores humanos, legais, organizacionais, económicos e de dimensão tecnológica.

Se, até há pouco tempo, a segurança de TI ambiente tem-se preocupado principalmente com a dimensão técnica., este modo de entender a segurança dos sistemas de informação, do ponto de vista técnico, reflecte-se no negligenciar da dimensão humana, ou seja, na mentalização dos "stakeholders" para a prevenção.

Noutro âmbito, muitas vezes, o incidente de segurança surge internamente, por descuido ou deliberadamente e externamente, também deliberadamente ou por falta de informação dos parceiros e/ou clientes [Fertik, Thompson (2010)].

A criminalidade é principalmente uma questão humana, e não técnica. Uma resposta puramente técnica é, portanto, inadequada para controlar o que é essencialmente um risco humano.

A abordagem para a resolução destes problemas é tipicamente de reacção e repressão. Ou seja, após a ocorrência de um incidente que, por definição, implicou uma lacuna destacada nas medidas de protecção.

É necessário, para prevenir e impedir ataques cibernéticos, o desenvolvimento de mecanismos de investigação / criminais, e, especialmente a identificação das políticas de segurança que sejam necessárias para responder aos ataques, punir os agressores, ou inibir as incúrias. Resume-se que é essencial o envolvimento e a distribuição de informação (e normativos) a todos os intervenientes na vida de uma organização.

## 7.5 Conclusões de dimensão política

### 7.5.1 Responsabilidade do Estado

O Estado possui considerável responsabilidade para fazer da segurança digital uma realidade. Isto é particularmente verdadeiro para a definição de um quadro jurídico adequado, que seja unificado e prático.

O Estado não deve apenas promover e incentivar a pesquisa e desenvolvimentos em segurança, mas também promover uma cultura de segurança em conformidade com as normas mínimas de segurança (a segurança deve ser construída em produtos e serviços), enquanto fortalece a aplicação da lei em matéria de cibercrime.

Tal acarreta questões do modelo financeiro subjacente às parcerias público-privadas para os planos de acção nacionais e internacionais.

Ao nível estratégico é necessário assegurar a notificação, prevenção, partilha de informação e gestão da segurança. É também necessário aumentar a consciencialização sobre as melhores práticas em gestão de riscos e de segurança.

Outro requisito importante é a coordenação e harmonização dos sistemas jurídicos. Requer-se a assistência do Estado para promover a aplicação da lei e da segurança, a elaboração de propostas de empreendimentos cooperativos (formal / informal, multilateral / bilateral, activo / passivo, nacional / internacional) também deverá ser definido.

Ao mesmo tempo, é essencial fornecer informações, educação e formação no processamento de informações e tecnologias de comunicação, não apenas de segurança e nas medidas de dissuasão. A sensibilização de questões de segurança não deve ser limitada à promoção de uma cultura de segurança e códigos de conduta cibernéticos. A cultura de segurança deve ser sustentada, a montante, por uma cultura de TI [ENISA (2009)].

Aos diferentes intervenientes devem ser dados os meios para aprender, lidar e gerir os riscos tecnológicos, operacionais e de informações.

Neste contexto, o Estado deve também incentivar a denúncia de casos de cibercrime e garantir que haja confiança entre os vários intervenientes do mundo económico e as autoridades legais e policiais.

Essas autoridades, mas também as autoridades de defesa civil, serviços de emergência, as forças armadas e forças de segurança, têm um papel táctico e operacional na luta contra a cibercriminalidade, a fim de proteger, perseguir e reparar.

Cabe a cada Estado definir uma política de desenvolvimento da sociedade da informação reflectindo os seus próprios valores, e fornecendo os recursos necessários para torná-la realidade. Tal inclui os meios de protecção e da luta contra a cibercriminalidade.

Para conter o cibercrime de uma forma global, centralizada e coordenada, é necessária uma resposta a nível político, económico, jurídico e tecnológico.

O desejo de simplicidade e eficácia na segurança está em desacordo com a complexidade das necessidades e ambientes, e faz a delegação e/ou o outsourcing dos serviços e da segurança uma opção atraente. Mas esta tendência cria um alto, ou total, grau de dependência. E isso é um grande risco de segurança. Os Estados devem evitar tornarem-se dependentes, na gestão estratégica, táctica e operacional da sua segurança, relativamente a entidades externas e/ou privadas, sem garantir que participa activamente no processo.

## 7.6 Conclusões de dimensão económica

Um dos aspectos intrínsecos à segurança é que esta não serve para fazer dinheiro, mas para evitar perdê-lo.
Embora possa parecer relativamente simples estimar os custos de segurança (orçamentos associados, o custo de produtos de segurança, formação, etc.), avaliar a rentabilidade da segurança é bem mais difícil. Adoptando uma abordagem subjectiva, pode-se supor que as medidas de segurança intrinsecamente possuem uma forma "passiva" de eficácia que impede que determinadas perdas potenciais.
No entanto, é difícil avaliar o custo da segurança e os custos associados com perdas devido a acidentes, erros ou actos maliciosos. O custo da segurança é uma função das necessidades da organização, e depende dos activos a serem protegidos e os custos dos danos resultantes de segurança insuficiente.

O valor económico da segurança deve, consequentemente, ser concebido no sentido mais amplo e social, tendo em conta o impacto das novas tecnologias sobre os indivíduos, organizações e nações. Este valor não pode ser reduzido a custos de instalação e manutenção.

## 7.7 Conclusões de Dimensão Social

É importante fazer todos os participantes na internet conscientes da importância de obter garantia, e quais os passos básicos são que irá reforçar o nível de segurança quando sejam claramente formulados, definidos e aplicados de forma inteligente.

Campanhas de informação e de educação cívica para uma sociedade da informação responsável, que abrange os desafios, os riscos e as medidas de segurança preventiva e

dissuasora, são necessários, a fim de educar todos os ciber-cidadãos no processo de segurança.

O ênfase deve ser sobre o dever de segurança, responsabilidade individual e medidas dissuasoras, bem como as possíveis implicações no direito penal de uma falha em respeitar as obrigações de segurança. Mais no geral, também é necessário para fornecer educação e formação em tecnologias de informação e comunicação, e não apenas sobre segurança e medidas de dissuasão: a sensibilização para as questões de segurança não deve ser limitada à promoção de uma cultura de segurança, mas o inverso: a cultura de segurança deve ser incorporada dentro de todos os aspectos quotidianos de uma organização, talvez na forma de licenciamento de software ou adopção de normas internacionais de segurança.

| Princípios para a Segurança da Informação | |
|---|---|
| Consciencialização | Todos os participantes são responsáveis pela segurança dos sistemas de informação e redes |
| Responsabilidade | Todos os envolvidos têm uma participação na segurança dos sistemas e redes de informação |
| Resposta | Os participantes devem agir de forma atempada e de cooperação para prevenir, detectar e responder a incidentes de segurança. |
| Ética | Os participantes devem respeitar os interesses legítimos de terceiros. |
| Democracia | A segurança dos sistemas e redes de informação devem ser compatíveis com os valores essenciais de uma sociedade democrática. |
| Avaliação de risco | Os participantes devem efectuar e efectivar avaliações de risco. |
| Design e segurança | Os participantes devem incorporar a segurança como um elemento essencial dos sistemas de informação e redes. |
| Responsabilidade individual | Os participantes devem adoptar uma abordagem abrangente para gestão de segurança. |
| Gestão de segurança | Os participantes devem rever e reavaliar a segurança dos sistemas de informação e redes, e fazer as modificações apropriadas para políticas de segurança, práticas, medidas e procedimentos. |

Tabela 7-1Princípios na gestão da segurança da informação [ENISA (2010)]

# *8* Recomendações para o combate ao cibercrime

## 8.1 Recomendações aos ISPs

Apesar de medidas anti-spam e Anti-*botnet* serem comprovadamente e geralmente eficazes, estes esforços ainda poderiam ser melhorados. Por exemplo:

- ISPs deverão ter uma abordagem mais pró-activa na monitorização de spam e identificação dos remetentes, para que acções apropriadas possam ser tomadas pelos ISPs originários. Tal implica uma rede inteligente de partilha de informação.
- Agregadores de informação partindo do lado de quem providencia a rede, ou seja, tornar os ISPs que concedem o acesso, os primeiros responsáveis em capturar os prevaricadores. Isto significa que um sistema de monitorização na rede, que incida sobre os protocolos HTTP, SMTP, DNS e IP, principalmente, deverá garantir que os cibercriminosos terão dificuldade em "sair" da sua rede, quanto mais entrar noutra.
- Os sistemas de reputação deverão ser fidedignos, e os mecanismos de auto e hetero correcção deverão cumprir com a necessidade de assegurar que é fácil remover um servidor ou domínio de uma lista negra, assim que os problemas ou erros tenham sido rectificados.
  E com tantas listas de reputação diferentes em uso, esforços de colaboração para partilha de dados ajudaria a resolver o problema.
- Os Fornecedores devem procurar soluções colaborativas para combater o spam, de preferência associando-se a uma entidade acima de suspeitas e com poder político. Ou seja, replicar as iniciativas já existentes, por exemplo, na Alemanha, com o projecto Anti-*botnet*.
- Os Fornecedores devem procurar aumentar a distribuição de relatórios de abuso, garantindo a inter-relação com outros fornecedores, e visando automatizar os processos de denúncia de abuso, possivelmente adoptando o formato técnico para denúncia de abuso (ARF).
- Os decisores políticos e autoridades reguladoras poderiam ajudar nos esforços de prevenção de spam clarificando os conflitos aparentes entre filtragem de spam, privacidade e obrigação de retenção de dados.

## 8.2 Recomendações Políticas e Sociais

### 8.2.1 Envolver o Governo

Tornar as actividades das *botnets* puníveis, depende quer de legislação adequada quer de apoios e incentivos à debelação deste problema.

Uma lei, a ser imposta, deve ser baseada em outras leis vigentes ou, melhor, no acórdão de entidades internacionais, designadamente os conselhos legislativos e de segurança da EU.

Um acordo no seio da EU pela razão óbvia de que estes crimes são, quase sempre, transnacionais, e determinados mecanismos jurídicos, tais como a extradição, o pedido de dados pessoais e mesmo a exposição de contas abrigadas por sigilos legais e bancários requer uma convergência de todos os estados membros [ENISA (2010)].

Para além deste facto, uma lei de cariz transnacional resultará, ao fim de certo tempo, de uma correcta análise e cruzamento de dados entre forças de segurança. Como exemplo, se o spam não fosse ilegal, por exemplo, na Grécia, seria inviável que Portugal conseguisse solicitar os dados de um *spammer* grego.

Processar (em ambos os sentidos) o cibercrime de forma consistente e coordenada (por exemplo em consonância com a Convenção Europeia dos Cibercrime, que ainda não foi ratificada por todos os países signatários) é, portanto, uma medida a acatar veemente.

A inacção, ou a falta de coordenação dos tomadores de decisões, num problema com uma extensão desmesurada, multiplica o problema e acções futuras.

### 8.2.2 Esclarecer e Harmonizar a legislação internacional

Em geral, os organismos que enfrentam a ameaça das *botnets* têm algum receio de se envolver em questões legais (de privacidade, de segurança, de abuso de poder, etc.), quando participam activamente nos esforços de mitigação.

A questão não estará tanto na falta de legislação mas na interpretação das leis existentes que, frequentemente, são adaptações do mundo real para o mundo virtual.

Infelizmente, as abordagens de mitigação mais promissoras e dinâmicas incorrem nos maiores obstáculos legais de forma a obter permissão explícita para implementar as abordagens.

As melhores práticas actuais, como monitorizar a rede, e identificar utilizadores infectados ou websites infecciosos, normalmente implica posteriormente revelar ou contactar o utilizador e entrar em contacto com o serviço responsável ou provedor e informá-los sobre a existência de serviços mal-intencionados na sua rede [ENISA (2010)].

A consequência, se o prestador de serviços for cooperativo, é o cancelamento do serviço ao infractor. Mas no caso de um prestador de serviços não-cooperativo, somente por via de acções legais se consegue atingir esses objectivos.

Onde contra medidas, que visam agressivamente atacar a *botnet* através de um ataque DoS ou uma aquisição remota do canal ou de instâncias de servidor da *botnet*, esbarra frequentemente

no direito ou não de tomar estas medidas. Muito mais problemas legais ocorrerão se o cenário for transfronteiriço.

Consequentemente, as leis e directrizes claras são uma condição necessária, se permitindo aos agentes de segurança concentrar-se na sua tarefa, e simultaneamente, enfrentar o mínimo de obstáculos na legislação, contando que mantenham as salvaguardas adequadas aos cidadãos.

### 8.2.3 Acelerar os processos judiciais

Leis globais versando o combate à cibercriminalidade parecem ser o elemento mais importante em falta, para reforçar o esforço necessário para combater eficientemente este problema.

É necessário, consequentemente, a rápida clarificação da legalidade do uso de ferramentas técnicas, uma vez que a situação jurídica em determinados países retarda o processo de desenvolvimento destas ferramentas, mesmo que estas desempenhem um papel decisivo na debelação do problema.

Além disso, a aplicação das regras para lidar com casos de emergência, onde a justificação para uma acção imediata é aceite, muitas vezes, tardiamente, requer uma examinação cuidada, pois ajudaria na concessão de esforços de mitigação no tempo de reacção necessário para contrariar as características altamente dinâmicas de *botnets* e *malware*.

### 8.2.4 Uma melhor cooperação entre a lei, agências executantes e empresas privadas (ISP, entidades financeiras, empresas de segurança, etc.)

Trabalhando para um melhor diálogo e existindo uma ajuda mútua para detectar, prevenir e reagir a incidentes com *botnets* é, obviamente, um caminho promissor.

<u>Recomendações:</u>

1. Equipas de Resposta de Emergência, à escala nacional, são um primeiro ponto de contacto com valor acrescentado. E, se a cooperação for à escala europeia, talvez organizações como a ENISA possam agir como um ponto focal adicional que permita a coordenação e a partilha das melhores práticas.
2. É necessária a consciencialização do utilizador, que usa um computador conectado à Internet. Este deve conhecer e compreender as ameaças que o poderão afectar.
   Uma educação adequada sobre medidas de segurança deve ser incluída nos currículos escolares, em especial no contexto das Novas tecnologias.
   Outras iniciativas de sensibilização serão sempre bem-vindas.

<u>Recomendações com uma vertente técnica</u>

1. Politicamente, deverão ser introduzidas medidas que controlem os softwares e aplicações informáticas. Por exemplo, a comercialização de um produto ou um serviço no espaço de um país deverá implicar um conjunto de aprovações e certificações, quer ao produto, quer ao produtor.

Algum do Investimento Estatal previsto para a indústria nacional deverá ser canalizado para o desenvolvimento de software seguro. Ainda mais, considerando a dependência de muitos sectores da sociedade em equipamentos tecnológicos.

2. Os ISPs são fundamentais para a solução, uma vez que podem detectar e bloquear *botnets* e *malware*.
   É natural que, para tal, os ISPs tenham necessidade de inspeccionar o tráfego do utilizador, o que poderá levar a problemas de privacidade.
   Orientações legais devem ser produzidas de modo a permitir que os ISPs possam inspeccionar tráfego suspeito para detectar e bloquear a comunicação ilegítima.
   Obviamente que a fiscalização e a introdução de normas que protejam a privacidade dos consumidores deverá acompanhar estar orientações legais.
3. Os decisores políticos devem monitorizar a ameaça de *botnets* e *malware* de perto. O quadro dos cibercrimes é constantemente mutável, e tem tendência a agravar.

### 8.2.5 Colaboração e/ou informação centralizada

A fim de apoiar a colaboração, criação de ferramentas, mecanismos e procedimentos para partilha de dados e informações que estejam relacionados com os incidentes e investigações em curso, deve ser instalado, ou criado, onde não exista.

Especialistas enfatizam que uma central de informações de partilha singular, ou agregada num conjunto de *hubs*, forneceriam uma melhoria significativa na maioria dos processos relacionadas com a luta contra os cibercrimes.

Obviamente, uma abordagem centralizada exige concessões de todas as partes envolvidas, já que o benefício correspondente não é necessariamente uniforme.

Portanto, para os agentes que tendem a criar mais benefícios para os outros do que podem receber, através do processo de partilha de informações, deverão ser incentivados adequadamente para compensar os seus esforços.

Provavelmente o mais importante benefício criado por um serviço central de gestão de informações é a agregação de "insights" e perspectivas sobre os processos em curso e a necessidade de evitar actividades mutuamente comprometedoras.

Do ponto de vista técnico, a integridade e a confidencialidade dos dados devem ser assegurados em relação aos sistemas de classificação de dados. Por exemplo, o acesso à informação partilhada tem que ser gerido com mecanismos de autenticação forte. Além disso, a posse e localização de dados partilhados, bem como os protocolos de troca, devem ser acordados e, preferencialmente, da responsabilidade de um organismo com presença Estatal.

Mesmo sem um armazenamento de dados central, uma instituição que permita uma comunicação mais rápida entre todas as partes envolvidas é benéfica na luta contra *botnets*.

### 8.2.6 Fomentar análises mais eficientes

Embora exista uma variedade de abordagens e ferramentas para a análise de amostras de *malware* e *botnets*, o desenvolvimento destas ferramentas é importante.

Por exemplo, o tempo gasto pelo sistema Conficker na análise ao *bot* "Stuxnet" levou várias semanas, o que ainda é claramente muito tempo para permitir uma resposta atempada às ameaças críticas.

Novas técnicas que permitam uma classificação mais rápida de reputação e uma mais eficiente análise de amostras de *malware* são necessários e devem ser apoiados por fundos e instituições de pesquisa.

### 8.2.7 Manter o sistema limpo para os cidadãos

O nível de responsabilidade que o utilizador final assume tem de ser aumentado.

O utilizador final deve ser encorajados a assumir maior responsabilidade para manter o próprio sistema limpo, nomeadamente porque um fracasso seu aumenta proporcionalmente o risco para os outros utilizadores e empresa, já para não mencionar a própria empresa, se se tratar de um ambiente corporativo.

Claramente, esta responsabilização deve ser acompanhada por uma educação e uma consciencialização "das consequências sociais de uma falta de responsabilidade para com a segurança pessoal e organizacional".

## 8.3 Recomendações Técnicas

Soluções de segurança devem contribuir para que se satisfaçam os critérios de segurança básicos, tais como integridade, disponibilidade e confidencialidade. Outros critérios que são frequentemente citados neste contexto são o de autenticação (o que torna possível verificar a identidade de uma entidade), "não-repúdio" e imputabilidade (que torna possível verificar que as acções ou eventos têm ocorrido).

### 8.3.1 Disponibilidade

Para garantir a disponibilidade dos serviços, sistemas e dados, os componentes da infra-estrutura devem ser adequadamente dimensionados e possuir a necessária redundância, além disso, a gestão operacional dos recursos e serviços devem ser prestados com rigor.

Disponibilidade é medida durante o período de tempo durante o qual o serviço prestado está operacional. O volume potencial de trabalho que pode ser tratado durante o período de disponibilidade do serviço determina a capacidade desse recurso (um servidor ou rede, por exemplo). A disponibilidade de um recurso está intimamente ligada à sua acessibilidade.

### 8.3.2 Integridade

A preservação da integridade do processamento de dados, ou serviços significa protegê-los contra modificação acidental e intencional, adulteração e destruição. Isto é necessário para garantir que eles permaneçam correctos e confiáveis.

Para evitar adulterações, uma forma de certificação permanente é necessária para garantir a imutabilidade durante o armazenamento ou transferência.

Integridade dos dados só pode ser garantida se os dados estão protegidos contra técnicas de *tapping*, que servem para modificar as informações interceptadas.

Este tipo de protecção pode ser fornecido recorrendo a mecanismos de segurança, tais como

- Protecção contra Vírus, *malware* e *botnets*.
- Controlos de acesso rigorosamente aplicados.
- Criptografia de dados.

### 8.3.3 Confidencialidade

A confidencialidade é a salvaguarda do sigilo da informação, fluxos de informação, operações, serviços ou acções realizadas no ciberespaço. A confidencialidade garante a protecção dos recursos contra a divulgação não autorizada.

Confidencialidade pode ser implementada por meios de controlo de acesso e criptografia.

(A criptografia ajuda a proteger a confidencialidade das informações durante a transmissão ou o armazenamento, transformando a mesma numa forma que é ininteligível para quem não possui os meios para decifrar a informação).

### 8.3.4 Identificação e Autenticação

O propósito de autenticação é remover qualquer incerteza sobre a identidade de um recurso. A autenticação pressupõe que todas as entidades (hardware, software e pessoas) estão correctamente identificadas e que certas características poderão servir como evidência de identificação para estas entidades.

Em particular, a lógica baseada em sistemas de controlo de acesso aos recursos de TI requer que a identificação e autenticação de entidades sejam adequadamente geridas.

Procedimentos de identificação e autenticação deverão ser implementados, a fim de ajudar a alcançar os seguintes pressupostos:

- Confidencialidade e integridade de dados (acesso a recursos é restrito a utilizadores autorizados e identificados, e os recursos são protegidos contra alterações por quaisquer entidades, excepto aquelas que estão autorizadas para o efeito);
- Não repúdio e imputabilidade (acções podem ser atribuídas a uma entidade identificada e autenticada), o rastreio de mensagens e transacções e comprovativos de destino.

### 8.3.5 "Não-repúdio"

Em algumas circunstâncias, é necessário verificar se um evento ou operação foi efectivamente realizada. Não-repúdio é um termo associado aos conceitos de responsabilidade, imputabilidade, rastreio e, em alguns casos, "auditabilidade".

Estabelecer a responsabilidade por determinado evento pressupõe a existência de mecanismos de autenticação de indivíduos e um método de atribuir os seus perfis às suas acções.

A possibilidade de gravação de informações para tornar possível rastrear a realização de uma acção torna-se importante quando há uma necessidade de reconstituir a sequência de eventos, especialmente para a realização de investigações.

As informações necessárias para realizar uma análise posterior, para fins de auditoria do sistema, precisa ser guardada (registo de informações) – o que se chama de "auditabilidade" do sistema.

### 8.3.6 Segurança Física

Os espaços onde estão localizados as estações de trabalho, servidores, áreas de TI e serviços necessitam de ser fisicamente protegidos contra acesso não autorizados e acidentes (incêndios, inundações, etc.)

Segurança física é o tipo mais fundamental e omnipresente do sistema de controlo de TI.

### 8.3.7 Aplicação das Regras básicas de cibersegurança

| O sistema deve… | Objectivos de segurança | Ferramentas de segurança |
|---|---|---|
| Ser usável | Disponibilidade<br>Sustentabilidade<br>Continuidade<br>Confiança | Dimensionamento<br>Redundância<br>Operações e procedimentos de Backup |
| Operar correctamente…. | Segurança de operações<br>Fiabilidade<br>Durabilidade<br>Continuidade<br>Operação correcta | Design<br>Performance<br>Ergonomia e Usabilidade<br>QoS (Qualidade de Serviço)<br>Manutenção operacional |
| Providenciar acesso a entidades autorizadas (bem como negar acessos desautorizados) | Confidencialidade<br>Integridade | Ferramentas de Segurança |
| …verificar acções | Autenticidades<br>Não-contestação<br>Não- repudiação | Dimensionamento<br>Redundância<br>Operações e procedimentos de Backup |

Tabela 8-1 Regras básicas de cibersegurança

# 9 Recomendações para debelar o problema da reputação

## 9.1 Recomendações aos ISPs

### 9.1.1 Fazer uma análise de ameaça ao Sistema de Reputação

Antes de conceber ou adoptar um sistema de reputação, uma análise das ameaças deve ser realizada, e os requisitos de segurança devem ser identificados.

As ameaças, e os respectivos ataques deverão ser vistos como distintos vectores de ameaça, precisando, por isso, de ser considerados no contexto da aplicação em particular ou no caso de uso, uma vez que cada elemento e entidade requerem segurança específica.

### 9.1.2 Desenvolver sistemas de reputação que respeitem os requisitos de Privacidade

Infelizmente o design dos sistemas actuais de reputação permite a geração de perfis de utilizadores, incluindo todos os contextos em que o utilizador esteve envolvido.

O anonimato do utilizador teria impacto positivo no aumento da precisão do sistema de reputação, uma vez que reduz ameaças, tais como extorsão, e reduz o medo comum de retaliação (face por exemplo, a exprimir uma opinião negativa num fórum).

Projectos de sistemas de reputação requerem que se averigúem e se sigam as melhores práticas em políticas de privacidade, pois tal permitirá, paralelamente, preservar a confiança fornecida às entidades pelo uso de reputações [Bauer, Van Eeten e Chattopadhyay (2008)].

Existem mecanismos que proporcionam a privacidade para os utilizadores e privacidade para os proprietários da reputação. Entre estes, por exemplo sistemas de gestão de identidade que ajudam os utilizadores a utilizar pseudónimos, são bastante úteis e eficazes.

### 9.1.3 Fornecer descrições das métricas de reputação

As métricas utilizadas para calcular e aferir a reputação de determinada entidade deverá ser aberto ao invés de fechado, para que estes sistemas possam ser avaliados pelo maior número possível de pesquisadores, em vez de se manterem em segurança através da obscuridade.

Da mesma maneira que uma agência de rating teria a ganhar se divulgasse quais os seus parâmetros de avaliação (ganhando com isso, avaliações externas e sugestões) da mesma maneira tal sucede com sistemas cujo objectivo é classificar pessoas, empresa e países.

### 9.1.4 Recomendações relativas ao interface de utilização

A usabilidade inerente aos sistemas de e baseados em reputação desempenha um papel importante, na medida em que transfere para o utilizador uma sensação de segurança e de domínio das tecnologias envolvidas, minimizando os erros e o desleixo.

Por exemplo, o sistema de reputação "comunitária" atribuído aos vendedores de produtos na Amazon.com deve à sua facilidade de utilização o seu sucesso e a sua implementação eficaz e abrangente.

Para atender a utilizadores com cada vez mais expectativas de "confiabilidade", os sistemas de reputação devem ser concebidas de tal forma que assegurem a transparência, para o utilizador facilmente compreender como a reputação é formada e atribuída (por exemplo, quais os factores que são levados em conta e qual a respectiva ponderação)

A "pesquisabilidade" também é um aspecto importante da usabilidade, uma vez que permite aos utilizadores inteirarem-se da própria reputação, bem como da reputação de outras entidades, com as quais interage, em determinado ecossistema.

Um sistema de reputação deve permitir que um utilizador personalize os componentes da reputação de forma a melhor acomodar as suas necessidades. Algo que também ajudaria à transparência.

Por exemplo, poderia ser possível subdividir determinada avaliação em diferentes atributos e permitir que o utilizador definisse um limite aceitável para cada um deles.

Outra personalização poderia ser permitir que o utilizador alterasse o peso das recomendações a ter em consideração, de acordo com a confiança que o próprio utilizador tem nesses pesos.

Também deveria ser possibilitado aos utilizadores um modo de avaliação qualitativa da reputação pois, do mesmo modo que a confiança está ligada à incerteza, as abordagens para determinar a confiança acabam por ser principalmente quantitativas, ainda que no ambiente da internet, tenham quase sempre de ser traduzidos quantitativamente, algo que acaba por ser difícil.

## 9.2 Recomendações aos governos e as Empresas

### 9.2.1 A Importância do E-government

Os governos não costumam utilizar sistemas de reputação automatizados, porém os decisores políticos devem ser encorajadas a investigar a possibilidade de usar sistemas "state-of-the-art", baseados em reputação, para os sistemas de governo electrónico.

Aplicações onde tal investigação pode valer a pena ser efectuada são aqueles relacionados com a habilitação e prova de serviços relacionados.

O exemplo típico é a emissão de um passaporte ou bilhete de identidade, que em alguns países exige testemunhas de confiança para atestar a associação de fotografia de um utilizador com o nome (um aspecto da sua reputação).

Por exemplo, no Reino Unido, pedidos de passaporte devem ser acompanhados por uma fotografia assinada por uma testemunha que tenha uma profissão respeitada.

Os governos devem examinar a possibilidade de automatizar e assegurar esses processos, aproveitando-os sistemas de reputação e a experiência em segurança adquirida em seu desenvolvimento.

Noutro exemplo, um modelo web-of-trust poderia ser usado como Autoridade de certificação para determinadas empresas.

As Empresas devem abraçar o potencial de sistemas de reputação:

- Para ajudar a diferenciar ou melhorar os seus produtos (por exemplo, pedindo feedback a clientes)
- Para tomar decisões business-to-business (por exemplo, quais os produtos a comprar para uso interno, quais os fornecedores de confiança, os parceiros de confiança, etc.)
- Para iniciar e / ou melhorar os modelos de negócios ou produtos subentendo-os a reputação externa e assim "homologando" os resultados.

### 9.2.2 Incentivar o Uso de Reputação

Sites online de Redes sociais são um dos maiores fenómenos tecnológicos de sempre. E estes estão constantemente ameaçados por cibercriminosos que pretendem, desde denegrir a imagem de uma empresa, até roubar os dados pessoais de um utilizador.

O uso de sistemas de reputação pode ser benéfico para enfrentar as ameaças vigentes.

Técnicas de reputação permitem a avaliação da "confiabilidade" e comportamental dos sistemas e dos próprios utilizadores.

A ENISA demonstrou a sua posição sobre os aspectos de segurança de Redes sociais, enumerando os possíveis benefícios de técnicas de reputação em websites Sociais, e não só:

> - *Filtragem de comentários maliciosos ou spam,*
> - *Filtragem de comentários com vista a aumentar a qualidade do conteúdo, aumentando a "confiabilidade" na partilha de dados e outros, com terceiros*
> - *Elaboração de relatórios sobre conteúdo impróprio ou com direitos de autor vigentes, de relatórios sobre perfis suspeitos, roubos de identidade, e relatórios versando diversos aspectos de comportamento inadequado*
> - *Reforço da actividade de moderação automática dos websites.*
> - *Aumento da percepção dos utilizadores na reputação, incentivando-os a tomar responsabilidade em construir comunidades mais honestas e mais auto-reguladas,*
>
> *[Enisa (2010)]*

**Promover acções de sensibilização**

Os utilizadores devem desenvolver habilidades para a compreensão de classificações de reputação e ganhar confiança percepcionando quais os processos, os motivos e as vantagens de utilizar determinado sistema de reputação.

Existem muitos cibercrimes cuja base dos ataques reside em adulterar, violar, usurpar ou enganar os sistemas de reputação defensores. De modo paralelo, os sistemas de reputação serão provavelmente a arma mais eficaz para garantir a segurança dos cidadãos e das empresas, pois muitos deles são baseados em comportamentos passados, humanos.

## 9.3 Requisitos de Segurança que minimizam os ataques à reputação de entidades

Uma série de requisitos de segurança para sistemas de reputação são identificados abaixo, e incluem requisitos que os utilizadores esperam de serviços que empregam sistemas de reputação, como seja a robustez contra ataques cibernéticos.

*Nota: Os requisitos aqui expostos agregam informações adaptadas de [Kurbalija Gelbstein (2005)] e [ITU (2007)]*

- **Disponibilidade** - Em particular, quando a reputação do sistema se torna fundamental para o funcionamento de todo o sistema. Sistemas centralizados poderão ser mais propensos a um único ponto de falha (a unidade central) do que sistemas descentralizados. Num sistema descentralizado, se entidades em quem o utilizador confia não estiverem disponíveis, então a reputação que pode obter dos seus pares pode ser insuficiente.

- **Integridade da Informação de Reputação -** Informações sobre a reputação devem ser protegidas de manipulações não autorizadas, tanto em transmissão como no armazenamento. Isso normalmente traduz-se em requisitos de segurança nas redes subjacentes - por exemplo, a protecção do canal de comunicação, a protecção do repositório reputação central, e a protecção ao nível de utilizadores, por exemplo, no caso de uso p2p onde a informação está dispersa por toda a rede. No mercado on-line de licitação, vendendo um item, a classificação de um membro em geral (como no eBay) precisa de ser confirmado por login com um *username* e uma palavra-chave, e em seguida, o canal é protegido por SSL.
  Além disso, a reputação de informações deve estar ligada a fontes "anonimizáveis" (por exemplo, nas redes p2p, a reputação dos pares não é necessariamente conhecida ou facilmente estabelecida).

- **Autenticação** - Torna-se obrigatório que uma entidade com direitos e acesso a um grupo ou rede deva estar devidamente autenticada (até para evitar as contribuições parciais para a avaliação de reputação da entidade como, por exemplo, em p2p redes). Além disso, a gestão de identidade e os seus mecanismos precisam de ser implementados para mitigar o risco de ameaças relacionadas com a mudança de identidade (ataques de *spoofing*, por exemplo).

- **Privacidade / Anonimato / Unlinkability -** A privacidade deve ser preservada, tal como o anonimato (em certas situações, como quando se expressa uma opinião ou se atribui uma pontuação). A privacidade deve ser garantida, tanto para o proprietário da reputação como para o eleitor e/ou utilizador da reputação.
  Infelizmente, os sistemas de reputação actualmente em uso permitem perceber qual a verdadeira identidade por detrás de um pseudónimo (um *username*) avaliando o interesse e comportamento do perfil (como tempo e frequência de participação, a valorização e o interesse em itens específicos). Mais comum é a tendência actual de se

ligarem os perfis de determinados websites com outros, normalmente de redes sociais, permitindo inclusive sistemas de SSO (Single sign-on - utilizar as mesmas credenciais de acesso em sistemas distintos) tornando ainda mais fácil a correlação.

- **Precisão -** O sistema de reputação deve ser preciso no cálculo dos ratings. Esta precisão também deve considerar o desempenho a longo prazo, ou seja, a métrica pode ser projectada de modo a que maus comportamentos menores e temporários se diluam com os bons comportamentos e não afectem significativamente a reputação (que poderia ser devido, por exemplo, a uma falha temporária, ou a um sistema comprometido).
  Outros aspectos incluem a solicitação (verdadeira) de feedback e a capacidade de distinguir entre um recém-chegado e uma entidade com uma má reputação estabelecida.
  No caso dos sistemas de anti-spam, o sistema deve ser ponderado relativamente aos eventuais falsos positivos (percentagem de emails legítimos erroneamente identificados como spam).

- **Usabilidade / Transparência -** Deve ser claro para ao utilizador como os votos de reputação são obtidos e o que eles significam.

- **Justiça -** Em particular, no mercado on-line, as propostas feitas são publicadas rapidamente; Isso ajuda os membros a verificar como estão sendo considerados a tempo de corrigirem e ajustarem ofertas. No entanto, os membros têm que confiar no provedor, para que o tempo de cada oferta ou venda seja registado com precisão e que as propostas listadas sejam feitas pelos membros listados.

- **Auto-correcção** - Poderá ser necessário, no caso da reputação global de cada membro estar ligada à opinião subjectiva dos eleitores, de proceder a auto-correcções na reputação. Por exemplo, botões de voto podem ser usados para relatar se um email declarado como spam o é efectivamente spam para o destinatário, ou dar a opção a um utilizador de uma firewall de Web de corrigir a classificação de um website. Outro aspecto da auto-correcção é a escolha apropriada do período durante o qual a reputação é estimada: uma estimativa durante um longo período permite ser construída uma forte reputação, o que pode fazer um evento isolado (como um email de spam) desprezível. A desvantagem é que uma entidade vai exigir mais tempo para corrigir uma reputação negativa.

- **Requisito de segurança nas redes básicas -** A rede básica deve ter mecanismos de segurança adequados no lugar de modo que os ataques a esta não comprometam o sistema de reputação. Tal torna-se importante pois existe uma possibilidade de aproveitar a fraqueza da infra-estrutura subjacente.

- **A eficiência de desempenho** - O sistema de reputação deve ter impacto mínimo no desempenho. Por exemplo, em ambientes descentralizados, tais como redes p2p, onde a informação da reputação está espalhada por todo a rede, pode haver um impacto sobre largura de banda e armazenamento.

- **"Confiabilidade"** - Deve abranger a confiança dos eleitores e utilizadores na reputação: mitigações possíveis incluem fazer uso de redes sociais existentes, e ponderação variável de acordo com recomendações.

- **Prestação de contas -** Cada entidade deve ser responsável em fazer avaliações de reputação. Além disso, cada membro deve ser responsável e responsabilizado pelas suas acções, mesmo que tenha o próprio sistema comprometido (com *botnets*) – assunto que deve ser lidado de maneira diferente e posterior.
  Se membros se comportam de maneira errada, punições devem ser consideradas, tanto dentro como fora do sistema. Por exemplo, num mercado on-line, os utilizadores podem reclamar sobre um comportamento injusto ao provedor. No caso do eBay, o membro desonesto recebe uma advertência e, após admoestações múltiplas, pode ser excluído da comunidade e inclusive ser sujeito a acções legais.

- **Protecção entidades bem-conectadas** - Entidades com uma capacidade superior de afectarem uma determinada reputação (por exemplo, aqueles com uma alta reputação de rating) são mais susceptíveis de ser atacados (Ataques distribuídos, por exemplo). Por exemplo no caso do anti-spam, é relativamente fácil identificar os endereços de correio electrónico mais valiosos e mais susceptíveis de serem corrompidos. Estes devem receber um maior nível de protecção já que comprometê-los coloca um alto risco na confiança / reputação da rede.

- **"Verificabilidade"** - Sempre que possível, a prova deve ser recolhida a partir da interacção que foi classificada, para demonstrar que a classificação é correcta ou pelo menos, tentou-o ser.
  Nos sistemas de anti-spam, as mensagens de spam são obtidas como prova. No mercado online, a prova é mais difícil de ser colectar se a troca disser respeito a bens físicos. Nestas situações, a fotografia pode constituir prova.

# *10* Formas de Implementação

*Nota: Este capítulo tem uma índole comercial, em acordo com a motivação da tese.*

## 10.1 A Implementação de um sistema de Anti-botnet

Cabe aos organismos reguladores nacionais darem os primeiros passos na criação de um sistema que proteja, ao nível nacional, os utilizadores.

A ANACOM, o CERT.pt, a FCCN ou outros, com o apoio natural do Governo, poderão adoptar as soluções já implementadas noutros países (com seja o caso flagrante da Alemanha) e "forçar" (ou pelo menos sugerir, e conceder vantagens aos aderentes) um sistema nacional Anti-Botnet.

O documento é explicativo nas vantagens para a população e para o país que uma medida deste género teria. Resta enumerar, do ponto de vista económico e de retenção de clientes, as vantagens que caberiam aos ISPs (para além da obrigação cívica):

## 10.2 Vantagens para os ISPs

Uma boa eficácia no combate ao spam e *botnets* nunca foi tão premente como agora, senão pelos motivos óbvios, pelo menos que este aumento do tráfego afecta negativamente a largura de banda e o armazenamento de dados disponíveis para os clientes.

Uma vez que os clientes esperam que os ISPs resolvam o problema, uma solução ineficaz afecta directamente a satisfação do cliente, provocando um aumento de abertura de chamadas no *helpdesk* e levando alguns clientes a encontrarem alternativas para a resolução do seu problema.

Esta insatisfação em alguns casos passa pela mudança de fornecedor do serviço.

Um produto que monitorize a rede de saída de um ISP e que consiga detectar, nos padrões mais comuns de comunicação, ou seja protocolos HTTP, SMTP e IP, actividade considerada suspeita. E que sobre estes acontecimentos, consiga identificar adequadamente os subscritores, então o proprietário desse produto (o ISP) poderá agir em conformidade e limitar a actividade. [Fortinet (2009)].

Além do factor óbvio de proteger o cliente, outras vantagens deverão ser consideradas:

### 10.2.1 Reputação na Internet

Nas situações em que os clientes ficam infectados por código malicioso e enviam de forma indiscriminada spam e *malware* para outros domínios da Internet, por vezes acontece que os destinatários se queixam a entidades na Internet que por sua vez colocam gamas de IPs em Listas negras. Este facto vai fazer com que algumas organizações temporariamente (períodos de um a dois dias) deixem de aceitar mensagens e tráfego vindas dessas gamas [Lüssi (2008)].

Parece também relevante referir que um dos caminhos que a indústria da segurança já tomou é o da utilização de mecanismos de reputação na tomada de decisão. Há medida que este caminho se tornar mais notório e universalmente aceite, os clientes dos ISPs não quererão aparecer associados a ISPs que não se preocupam com a sua reputação e a dos seus clientes.

### 10.2.2 Redução da taxa de abandono (Churn Rate)

A empresa Gartner num estudo de 2004 estimava que:

- 7% de *Churn Rate* num ISP está directamente relacionada com spam
- 36% dos utilizadores de Internet consideram mudar de ISP para reduzir o volume de spam
- 75% dos utilizadores de Internet consideram que o seu ISP deverá ser responsável por resolver os seus problemas de spam.

Dos dados acima referidos facilmente se constata que o spam é claramente um factor que contribui para o aumento do *Churn Rate* num ISP. Implementando um sistema eficaz de anti-spam é possível reduzir a taxa de abandono (*Churn Rate*).

### 10.2.3 Redução da utilização de largura de banda

Actualmente o tamanho das mensagens de spam situa-se aproximadamente entre os 5KB e os 20KB, embora o spam de imagem que recentemente tem surgido tenha vindo a provocar um aumento do valor médio do tamanho de mensagem.

Ao reduzir o número de mensagens de spam que chegam aos clientes consegue-se uma redução da utilização da largura de banda por dois motivos:

1. **Menos tráfego de email -** Como existem menos mensagens a serem entregues nos servidores que possuem as caixas de correio dos clientes, existirão menos dados a serem trazidos pelos clientes para os seus clientes de correio electrónico.
2. **Menos tráfego produzido por *zombies* -** Um *zombie* é um computador infectado com um *bot* ou outro tipo de código malicioso e que permite que mensagens de correio electrónico sejam enviadas através de si próprio. Hoje em dia é muito frequente este código malicioso que infecta a máquina do cliente colocar a mesma sob as ordens de um *spammer*. Este *spammer* sempre que entende pode dar instruções aos computadores que estão sob o seu comando para proceder a envios massivos de spam.

   Por outro lado, os computadores infectados tentam frequentemente comunicar com o seu "controlo" e/ou tentar infectar outros computadores enviando massivamente vírus.

Também existem Botnets que pretendem fazer ataques massivos de DDoS (tráfego imenso que bloqueia os sistemas de destino).

A poupança de largura de banda que se obtém com a redução do spam e da comunicação das Botnets pode libertar a infra-estrutura de rede para outro tipo de serviços.

### 10.2.4 Redução da utilização de espaço em disco

Uma vez que existe um número significativo de mensagens que podem ficar retidos nos servidores de recepção do correio electrónico, o espaço ocupado em disco pelos servidores onde se encontram hospedadas as caixas de correio dos clientes será substancialmente reduzido.

O espaço em disco poupado pode ser utilizado para outros fins, o que representa uma diminuição considerável em custos.

**Redução de custos com storage e backups**

Como foi explicado no ponto anterior, uma vez que o espaço ocupado pelos dados em disco diminui, o número de tapes necessárias para fazer o *backup* a todo o correio electrónico diminui igualmente. Consegue-se desta forma uma poupança significativa em termos da quantidade de tapes utilizadas. Ao reduzir também a janela de tempo para execução dos *backups* estamos também a diminuir a carga que o mesmo provoca em termos de performance, aumentando consequentemente a satisfação dos clientes.

### 10.2.5 Diminuição do tempo de reposição dos dados

Em caso de falha grave, uma vez que o tamanho dos *backups* dos dados do correio electrónico dos clientes são mais pequenos, o tempo necessário para fazer a recuperação dos dados será igualmente menor.

### 10.2.6 Possibilidade de oferecer serviços de valor acrescentado e segmentação da oferta.

Existem soluções de anti-spam que permitem disponibilizar comportamentos e funcionalidades distintas em função de atributos dos clientes, isto é, oferecer diferentes experiências de anti-spam conforme o produto adquirido pelo cliente.

Desta forma seria por exemplo possível oferecer aos clientes de topo a possibilidade de definirem:

- Os endereços de quem querem sempre receber as mensagens.
- Os endereços de quem nunca querem receber mensagens.
- Níveis de sensibilidade de decisão (mais ou menos agressiva).

### 10.2.7 Diminuição dos serviços para o suporte

A recepção de spam é um dos motivos que leva os nossos clientes a contactarem o suporte. Por vezes o spam é o motivo directo do contacto, pois os clientes queixam-se da recepção

excessiva de mensagens não solicitadas. Indirectamente o spam é também responsável pela abertura de chamadas no suporte. Ao aceder aos links sugeridos nas mensagens de spam, os clientes acabam instalando involuntariamente código malicioso nas suas máquinas.

Não raras vezes este código vai tornar os computadores dos clientes mais lentos e o acesso à Internet deteriora-se. Ao evitar problemas com os computadores dos clientes estamos a reduzir o número de vezes que estes recorrem ao suporte.

### 10.2.8 Redução do número de servidores necessários

Com a diminuição significativa do número de mensagens com que os clientes terão de lidar, baixa consideravelmente o processamento efectuado por parte dos servidores, conseguindo-se desta forma a redução do número de servidores necessários, nomeadamente, POP e IMAP.

# *11* Limitações ao Estudo

## 11.1 O impacto de eventuais medidas de segurança em ISPs na reputação do país e respectivos benefícios económicos

Partindo do princípio defendido por alguns autores [Brown (1998) citado pelos autores] de que a imagem da empresa se forma na mente de indivíduos de diferentes grupos e que poderão ter uma percepção diferente, ou ainda, [Van Riel (1998) citado pelos autores] a opinião de que não existe ainda um método capaz de medir todos os aspectos de "corporate reputation" [Davies, Chun, Silva, (2002)], e se alargamos a medição a um a pais, percebemos a dificuldade de medir a reputação do mesmo, para os diversos agentes económicos. Com se não fosse tal factor impeditivo o suficiente, adicionemos o hipotético cenário de que medidas são tomadas, pelos ISPs portugueses, para mitigar a cibercriminalidade em Portugal:

- Não é mensurável até que ponto iria a eficiência desta medida. Os crimes informáticos, em especial a componente técnica são muito mutáveis e com um grau de evolução espectacularmente elevado.
- Este documento não explora como iriam os agentes governamentais usufruir (ou, dito de outro modo, publicitar) da sua melhoria ao nível da segurança informática.
- Pelo observado em outros países, como a Alemanha ou o Japão, a melhoria da segurança dos cidadãos em Portugal seria, provavelmente, para equilibrar Portugal num ranking sobre os países mais seguros e, dificilmente (dado o diferencial de capitais técnicos e económicos, bem como o atraso temporal face a estes países pioneiros) suplantá-los. Significa isto que a melhoria supra mencionada permitiria a Portugal ser rotulado como um dos países mais seguros, integrando, metaforizando, um pelotão da frente. Parece claro as diferenças ao nível de reputação entre ser "o mais seguro" e ser "um dos mais seguros". Este impacto também não está avaliado.

## 11.2 A impossibilidade de dissociar eventuais melhorias na segurança dos ISPs com o meio envolvente

Assumindo, corroborando a tónica deste documento, que melhorando a segurança, em especial nos ISPs, tal terá um impacto significativo nas Reputações (virtuais e reais) dos próprios ISPs, das Empresas e do País, contribuindo para a segurança dos mesmos e para que a sociedade global determinassem estas entidades como mais seguras (que a média) e portanto como tendo um indicador positivo, Existem factores não previstos, por vezes nem estudados, na evolução e predisposição dos agentes económicos neste processo.

- Carece de conclusão determinística até que ponto ter uma internet segura é determinante para, por exemplo uma empresa farmacêutica se implementar em Portugal. Recorrendo ao léxico comum, cada caso é um caso e só podemos determinar, casuisticamente que, em empresas com conteúdo tecnológico, a segurança da infra-estrutura de comunicações electrónicas seria um factor considerável, logo após das considerações legais, geográficas, e sociais de um país.
- Carece de determinação até que ponto a interacção de um país, ou de uma empresa com a sociedade em geral, em particular a componente criminosa são apaziguariam a qualidade em termos de segurança desse país. Dito de outra maneira, se exceptuarmos as actividades criminosas com motivações económicas, todas as outras reacções (descredibilizar pessoas e entidades, motivações políticas e sócias) estão intimamente ligadas a acções prévias.
  Exemplificando, a Sony decerto usufruía de uma infra-estrutura segura, mas as suas acções (quando agiu legalmente contra hackers que desbloquearam a sua consola de jogos) fizeram convergir um conjunto muito elevado de ataques contra si, expondo até a mais pequena das fraquezas, e infligindo perda de reputação, não só para a Sony, mas para o país de onde esta provém.
  Se pensarmos que Portugal é relativamente benigno na maneira como o país, as empresas e os cidadãos se comportam na sociedade global (talvez Mourinho (pela animosidade que gera nos adeptos de futebol), Durão Barroso (pela influência nas políticas europeias), as políticas contra a Indonésia (o último grande caso português de animosidade de país contra país), e a Galp (pelo impacto ecológico) sejam as excepções), mas decerto haverão mais nos (micro) ambientes onde algumas empresas e pessoas se movem.

## 11.3 A divergência ente a imagem externa e a identidade interna de Portugal

"A imagem é influenciada pela experiência que os grupos externos têm com a organização enquanto a identidade é similarmente induzida pelas experiências de empregados no trabalho. Se a visão e a liderança da empresa forem apropriadas, a imagem e a identidade serão coincidentes" [Hatch e Shultz (2000)].

Esta citação permite deslindar outra das lacunas existentes na correcta avaliação do que uma eventual melhoria da segurança traria globalmente a Portugal, dada a natureza psicossocial dos seus habitantes, nomeadamente agentes de media e agentes políticos, possui, em certa medida, uma consagrada apetência nacional para minimizar e destronar os feitos atingidos internamente.

Existe alguma probabilidade, não mensurável, de que esta vantagem técnica, aos mínimos dissabores (problemas técnicos, problemas políticos, etc.) seja minimizada e o resultante "feedback" propagado internacionalmente, condicionando uma hipotética opinião (Imagem percepcionada) favorável que os agentes externos pudessem ter do País. Recorrendo a um exemplo fictício, um empresário poderia obter informação de que o sistema de comunicações electrónicas em Portugal seria muito seguro, estando a considerar implantar-se no país, seria "bombardeado" com opiniões e escândalos, quer sobre as funcionalidades técnicas, quer sobre as componentes políticas que rodeariam este tema.

# *12* Bibliografia


| **Bibliografia** | | | | |
|---|---|---|---|---|
| **tipo** | **Autor** | **Ano** | ***Título*** | **In** |
| | | | | |
| Livros | Amoroso, Edward G | 2011 | *Cyber Attacks - Protecting National Infrastructures* | Butterworth-Heinemann / Elsevier Inc. |
| Livros | Gillespie, Kate; Jeannet, Jean-Pierre; Hennessey, H. David | 2011 | *Global Marketing, Third edition* | Cengage Learning,inc |
| Working Papers | J. van Eeten, Michael; Bauer, Johannes M. | 2008 | *Economics of Malware* | OCDE - Organização de Cooperação e de Desenvolvimento Económicos |
| Patentes | Alcatel Lucent | 2010 | *Alcatel, Lucent, Patent registration, Infiltration of Malware Communication* | Alcatel-Lucent technologies, corp. |
| Teses | Asghari, Hadi | 2010 | *Botnet Mitigation and the Role of ISPs* | Delft University of Technology Faculty of Technology, Policy and Management Section Policy, Organization, Law and Gaming |
| Livros | Beal, Any; Strauss, Judy | 2008 | *Radically tranparent: Monitoring and Managing Reputations Online* | Wiley Publishing, inc, Indianapolis |
| Working Papers | CA Technologies | 2010 | *State of the Internet 2010: A Report on the Ever-Changing Threat Landscape* | CA Technologies |
| Publicação | Cardoso, Luís | 2008 | *Estratégia e Competitividade, 2ª Edição* | Editorial Verbo |
| Whitepaper | Cavallaro, Lorenzo ; Kruegel, Christopher; Vigna, Giovanni | 2009 | *Mining the Network Behavior of Bots* | *University of California, Santa Barbara* |
| Publicações | CERT.pt | 2010 | *Boas práticas de segurança para DNS* | FCCN - Fundação para a Ciência e Computação Nacional |

| | | | | |
|---|---|---|---|---|
| Livros | Click, Rick L.; Duening, Thomas N. | 2005 | *Business Process Outsourcing: the Competitive Advantage* | John Wiley & Sons, Inc |
| Publicações | da Silva, Rui Vinhas | 2010 | *Os Novos Desafios da Economia Global* | Caleidoscópio, Edições e Artes Gráficas, S.A. |
| Imprensa | Damballa | 2008 | *Damballa, Anatomy of a targeted attack* | Damballa corp. |
| Livros | Davies, Gary; Chun, Rosa; Silva, Rui V. da | 2002 | *Corporate Reputation Competitiveness , 1 ª Ed.* | Routledge, New York |
| Periódicos Científicos | ENISA | 2009 | *Network Resilience and Security: Challenges and Measures - Report of the ENISA Virtual Working Group on Network Providers' Resilience Measures* | ENISA |
| Periódicos Científicos | ENISA | 2011 | *Botnets measurement and defense* | ENISA |
| Periódicos Científicos | ENISA | 2010 | *What Are the Measures Used by European Providers to Reduce the Amount of Spam Received by Their Customers - Third ENISA Anti-Spam Measures Survey* | ENISA |
| Periódicos Científicos | ENISA | 2009 | *ENISA 2009 spam survey* | ENISA |
| Working Papers | EP3R Workshop | 2010 | *Non-Paper on the Establishment of a European Public-Private Partnership for Resilience (EP3R). EP3R Workshop, 2010.* | EP3R Workshop |
| Livros | Fertik, Michael; Thompson, David | 2010 | *Wild West 2.0: How to protect and restore your online reputation on the untamed social frontier* | American Management Association, NY, USA |
| Whitepapers | Fortinet | 2009 | *ISP Protection against BlackListing* | Fortinet corp. |
| Livros | Friedman, Thomas | 2007 | *The world is flat - A Brief History of the Twenty-first century* | Farrar, Straus, and Giroux, New York |
| Whitepapers | Gartner | 2010 | *Critical Capabilities for Secure E-Mail Gateways, Gartner* | Gartner, inc. |
| Whitepapers | Gartner | 2010 | *Effective Security Monitoring Requires Context, Gartner* | Gartner, inc. |
| Working Papers | Gartner | 2010 | *Hype Cycle for Infrastructure Protection, 2010, Gartner* | Gartner, inc. |
| Whitepaper | Gartner | 2010 | *Magic Quadrant for Secure Web Gateway, Gartner* | Gartner, inc. |

| | | | | |
|---|---|---|---|---|
| Working Papers | Goodman, Joshua ; Rounthwaite, Robert | 2004 | *Stopping Outgoing Spam - Microsoft Research* | MicrosoftResearch |
| Referências não publicadas retiradas da internet | Governo Alemão e parceria público-privada | - | *German Anti-Botnet Initiative [Online] http://www.botfrei.de* | |
| Periódicos Governamentais | Governo da República Portuguesa | 2004 | *Decreto-Lei n.º 7/2004* | Diário da República, Casa nacional da Moeda |
| Relatórios | Internet Crime Complaint Center | 2010 | *Internet Crime Report 2010* | I3c, National White Collar Crime Center, Bureau of Justice Assistance, Federal Bureau of Investigation |
| Publicações | ITU | 2007 | *Cybersecurity guide for developing countries* | International Telecommunications Union (ITU) |
| Referências não publicadas retiradas da internet | Kabay, M,E | 2011 | *http://www.networkworld.com/newsletters/sec/2011/081511sec1.html?source=NWWNLE_nlt_security_strategies_2011-08-16* | networkworld.com |
| Publicações | Kauffman Foundation | 2011 | *Rules for Growth - Promoting Innovation and Growth Through Legal Reform* | Ewing Marion Kauffman Foundation |
| Relatórios | Kroes, Neelie | 2011 | *The Internet belongs to all of us* | European Commission vice-President for the Digital Agenda, discurso em Bruxelas, 19 de Abril 2011 |
| Publicações | Kurbalija, Jovan; Gelbstein, Eduardo | 2005 | *Internet Governance* | DiploFoundation, Global Knowledge Partnership |
| Teses | Lüssi, Cécile | 2008 | *Signature-based Extrusion Detection* | Institut für Technische Informatik und Kommunikationsnetze |
| Working Papers | McAffee | 2011 | *Botnes Demystified and Simplified* | McAffee inc. |
| Referências não publicadas retiradas da internet | Miniwatts Marketing Group | 2011 | *http://www.internetworldstats.com/eu/pt.htm* | Miniwatts Marketing Group |

| | | | | |
|---|---|---|---|---|
| Relatórios | OCDE - Organização de Cooperação e de Desenvolvimento Económicos | 2002 | *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* | OCDE - Organização de Cooperação e de Desenvolvimento Económicos |
| Working Papers | OstermanResearch | 2010 | *Results of a Survey on 2010 Messaging Issues, Osterman Research 2010* | Osterman Research inc. |
| Working Papers | OstermanResearch | 2010 | *The importance of Web messaging* | Osterman Research inc. |
| Publicações Governamentais | Parlamento Europeu | 2011 | *Network Neutrality: Challenges and responses in the EU and in the U.S.* | Directorate-General for Internal Policies, European Parliament |
| Publicações Governamentais | Parlamento Europeu | 2011 | *Network Neutrality: Challenges and responses in the EU and in the U.S* | Directorate-General for Internal Policies, European Parliament |
| Legislação | Parlamento Europeu e Conselho Europeu | 2006 | *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications* | Parlamento Europeu e Conselho Europeu |
| Referências não publicadas retiradas da internet | Pingdom | 2011 | *http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/* | Pingdom.com |
| Whitepapers | Pivotal Veracity | 2009 | *What's in store at the ISPs 2009-2010* | Pivotal Veracity LLC |
| Relatórios | Radunovic, Vladimir | 2011 | *Network Neutrality in law: a step forwards or a step backwards?* | DIPLO: Internet Governance and Policy |
| Imprensa | Safenet | 2008 | *Safenet, Outbound Spam Prevention* | Safenet corp. |
| Referências não publicadas retiradas da internet | Sapo.pt | 2011 | *Sapo.pt / Notícias Tek / 21 de Julho de 2011* | Sapo.pt, Portugal Telecom |
| Referências não publicadas retiradas da internet | Sapo.pt | 2011 | *http://tek.sapo.pt/noticias/telecomunicacoes/governo_transpoe_directiva_das_comunicacoes_e_1169880.html* | Sapo.pt, Portugal Telecom |

| | | | | |
|---|---|---|---|---|
| Livros | Schultz, M.; Hatch, M.J.V Larsen, M.H. | 2000 | *The Expressive Organisation : Linking Identity, Reputation, and the Corporate Brand* | Oxford University Press, Oxford |
| Relatórios | Symantec Corporation | 2011 | *Norton Cybercrime Report 2011* | Symantec Corporation |
| Imprensa | Umbradata | 2011 | *Umbradata – noticia sobre o novo produto deles.* | Umbradata, ldt |
| Relatório | UMIC | 2010 | *A sociedade da Informação 2010* | UMIC |
| Publicações | Verizon; Google | 2010 | Verizon-Google Legislative Framework Proposal | Verizon; Google inc. |
| Livros | Wilson, Tony | 2011 | *Manage your online reputation* | International Self-Counsel Press Ltd. |
| Working Papers | Yu, Shu; de Haan, Jakob; Beugelsdijk, Sjoerd | 2011 | *Trade, Trust and Institutions* | CESifo Working Paper No. 3571 |


----Fim de Documento ----

ISCTE Business School
Instituto Universitário de Lisboa

MITIGAÇÃO DO MALWARE PARA O DESENVOLVIMENTO EMPRESARIAL EM PORTUGAL:

# ANEXO I

Rui Diogo Duarte Mendes Serra

Tese de Mestrado em Marketing

*Orientador:*
Prof. Doutor Rui Vinhas da Silva, Prof. Auxiliar,
ISCTE Business School, Departamento de Gestão

Lisboa, Novembro 2011

# Conteúdo

# 1 Revisão da Literatura: *Net neutrality*

O assunto da Net Neutrality (Neutralidade da rede) tem sido uma questão controversa nos Estados Unidos há vários anos, mas é cada vez mais debatido em outros lugares, como a UE, vários outros países europeus, e o governo japonês, todos os examinar o assunto da neutralidade.

Os opositores da neutralidade da rede alegam que as regras de neutralidade de rede são desnecessárias, propensas a reduzir o investimento na rede, e levar ao uso ineficiente de infra-estrutura existente. Regulamentos de neutralidade da rede também podem reduzir a inovação, diminuindo a utilidade de certas aplicações, tais como aqueles que requerem conexões em tempo real e, portanto, podem não funcionar correctamente sem a prioritização de pacotes, como VoIP ou aplicações de telemedicina.

Em princípio, um fornecedor de infra-estrutura pode ter um incentivo para se servir de um comportamento anti-concorrencial contra um provedor de conteúdo que concorre para fornecer o serviço: por exemplo, um provedor de banda larga que tenha o seu próprio video-on-demand pode ter um incentivo em degradar a qualidade de uma empresa que tenta vender um serviço similar. Tais comportamentos provavelmente violam as leis "*antitrust*" na maioria dos países industrializados, mas os defensores da neutralidade da rede argumentam que processos *antitrust* são geralmente muito lentos para que sejam eficientes.

Debates sobre a neutralidade da rede nos EUA têm se focado principalmente na regulamentação a respeito de como Fornecedores de banda larga poderiam gerir o preço e o tráfego nas suas redes. O debate na Europa, e na UE, em particular, preferiu concentrar-se na separação de papéis – redes obrigatórias e outros serviços -, movendo-se consequentemente num campo híbrido, no que toca a neutralidade.

Os defensores e opositores da neutralidade da rede em geral concordam que a concorrência pode atenuar preocupações da neutralidade da rede, pois os utilizadores poderiam simplesmente mudar de fornecedor, se não gostarem da maneira como um determinado prestador gere o tráfego de rede. Mas os políticos e os estudiosos divergem sobre o quanto a concorrência é suficiente e, especialmente, sobre a capacidade dos utilizadores discernirem se estão ou não a ser preteridos no acesso a, por exemplo, a largura de banda.

Apesar de ter suas origens num projecto governamental, a Internet tem-se desenvolvido, desde então, em ambiente liberto de regulamentação. Tem havido muitas tentativas de intervenção reguladora, a maioria dos quais sendo vistas como prejudiciais.

Os governos de muitos países menos desenvolvidos, têm tentado censurar o acesso a informação (pela internet) com variados graus de sucesso. O "Grande Firewall da China é muito discutido, mas muitos outros exemplos, de menor escala, existem no mundo. Empresas

de telecomunicações ocidentais que tentam deliberadamente bloquear informações de concorrentes é um procedimento com alguns casos conhecidos.

Eis algumas premissas que advogam aqueles que debatem os limites entre a regulação e a "desregulação" do mercado da internet e telecomunicações, e que advogam o direito a:

## 1.1 Net neutrality:

- A liberdade e a qualidade do acesso à Internet

"... De acordo com as disposições legislativas que estão em vigor, os ISPs de acesso à Internet devem ser obrigados a fornecer aos utilizadores finais:

  - A capacidade de enviar e receber o conteúdo da sua escolha;
  - A capacidade de utilizar os serviços e executar as aplicações da sua escolha;
  - Conectar o hardware e utilizar os programas de sua escolha, desde que não prejudiquem a rede;
  - Uma qualidade suficientemente alta e transparente de serviço. "

- A não discriminação entre os fluxos de tráfego Internet

"... Como regra geral, nenhuma diferenciaçãodeve ser feita entre a maneira como cada fluxo de dados individuais é tratado, de acordo com o tipo de conteúdo, o serviço, a aplicação do dispositivo ou o endereço do fluxo de origens ou destino. Isso aplica-se a todos os pontos ao longo da rede, incluindo pontos de interconexão. "

- Supervisão de Internet e mecanismos de gestão de tráfego

"... Quando os ISPs não empregarem mecanismos de gestão de tráfego para garantir o acesso à Internet, que estejam em conformidade com os princípios gerais de relevância, proporcionalidade, eficiência, não discriminação entre as partes e transparência. "

- Gestão de serviços

Para manter em todos os intervenientes a capacidade de inovar, todos os operadores de comunicações electrónicas devem ser capazes de oferecer ao mercado uma gestão de serviços própria ou delegada, no acesso à Internet, para utilizadores finais e fornecedores de serviços da sociedade da informação, desde que o serviço gerido não degrade a qualidade do acesso à Internet e mantenha um certo nível satisfatório, forçando os fornecedores a agir de acordo com as leis da concorrência existentes bem como a regulamentação específica do sector. "

- Aumento da transparência para os utilizadores finais

"... Informações claras, precisas e relevantes sobre: os serviços e aplicações que podem ser acedidos através destes serviços de dados, a sua qualidade de serviço, as suas possíveis limitações, e todas as práticas de gestão de tráfego.

  - O termo "Internet" não pode ser usado para justificar os serviços e as informações, ou a falta destas.
  - O termo "ilimitado" não pode ser usado para descrever ofertas de serviços que incluam "fair use" e outras limitações do tipo que resultem em acesso que se corta temporariamente ou uma facturação extra ara os serviços, ou uma degradação excessiva de velocidades de acesso ou a qualidade do serviço. "

Quando a regulação é deficitária (propositadamente ou não) no fomento de concorrência, causando acessos à Internet limitados e relativamente caros, o resultado são monopólios de telecomunicações locais, que restringem facilmente o acesso (à internet, a redes telefónicas e a televisão), simultaneamente impossibilitando infra-estruturas de maior e melhor qualidade tornando esses sítios (e as pessoas que usam a infra-estrutura) altamente susceptíveis a ataques.

É interessante verificar que os locais que mais criam impedimentos aos utilizadores, normalmente se vêem mais facilmente comprometidos.

Podemos supor vários motivos, mas destacar-se-ia que uma sociedade onde não existe a proliferação livre de informação, também não usufrui dessa informação para se proteger.

Ninguém pode garantir que foi de facto a China ou o Paquistão que perpetrou ataques a países rivais. Pois, enquanto Estados, nenhum destes países está devidamente preparado para impedir de ser sabotado. E de ter alguém a fazer-se passar por estes países.

Na mesma lógica, E simulando uma teoria de conspiração cuja falta de dados credíveis deve desconsiderá-la, quando a agência de rating Moody's baixou o rating de Portugal e, horas depois, viu o seu website comprometido (bloqueado, e com mensagens de protesto em Português) ninguém poderá assumir que foi de facto alguém português que fez o ataque. Portugal (os seus cidadãos) tinha motivos e meios para isso mas, no inseguro mundo da internet, também alguém com interesse em desprestigiar Portugal, ou desprestigiar a Moody's, ou mesmo provar à Moody's a insegurança do seu website, usufruiriam com o sucedido.

Com a proliferação dos crimes na internet, em especial com a utilização de *bots* (que permitem esconder e/ou encapsular a identidade do verdadeiro atacante) o tipo de ataques cibernéticos de proveniência insolúvel é cada vez maior e mais inteligente, causando danos gravosos quer nos destinatários dos ataques, mas também nos hipotéticos atacantes.

Tem havido controvérsia na aplicação de leis e inteligência com finalidades de vigilância da internet.

Na década de 1990, a administração Clinton tentou controlar a criptografia, algo que a indústria viu como uma ameaça não apenas à privacidade, mas ao crescimento de e-commerce e outros serviços online.

Então, o governo Clinton fez promulgar a lei Law Enforcement Act (CALEA), em 1994, com a obrigatoriedade de cooperação entre os operadores de telecomunicações e o governo, para escutas telefónicas e registos ("logging") da actividade de utilizadores na internet.

A UE seguiu esse caminho aplicando directivas relativas à conservação de escutas telefónica, e mesmo mensagens de email.

Os governos que se preocupam com a infra-estrutura crítica nacional podem ver a regulamentação da Internet como uma questão de Segurança Nacional, assim como a introdução de graus de sigilo e organizações sombrias, que não fazem nada para dissipar as preocupações sobre a motivação.

Seja qual for a motivação, as políticas do governo são muitas vezes formuladas com contribuição técnica e científica insuficientes e muitas vezes aparentam não ter noção da realidade ou dos meios ideais para combater o cibercrime e ciberterrorismo.

A verdade é que o mercado não parece oferecer incentivos para manter a resiliência do sistema de intercomunicações num nível socialmente óptimo. Para além deste factor, as tentativas de enfrentar qualquer uma das questões por regulamento é dificultada por uma série de factores:

- **A falta de boas informações sobre o estado e o comportamento dos sistemas** - É difícil determinar quais os assuntos e materiais susceptíveis de serem averiguados. É difícil determinar qual o efeito que uma dada iniciativa é susceptível de ter – será boa ou má para a sociedade e a proliferação da internet
- **A escala e a complexidade do sistema** - A escala global pode tornar ineficazes as iniciativas locais, enquanto que a complexidade significa que é difícil prever como o sistema irá responder e adaptar-se a uma dada iniciativa.
- **A natureza dinâmica do sistema** - Facilmente emergem componentes importantes, sob a internet, que tornam a sua evolução imprevisível. Os utilizadores (e os criminosos) adaptam-se e acolhem estas mudanças com maior rapidez do que as forças de segurança e governos. Como exemplo, a popularidade súbita do *videostreaming* (como o Youtube) que originou diversos problemas, quer ao nível das conexões e largura de banda, quer à possibilidade de explorar falhas e introduzir *malware* nos vídeos.

Até agora, a falta de incentivos para fornecer resiliência (e em particular para fornecer excesso de capacidade) tem sido relativamente pouco importante: a Internet tem vindo a crescer tão rapidamente que se afastou muito longe do ponto de equilíbrio, e assumiu-se simplesmente que seria um ecossistema praticamente incontrolável, devendo-se concentrar esforços em sistemas críticos. E deixar que as empresas se auto-regulem (por estarem a competir pelos clientes, num mercado totalmente aberto, e por existirem recursos ilimitados – como largura de banda).

Mas é preciso salientar que a liberalização, privatização e reestruturação de serviços públicos em todo o mundo levou à fragmentação institucional numa série de indústrias de infra-estruturas críticas que poderiam, em teoria, sofrer de degradação da "confiabilidade" e resistência contra a mesma.

Existe uma percepção global que, num mercado tão libertino como o da Internet, o Governo deveria posicionar-se de determinada maneira. Alguns consideram que deveria haver uma regulação eficaz, outros que deveria simplesmente ser um espectador que, no máximo balizaria com grande folga a actividade neste ecossistema.

Existem, no entanto, duas ideias que têm vindo a ganhar forma:

- Que os governos devem incentivar que determinadas empresas (como os ISPs) estejam suficientemente capacitados para lidar com os problemas de segurança na internet e
- Que os governos devem agir como último recurso, estando sempre presentes, e com uma monitorização, directa ou indirecta, do espaço da internet e das telecomunicações. A recente crise económica ensinou que deixar um mercado entregue a si próprio, com grandes índices de competitividade e globalização, poderá causar a implosão do mesmo, fruto da disparidade no comportamento (muitas vezes ilícito) de alguns.

### 1.1.1 Casos existentes debruçando o tema da Net Neutrality

Em 9 de Junho de 2011, a Holanda tornou-se no primeiro país a implementar o princípio da neutralidade da rede para o direito nacional, garantindo que as telecomunicações e os Fornecedores de Internet não colocariam restrições de acesso ao utilizador, ou discriminassem qualquer utilizador com base nos tipos de conteúdo de Internet, serviços ou aplicações.

Em certa medida, estas medidas funcionam como retaliação ao abuso de poder verificado, sendo conhecidos casos em que fornecedores de telecomunicações Holandeses abertamente bloqueavam o acesso ao Skype e sistemas similares de VoIP, dando primazia aos seus próprios serviços de VoIP.

Violações semelhantes dos princípios da neutralidade da rede são feitas pelos ISPs e Telcos em muitos outros países. Restringir o acesso a algumas aplicações online e serviços é uma maneira um tanto rude para proteger os seus próprios interesses, criando claramente uma antipatia com o consumidor, mas existem abordagens mais sofisticadas, como o controlo de tráfego inteligente para algumas aplicações, em detrimento de outras, o *throttling* (reduzir propositadamente o tráfego) baseado em reputação e nos serviços utilizados e um conjunto de planos de negócio que beneficiam uns serviços em detrimento de outros.

Se, claramente, isso incomoda e preocupa os utilizadores - que reclamam uma Internet aberta com acesso irrestrito a qualquer aplicação on-line, conteúdo ou serviço - Por outro lado, e compreensivelmente, as empresas de telecomunicações e ISPs procuram modelos de negócios que garantam retornos adequados sobre os seus investimentos em infra-estrutura, e precisam de motivar os utilizadores a investir mais (nas aplicações), a fim de fornecer o serviço com uma qualidade devida.

Governos e reguladores enfrentam o desafio de encontrar o equilíbrio.

Um dos principais desafios é agir preventivamente, a fim de prevenir possíveis violações do princípio da neutralidade da rede, ou para responder com base em precedentes uma vez que o problema ocorra. Outro desafio é se o problema deve ser tratado com "hard law" – legislação e dispositivos legais, bem como penalidades - ou se "soft laws" (directrizes e políticas) seriam suficientes.

As opiniões são muito divergentes: “Telcos” e ISPs frequentemente defendem que as leis de concorrência de telecomunicações e as directivas *antitrust* e anti-monopólio são respostas mais que suficientes para lidar com a “Net Neutrality”. Paralelamente, grupos de consumidores e de empresas de software (fora das boas graças dos ISPs) consideram precisamente o contrário.

O problema é que existe uma notória falta de concorrência neste sector. Poucos ISPs controlam a maioria dos acessos à Internet.

Por exemplo, o problema dos EUA com a falta de concorrência nas Telecomunicações é público e notório: a Federal Communications Commission (FCC) está em luta há muitos anos com as principais “Telcos” para forçar a aplicação dos seus princípios de Neutralidade.

O Japão, que prevê o congestionamento da rede em breve, devido ao rápido crescimento dos serviços de banda larga, fomenta abertamente a criação de concorrência esperando, em paralelo, que a neutralidade da rede surja com os novos intervenientes.

A União Europeia, que tem uma concorrência sólida e um abrangente quadro jurídico sobre as telecomunicações, forneceu ainda assim directrizes para as autoridades reguladoras nacionais promoverem "a capacidade dos utilizadores finais em acederem e distribuírem informações ou executar aplicações e serviços da sua escolha," isto no âmbito da sua Directiva-Quadro alterada no final de 2009 (ainda continua a ser muito cautelosa para não pôr em perigo as inovações e investimentos das empresas).

A Declaração do Comité de Ministros do Conselho da Europa sobre a neutralidade da rede no final de 2010 claramente apoia os princípios da Net Neutrality, e tenta agregar os Estados membros e o sector privado para trabalharem ainda mais sobre estas orientações, esperando atingir um compromisso. Nenhuma das abordagens, no entanto, apela a um dos pólos, mas sim a posições intermediárias.

As directrizes mais bem sucedidas são as Directrizes da autoridade reguladora da Noruega (NPT): um regulamento macio baseado no diálogo de colaboração com a indústria da Internet e com comunidade. Voluntária, mas amplamente apoiada, esta nova abordagem "colaborativa" à regulamentação da Internet está a ter algum sucesso. Talvez porque, em última instância, os reguladores poderão sempre optar por transformar a Directriz em lei vigente, e dura, caso falhem os princípios colaborativos previstos.

A Holanda, que claramente escolheu um dos lados, aplicou uma legislação dura e efectiva, que certamente irá satisfazer os utilizadores, A questão aqui é se esta lei vai abalar as políticas de investimentos das “Telcos”, que terão de equilibrar os seus produtos e serviços com quaisquer outros disponíveis na internet. Se isso acontecer, os holandeses poderão precisar de reverter a sua política para uma abordagem mais equilibrada.

### 1.1.2 Como o debate de Net Neutrality influi na Segurança das Empresas e dos Países

Tentando enquadrar o assunto, muito debatido, e bastante importante, da Net Neutrality, no vértice Segurança - Reputação dos países, é possível perceber quais os pontos de contacto:

- Um ambiente neutral facilita a proliferação de actos cibercriminosos na rede. A pirataria e o envio de spam são algumas das faces visíveis.
- Por outro lado, restringir o acesso a determinados sistemas é sempre uma má política de segurança, se estivermos a falar de outros antivírus, ou outras listas de reputação. Existe um princípio claro e clássico da segurança na internet que diz que quanto mais camadas de segurança distintas (em função, em fabricante, etc.) existirem, melhor será a segurança. Ser obrigado a adoptar determinados sistemas e contraproducente e, a médio prazo, perigoso, pois será nesses sistemas que os cibercriminosos se empenharão em ultrapassar.
- Saliente-se ainda que parte dos cibercriminosos agem por motivações ideológicas, e não económicas: Países e ISPs, com políticas, digamos, totalitaristas, serão sempre alvos preferenciais para este tipo de terrorismo, com impacto em toda a comunidade.

No caso particular da reputação de um país como seguro e aprazível para se fazer negócios, qualquer um dos vértices da discussão tem vantagens e desvantagens. Dir-se-ia que depende de empresa para empresa, se prefere um ecossistema mais balizado, seguro e confinado, gerido por poderosos e tecnicamente evoluídos ISPs, ou se prefere a liberdade de utilizar múltiplos sistemas, sem restrição e frequentemente com outras vantagens (de por exemplo utilizar programas gratuitos). Numa perspectiva paralela, se o negócio das empresas implicar uma presença na internet (cada vez mais frequente) será benéfico que os utilizadores acedam aos seus produtos e serviços tão facilmente.

# *2* Research Design: Determinando o impacto da Internet na Sociedade

A quantidade e qualidade da informação disponível, em especial na Internet, torna qualquer tentativa de compilar os demais dados como parcial e infrutífera. Em especial porque governos e organismos de direito público (como a ANACOM ou a FCCN em Portugal, e a ENISA e a Comissão Europeia, na Europa) produzem exaustivos compêndios sobre o tema.

Resta sim, tentar agregar, compilar e resumir a informação com os seguintes objectivos, em acordo com a revisão da literatura:

- Perceber, com recurso a estatísticas, a dimensão do problema, paralelizando com a importância crescente da internet
- Perceber, no nosso contexto (Português), quais as medidas tomadas, em especial no âmbito governamental (legislação) e ISPs (medidas a tomar).

## 2.1 O potencial da internet

Eis alguns dados que permitem aferir o impacto da internet na vida comunitária global:

**E-mail**

- 25% - Percentagem de contas de e-mail que são corporativos.
- 89,1% - A proporção de e-mails que eram spam.
- 107 Mil biliões - O número de e-mails enviados pela Internet em 2010.
- 294000000000 - Número médio de mensagens de e-mail por dia.
- 1880000000 - O número de utilizadores de e-mail em todo o mundo.
- 480 Milhões - Novos utilizadores de e-mail desde o ano anterior.
- 262000000000 - O número de e-mails de spam por dia (assumindo 89% são spam).
- 2900000000 - O número de contas de e-mail em todo o mundo.

> *Acerca do e-mail, o The Radicati Group, numa pesquisa de mercado de tecnologia (...) estima que 247 bilhões (= mil milhões) de e-mails por dia foram enviados em 2009 (dos quais 81 por cento foram Spam)*
>
> *O Grupo Radicati também estimou que a média dos colaboradores das empresas envia e recebe cerca de 110 mensagens diárias, e cerca de 18 por cento dos e-mails são Spam, o que inclui Spam real e o que é denominado graymail (ie, boletins indesejados, alertas).*
>
> *Manage Your Online Reputation Tony Wilson2011 by International Self-Counsel Press Ltd.*

**Websites**
- 255 Milhões - O número de websites adicionados depois de Dezembro de 2010.
- 21400000 - Sites adicionados em 2010.

**Servidores Web**
- 39,1% - Crescimento no número de websites Apache em 2010.
- 15,3% - Crescimento no número de websites IIS em 2010.
- 4,1% - Crescimento no número de websites nginx em 2010.
- 5,8% - Crescimento no número de websites Google GWS em 2010.
- 55,7% - Crescimento no número de websites Lighttpd em 2010.

**Servidores Web** e **Nomes de domínio**
- 88800000 - Nomes de domínio .com no final de 2010.
- 13200000 - Nomes de domínio .net no final de 2010.
- 8,6 Milhões - nomes de domínio .org no final de 2010.
- 79,2 Milhões - O número de domínios com código de país, de nível superior (por exemplo, CN, UK, DE, etc.).
- 202 Milhões - O número de nomes de domínio em todos os domínios de nível superior (Outubro 2010).
- 7% - O aumento nos nomes de domínios desde o ano anterior.

**Utilizadores de internet**
- 1970000000 - Internet de utilizadores no mundo (Junho de 2010).
- 14% - Aumento de utilizadores de Internet desde o ano anterior.
    - 825100000 - Utilizadores da Internet na Ásia.
    - 475100000 - Utilizadores de Internet na Europa.
    - 266200000 - Utilizadores de Internet na América do Norte.
    - 204700000 - Utilizadores de Internet na América Latina / Caribe.
    - 110900000 - Utilizadores da Internet na África.
    - 63200000 - Utilizadores de internet no Oriente Médio.
    - 21300000 - Utilizadores da Internet na Oceânia / Austrália.

**Social Media**
- 152 Milhões - O número de blogs na internet (como rastreado por BlogPulse).
- 25000000000 - Número de tweets enviados no Twitter em 2010
- 100 Milhões - Novas contas adicionadas ao Twitter em 2010
- 175000000 - Pessoas no Twitter em setembro de 2010
- 7.700.000 - Pessoas seguindo @ ladygaga (Lady Gaga, o utilizador mais seguido do Twitter).
- 600 Milhões - Pessoas no Facebook, no final de 2010.
- 250 Milhões - Novas pessoas no Facebook, em 2010.
- 30000000000 - Pedaços de conteúdo (links, notas, fotos, etc.) partilhados no Facebook, por mês.
- 70% - Percentagem de utilizadores do Facebook localizados fora dos Estados Unidos.

- 20 milhões - O número de aplicações do Facebook instalados diariamente.

**Vídeos na Internet**

- 2000000000 - O número de vídeos assistidos por dia no YouTube.
- 35 - Horas de vídeo enviadas para o YouTube a cada minuto.
- 186 - O número de vídeos on-line vistos, em media, por utilizadores da Internet, por mês (EUA).
- 84% - Percentagem de utilizadores de internet que assistir a vídeos on-line (EUA).
- 14% - Percentagem de utilizadores de Internet que enviou vídeos on-line (EUA).
- >2 Mil milhões - O número de vídeos assistidos por mês no Facebook.
- 20000000 - Vídeos carregados para o Facebook por mês.

**Imagens**

- 5000000000 - Fotos hospedadas pelo Flickr (Setembro 2010).
- > 3000 - As fotos enviadas por minuto para o Flickr.
- > 3 Mil milhões - Fotos adicionadas por mês para o Facebook.
- 36000000000 - No ritmo actual, o número de fotos enviadas para o Facebook por ano.

### 2.1.1 Estatísticas de Portugal

- População: 10,760,305 (2011)
- Área geográfica de Portugal: 92,391 km2.
- Utilizadores de internet: 5,168,800 (Junho 2010) com uma taxa de penetração de 48.0%.
- Utilizadores de Facebook: 3,869,780 (Junho 2010) com uma taxa de penetração de 36.0%.

*(Miniwatts Marketing Group [2011])*

| Ano | Utilizadores | População | % Pop. | Fonte |
|---|---|---|---|---|
| 2000 | 2,500,000 | 10,318,084 | 24.2 % | ITU |
| 2004 | 3,600,000 | 10,463,170 | 34.4 % | CIA |
| 2006 | 6,090,000 | 10,501,051 | 58.0 % | Comp. Ind. Almanac |
| 2007 | 7,782,760 | 10,539,564 | 73.8 % | IWS |
| 2010 | 5,168,800 | 10,735,765 | 48.1 % | ITU |

Table 2-1 Estatísticas de Portugal

- No final de 2010, a penetração do acesso à Internet em banda larga na população atingiu 44% (quase o quádruplo do final de 2004), 20% em acessos fixos (41%, cerca de três vezes e meia a que era no final de 2004) e 24% em acessos móveis (mais de 37 vezes o valor do final de 2005). O aumento de clientes de banda larga móvel explodiu de 2005 para 2009.
- Em penetração de banda larga fixa na população na UE27, Portugal (15%) era no final de 2010 o 5º país em ligações maiores ou iguais a 10 Mbit/s, ex-aequo com a

Suécia e a seguir apenas a Holanda (22%), Dinamarca (19%), França (18%) e Bélgica (18%), e com um valor 1,5 vezes a média da UE27 (10%).

- O acesso a serviços de subscrição de TV digital por cabo, satélite ou fibra óptica é uma nova realidade, com 23% de penetração nos agregados familiares, quase o triplo do que era dois anos antes e ultrapassando a penetração da TV analógica por cabo.
- 45% dos agregados familiares possuem computadores portáteis, muito mais do triplo de 2005 (era 12%) e mais do dobro de três anos antes (era 20%), uma óbvia consequência positiva dos programas governamentais de apoio à aquisição de computadores portáteis para estudantes.
- 50% dos agregados familiares dispõem de ligações em banda larga à Internet, muito mais do dobro de 2005 (era 20%).
- 96%, 92% e 34% das pessoas (de 16 a 74 anos) com, respectivamente, habilitação superior, secundária, e de 9º ano ou inferior, utilizam Internet. Portugal ocupa nestes indicadores, respectivamente o 6º, 4º e 22º lugar na UE27. Os valores destes indicadores para Portugal são superiores às médias da União Europeia (UE) para pessoas com habilitação superior e com habilitação secundária, as quais são 92% e 74%, respectivamente, neste último caso com uma grande diferença. A percentagem de utilizadores da Internet nas pessoas com habilitação inferior a secundária é baixa (34%) mas mais do que duplicou desde 2005, com aumentos especialmente elevados nos grupos de idades 55-74 anos (agora o valor é superior ao quíntuplo de 2005), e 25-54 anos (valor muito superior ao dobro de 2005), e atingindo um valor 1,4 vezes o que era em 2005 no grupo de idades 16-24 anos. A percentagem de utilizadores da Internet nas pessoas de idades 55-74 anos é baixa (20%) mas aumentou para mais do quíntuplo de 2005 nas pessoas com habilitação inferior a secundária, para muito mais do dobro de 2005 nas pessoas com habilitação secundária, e atingiu um valor 1,6 vezes o que era em 2005 nas pessoas com habilitação superior.
- 97%, 94% e 40% das pessoas (de 16 a 74 anos) com, respectivamente, habilitação superior, secundária, e de 9º ano ou inferior, utilizam computador. Portugal ocupa nestes indicadores, respectivamente o 3º, 3º e 22º lugar na UE27, nas pessoas com habilitação superior apenas abaixo da Holanda (99%) e do Luxemburgo (99%), e nas pessoas com habilitação secundária apenas abaixo da Holanda (96%) e França (95%). Os valores destes indicadores para Portugal são superiores às médias da UE para pessoas com habilitação superior e com habilitação secundária, dado que estas médias são 93% e 77%, respectivamente, neste último caso com uma grande diferença. A percentagem de utilizadores de computador nas pessoas com habilitação inferior a secundária é agora 1,7 vezes o que era em 2005. 95% e 100% dos estudantes usam, respectivamente, Internet e computador. São resultados de uma eficaz introdução da Internet e de computadores nas escolas, depois de Portugal ter sido em 2001 um dos países pioneiros na Europa na ligação de todas as escolas à Internet, assim como no início de 2006 foi um dos países pioneiros na Europa na ligação de todas as escolas públicas em banda larga. 75% das pessoas que utilizam a Internet declaram utilizá-la todos os dias ou quase todos os dias, 1,3 vezes o que era em 2005. As actividades realizadas na Internet indicadas por mais utilizadores são as de pesquisa de informação sobre bens e serviços (86%), de comunicação, interacção e colocação de conteúdos – correio electrónico (88%), chats, Messenger, fóruns e semelhantes (69%) –, de consulta da Internet com o propósito de aprender (77%), de pesquisa de informação sobre saúde (59%), de procura de informação sobre educação ou formação (57%), de download/leitura de jornais/revistas (56%), de audição/visão de rádio/TV (50%), de download de software (46%), de download de jogos, imagens ou música (44%), de pesquisa de informação traduzida em compras offline (42%), de obtenção de

informações de organismos da Administração Pública (40%), de colocação de conteúdo pessoal num sítio na Internet (40%), de home banking (38%). Os maiores aumentos da utilização da Internet de 2005 para 2010 observaram-se em: telefonar/contactar por videoconferência (muito mais do dobro de 2005; agora 26%), desenvolvimento de blogs (mais do dobro de 2005; agora 14%), pesquisa de informações sobre a saúde (quase o dobro de 2005; agora 59%).  74% das pessoas utilizam o Multibanco. As transacções de comércio electrónico pelo Multibanco realizadas por estas pessoas incluíram carregamentos de telemóvel com saldo (75%) e compras de bilhetes para espectáculos e transportes (11%). 33% das pessoas que fazem transacções de comércio electrónico em páginas da Internet pagam encomendas através do Multibanco. 71% dos utilizadores de Multibanco realizam por este meio vários outros tipos de pagamentos: de serviços de fornecimento de água, luz, telefone, TV por cabo, etc., de compras de bens e serviços, de impostos, prestações para segurança social, multas, etc. ao Estado. 62% das pessoas realizam comércio electrónico através de Multibanco, páginas da Internet ou sistemas de identificação por rádio frequência nos três meses anteriores ao inquérito, e 58% através de Multibanco ou páginas da Internet. O comércio electrónico realizado através do Multibanco (por mais de 55% dos indivíduos e mais de 75% dos utilizadores do Multibanco) excede largamente as encomendas através de páginas na Internet. Na verdade, estas são realizadas por apenas 10% dos indivíduos, mesmo sendo muito mais do dobro de 2005, e embora 44% dos indivíduos (86% dos utilizadores da Internet) pesquisem informações sobre bens e serviços na Internet, uma percentagem 1,7 vezes a de 2005 (era 26%).

- Relativamente aos jovens de 10 a 15 anos de idade, destacam-se como principais resultados os seguintes: 91% dos jovens de 10 a 15 anos utilizam Internet, raparigas e rapazes. A utilização de Internet é de 100% nos jovens no 3º ciclo de escolaridade básica. 84% dos jovens de 10 a 15 anos utilizam Internet em casa, muito mais do dobro de 2005 (era 32%). 67% dos jovens de 10 a 15 anos declaram utilizar a Internet todos os dias ou quase todos os dias, quase o triplo de 2005.  As principais actividades de jovens de 10 a 15 anos que utilizam Internet são: pesquisa de informação para trabalhos escolares (97%), mensagens em chats, blogs, websites de redes sociais, newsgroups, fóruns de discussão online ou mensagens escritas em tempo real (86%), correio electrónico (86%), jogos ou download de jogos, imagens, filmes ou música (79%), consulta de websites de interesse pessoal (63%), colocação de conteúdo pessoal num website para ser partilhado (55%), pesquisa de informação sobre saúde (47%). 96% dos jovens de 10 a 15 anos utilizam computador, tanto raparigas como rapazes. A utilização de computador é de 100% nos jovens no 3º ciclo de escolaridade básica. 92% dos jovens de 10 a 15 anos utilizam computador em casa, 1,6 vezes o valor de 2005. 77% dos jovens de 10 a 15 anos declaram utilizar computador todos os dias ou quase todos os dias, 1,7 vezes o valor de 2005. As actividades indicadas por mais jovens de 10 a 15 anos que utilizam computador são: trabalhos escolares (93%), audição de música ou filmes (84%), jogos (84%), utilização de software educativo (54%). 87% dos jovens de 10 a 15 anos utilizam telemóvel, 1,4 vezes o valor de 2005. As principais actividades de jovens de 10 a 15 anos que utilizam telemóvel são: chamadas telefónicas (97%), comunicação de mensagens escritas (94%), jogos sem ligação à Internet (54%), envio de fotografias ou ficheiros (36%), navegação na Internet (9%).

**Administração Pública Central**

Como principais resultados, destacam-se:

- Todos os Organismos da Administração Pública Central dispõem de ligações à Internet, 84% com larguras de banda superiores ou iguais a 2 Mbit/s (mais do dobro de 2005 (era 37%)). 29% dos organismos têm ligações com larguras de banda iguais ou superiores a 16 Mbit/s.
- 91% dos organismos da Administração Pública Central têm políticas internas de acesso generalizado à Internet.
- Houve aumentos particularmente elevados desde 2005 nas percentagens de Organismos da Administração Pública Central que realizam as seguintes actividades na Internet: o Consulta de Catálogos de Aprovisionamento (agora 87% dos organismos, muito mais do quíntuplo de 2005); o Comunicação Externa com Empresas (agora 84% dos organismos, mais do triplo de 2005); o Comunicação Externa com Cidadãos (agora 82% dos organismos, mais do triplo de 2005); o Comunicação Externa com Outros Organismos (agora 95% dos organismos, 65% a mais do dobro de 2005).
- 61% dos Organismos da Administração Pública Central utilizaram comércio electrónico para efectuar encomendas (muito mais do dobro de 2005 (era 24%)).
- 33% dos Organismos da Administração Pública Central dispõem de e utilizam equipamento de videoconferência (muito mais do dobro de 2005 (era 12%)).
- Relativamente a segurança informática, 68% dos Organismos da Administração Pública Central têm servidores seguros (1,7 vezes o valor de 2005 (era 40%)), 93% utilizam filtros anti-spam (1,5 vezes o valor de 2005 (era 61%)), e 52% asseguram cópias de segurança dos sistemas de informação em locais exteriores (1,5 vezes o valor de 2005 (era 34%)). Os organismos com software anti-vírus e firewall são, respectivamente, 98% e 96%.

**Organismos da Administração Pública Central por tipo de actividades informatizadas**

(%) Organismos da Administração Pública Central

| | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Troca interna de ficheiros e outra informação | 82 | x | x | 81 | 84 | 94 | 91 | 89 | 90 | 93 | 94 |
| Gestão financeira e administrativa | 71 | x | x | 87 | 88 | 86 | 87 | 90 | 88 | 87 | 93 |
| Gestão de recursos humanos | 62 | x | x | 67 | 72 | 76 | 79 | 82 | 81 | 82 | 89 |
| Organização da informação em bases de dados | 67 | x | x | 65 | 68 | 82 | 81 | 85 | 88 | 89 | 89 |
| Gestão da correspondência | 60 | x | x | 60 | 65 | 75 | 79 | 84 | 84 | 82 | 88 |
| Registo de informação | 67 | x | x | 59 | 71 | 82 | 84 | 87 | 85 | 88 | 87 |
| Processamento e tratamento de informação | 67 | x | x | 64 | 68 | 81 | 79 | 83 | 85 | 85 | 84 |
| Comunicação interna | 55 | x | x | 61 | 63 | 75 | 75 | 80 | 79 | 83 | 84 |
| Difusão da informação | 57 | x | x | 59 | 63 | 76 | 73 | 76 | 79 | 80 | 84 |
| Recolha / Recepção de informação | 64 | x | x | 56 | 66 | 77 | 80 | 84 | 79 | 82 | 83 |
| Gestão documental / Centros de documentação | 45 | x | x | 50 | 48 | 63 | 62 | 63 | 69 | 70 | 69 |
| Gestão de *stocks* | 45 | x | x | 44 | 50 | 55 | 58 | 60 | 62 | 63 | 66 |
| Planeamento e calendarização de actividades | 24 | x | x | 27 | 28 | 39 | 40 | 41 | 42 | 49 | 50 |
| Concepção de projectos | 15 | x | x | 19 | 20 | 29 | 31 | 30 | 30 | 32 | 37 |

Fonte(s): OCT, Instituto de Informática do Ministério das Finanças, Inquérito à Utilização das TIC na Administração Pública Central 2000; OCT, Inquérito à Utilização das TIC na Administração Pública Central 2002; UMIC, Instituto de Informática do Ministério das Finanças, Inquérito à Utilização das TIC na Administração Pública Central 2003-2004; UMIC, Inquérito à Utilização das TIC na Administração Pública Central (a partir de 2005, inclusivé).

**Organismos da Administração Pública Central por aplicações de segurança utilizadas**

(%) Organismos da Administração Pública Central

| | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|---|---|
| Software anti-vírus | 98 | 97 | 98 | 98 | 98 | 99 | 98 | 98 |
| *Firewall* | 85 | 85 | 90 | 94 | 96 | 94 | 94 | 96 |
| Filtros *anti-spam* | x | x | 61 | 69 | 80 | 88 | 93 | 93 |
| Servidores seguros (ex: recorrendo a protocolos shttp) | x | x | 40 | 49 | 60 | 59 | 66 | 68 |
| *Backup* de informação numa localização externa ao Organismo | x | x | 34 | 40 | 42 | 45 | 51 | 52 |

Fonte(s): UMIC, Instituto de Informática do Ministério das Finanças, Inquérito à Utilização das TIC na Administração Pública Central 2003-2004; UMIC, Inquérito à Utilização das TIC na Administração Pública Central (a partir de 2005, inclusivé).

**Organismos da Administração Pública Central que detectaram problemas de segurança**

(%) Organismos da Administração Pública Central

| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|
| **Organismos da Administração Pública Central que detectaram problemas de segurança** | **15** | **8** | **9** | **11** | **18** | **15** |
| Ataque de vírus informático resultando na perda de informação ou de horas de trabalho | 14 | 7 | 6 | 10 | 13 | 12 |
| Chantagem ou ameaças aos dados ou ao software do Organismo | o | 1 | 0 | 1 | 1 | 2 |
| Acesso não autorizado à rede de computadores ou a dados do Organismo | 2 | 2 | 3 | 1 | 1 | 1 |

Fonte(s): UMIC, Inquérito à Utilização das TIC na Administração Pública Central.

**Organismos da Administração Pública Central por actividades realizadas na Internet**

(%) Organismos da Administração Pública Central

| | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|---|---|
| Procura e recolha de informação / documentação | 83 | 80 | 82 | 84 | 75 | 99 | 98 | 98 |
| Comunicação externa com outros Organismos da AP | 40 | 45 | 36 | 46 | 67 | 89 | 88 | 95 |
| Acesso a bases de dados | 54 | 50 | 49 | 55 | 63 | 87 | 87 | 91 |
| Consulta de catálogos de aprovisionamento | 17 | 16 | 16 | 19 | 60 | 80 | 84 | 87 |
| Comunicação interna entre os departamentos do Ministério | 43 | 53 | 47 | 49 | 60 | 79 | 83 | 85 |
| Comunicação externa com empresas | 25 | 27 | 27 | 38 | 65 | 79 | 85 | 84 |
| Comunicação externa com cidadãos | 25 | 24 | 27 | 29 | 60 | 77 | 77 | 82 |
| Interacção com outros Organismos da AP com vista ao aumento da eficiência no atendimento aos utentes *(Guichet* Único) | 4 | 3 | 3 | 6 | 16 | 24 | . | . |

Fonte(s): UMIC, Instituto de Informática do Ministério das Finanças, Inquérito à Utilização das TIC na Administração Pública Central 2003-2004; UMIC, Inquérito à Utilização das TIC na Administração Pública Central (a partir de 2005, inclusivé).

**Organismos da Administração Pública Central por serviços / funcionalidades disponibilizadas no sítio da internet**

(%) Organismos da Administração Pública Central

| | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Informação (institucional) acerca do Organismo | 96 | x | x | 85 | 83 | 85 | 87 | 88 | 90 | 94 | 95 |
| Endereço electrónico para recepção de mensagens ou pedidos de informação | 93 | x | x | 84 | 84 | 85 | 86 | 86 | 90 | 93 | 94 |
| Informação acerca dos serviços prestados | 87 | x | x | 79 | 78 | 83 | 83 | 86 | 87 | 89 | 93 |
| Legislação | x | x | x | x | 68 | 77 | 79 | 85 | 84 | 90 | 92 |
| Disponibilização de formulários para *download* | 37 | x | x | 46 | 50 | 56 | 55 | 64 | 68 | 74 | 78 |
| Disponibilização de formulários para preenchimento e submissão online | 22 | x | x | 22 | 25 | 31 | 37 | 44 | 46 | 53 | 60 |
| Apoio ao utilizador (*helpdesk*, FAQ's) | x | x | x | 48 | 24 | 24 | 49 | 48 | 49 | 57 | 59 |
| Disponibilização de acesso a bases de dados | 36 | x | x | 37 | 41 | 46 | 51 | 55 | 55 | 54 | 56 |
| Distribuição gratuita de bens ou serviços em formato digital *online* | 31 | x | x | 36 | 39 | 40 | 43 | 45 | 48 | 53 | 54 |
| Oportunidades de recrutamento (bolsa de emprego) | 12 | x | x | 14 | 17 | 16 | 21 | 26 | 28 | 37 | 53 |
| Aferição do grau de satisfação dos utilizadores | x | x | x | 9 | 12 | 11 | 11 | 21 | 22 | 29 | 30 |
| Venda de bens ou serviços em formato digital online | 6 | x | x | x | 7 | 9 | 11 | 9 | 11 | 16 | 12 |
| Recebimentos online | 7 | x | x | x | 7 | 7 | 6 | 8 | 9 | 9 | 11 |

Fonte(s): OCT, Instituto de Informática do Ministério das Finanças, Inquérito à Utilização das TIC na Administração Pública Central 2000; OCT, Inquérito à Utilização das TIC na Administração Pública Central 2002; UMIC, Instituto de Informática do Ministério das Finanças, Inquérito à Utilização das TIC na Administração Pública Central 2003-2004; UMIC, Inquérito à Utilização das TIC na Administração Pública Central (a partir de 2005, inclusivé).

**Organismos da Administração Pública Central que efectuam pagamentos online de bens e/ou serviços encomendados via comércio electrónico**

(%) Organismos da Administração Pública Central que utilizam comércio electrónico para efectuar encomendas

| | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|---|
| Organismos da Administração Pública Central que efectuam pagamentos online de bens e/ou serviços encomendados via comércio electrónico | 28 | 11 | 16 | 20 | 27 | 32 | 30 |

Nota(s):

⊥ A partir de 2009 (inclusivé), para além das encomendas através da Internet, consideram-se ainda as encomendas efectuadas através de outras redes electrónicas.

Fonte(s): UMIC, Instituto de Informática do Ministério das Finanças, Inquérito à Utilização das TIC na Administração Pública Central 2004; UMIC, Inquérito à Utilização das TIC na Administração Pública Central (a partir de 2005, inclusivé).

## Tecido empresarial

- 97% das PMEs usam computador, valor que é 100% tanto para as médias como para as grandes empresas.
- 94% das PMEs têm acesso à Internet, e 83% em banda larga (1,3 vezes o valor de 2005). Estes números sobem, respectivamente, para 100% e 90% para médias empresas, e para 100% e 98% para grandes empresas. O crescimento desde 2005 foi particularmente elevado para pequenas empresas (respectivamente, 1,2 vezes e 1,4 vezes o valor de 2005).
- O crescimento das empresas com ligações em banda larga foi particularmente elevado nos sectores de Construção e de Indústrias Transformadoras, em que atingiram valores de, respectivamente, quase o dobro e 1,5 vezes o valor de 2005, sendo agora 78% e 83%, respectivamente.
- 63% das empresas têm redes electrónicas internas (1,7 vezes o valor de 2005), e 35% têm redes sem fios (mais do triplo de 2005).
- 52% das empresas têm presença na Internet; 1,4 vezes o valor de 2005. A presença na Internet é assegurada por 94% das grandes empresas e por 75% das pequenas e médias empresas.
- O crescimento das empresas com presença na Internet foi particularmente elevado nos sectores de Construção, muito mais do dobro de 2005, e de Comércio por Grosso e a Retalho, em que atingiu 1,6 vezes o valor de 2005.
- 31% das empresas usam a Internet para actividades de educação e/ou formação; o dobro de 2005.

- 75% das empresas utilizam a Internet para interagirem com o Estado, 1,3 vezes o valor de 2005, e coloca Portugal na média da UE27.
- 68% das empresas preenchem e enviam formulários online para o Estado. Portugal está no 8º lugar da UE27 neste indicador, acima da média da UE27 (60%).
- 52% das empresas tratam pelo menos um processo administrativo com o Estado online. Portugal está no 10º lugar da UE27 neste indicador, acima da média da UE27 (48%).
- 20% das empresas apresentam propostas online em concursos de compras públicas ("e-Tendering").
  Portugal está no 3º lugar da UE27 neste indicador, muito acima da média da UE27 (13%).
- 35% das empresas utilizam a Internet ou outras redes electrónicas para efectuarem e/ou receberem encomendas, valor que sobe para 45% e 59%, respectivamente para as médias e grandes empresas.
- Portugal está no 9º lugar da UE27 nas empresas que receberam encomendas online (19%), mais do dobro de 2005 e acima da média da UE27 (14%). Para pequenas empresas (18%) a percentagem em Portugal é 1,5 vezes a da média da UE27 (12%).

- Portugal está particularmente desenvolvido em aspectos de negócio electrónico (e-Business), nomeadamente pela adopção de sistemas de partilha ou troca automática de dados electrónicos: o 1º lugar (40%) na UE27 nas empresas cujos processos de negócio estão automaticamente ligados aos de fornecedores ou clientes, mais do dobro da média da UE27 (18%); o 3º lugar (44%) na UE27 nas empresas que partilham informação electrónica sobre compras com software utilizado para uma função interna, muito acima da média da UE27 (31%); o 5º lugar (55%) na UE27 nas empresas que partilham informação electrónica sobre vendas ou compras com software utilizado para uma função interna, muito acima da média da UE27 (41%); o 9º lugar (35%) na UE27 nas empresas que usam troca automática de dados com clientes ou fornecedores, acima da média da UE27 (34%). É de notar que com o alargamento em 2009 do universo das actividades económicas das empresas consideradas, nomeadamente a inclusão, entre outras, das empresas de restauração, as quais têm níveis de informatização relativamente baixos, os indicadores gerais para 2009 e 2010 não são estritamente comparáveis com os de anos anteriores dado que seriam mais elevados se não tivesse havido esse alargamento.

**Empresas do Sector Financeiro (com 10 ou mais pessoas ao serviço)**

Como principais resultados de 2010, destacam-se:

- 100% das empresas do sector financeiro utilizam computadores e Internet, e 93% têm ligações à Internet em banda larga (era 89% em 2005).
- 96% das empresas do sector financeiro têm presença na Internet, quase o dobro de 2005 (era 50%).
- 98% das empresas utilizam a Internet para interagirem com o Estado (eram 86% em 2005).

**Microempresas (empresas com menos de 10 pessoas ao serviço)**

Os indicadores seguintes para microempresas tiveram aumentos particularmente elevados de 2005 para 2010:

- 17% têm presença na Internet, quase o dobro de 2005.
- 15% utilizam a Internet ou outras redes electrónicas para efectuarem e/ou receberem encomendas de bens e/ou serviços, quase o dobro de 2005.
- 37% utilizam a Internet para interagirem com o Estado, 1,8 vezes o que valor de 2005.
- 40% têm ligações em banda larga, 1,6 vezes o valor de 2005.
- 53% têm ligações à Internet, 1,4 vezes o valor de 2005.

### 2.1.2 Dados gerais das populações portuguesa e europeia

**Agregados domésticos com equipamentos TIC**

(%) Agregados domésticos com pelo menos um indivíduo entre os 16 e os 74 anos

| | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|---|---|---|
| Televisão | 87 | 99 | 99 | 99 | 100 | 99 | 99 | . | . |
| Telemóvel | 69 | 80 | 79 | 83 | 86 | 87 | 87 | . | . |
| Telefone (operador fixo) | x | x | 75 | 74 | 71 | 71 | 70 | . | . |
| Computador* | 27 | 38 | 41 | 42 | 45 | 48 | 50 | 56 | 60 |
| Computador portátil | 3 | x | x | 12 | 15 | 20 | 25 | 40 | 45 |
| *Desktop* | 26 | x | x | 39 | 40 | 41 | 39 | 38 | 36 |
| *Palmtop* | o | 2 | 2 | 1 | 2 | 3 | 2 | 4 | 2 |
| Consola de jogos | x | x | 14 | 19 | 18 | 20 | 18 | . | . |

Nota(s):

* Dados relativos a computador incluem *desktop*, computador portátil e *palmtop.* Até 2007, incluiam apenas *desktop* e computador portátil.
Fonte: INE/UMIC, Inquérito à Utilização de Tecnologias de Informação e Comunicação pelas Famílias.

**Agregados domésticos com computador na União Europeia**

(%) Agregados domésticos com pelo menos um indivíduo entre os 16 e os 74 anos

| | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|---|---|---|
| **UE27** | **x** | **x** | **52** | **58** | **61** | **64** | **68** | **71** | **74** |
| Países Baixos | 69 | 71 | x | 78 | 80 | 86 | 88 | 91 | 92 |
| Suécia | x | x | x | 80 | 82 | 83 | 87 | 88 | 90 |
| Luxemburgo | 53 | 58 | 67 | 75 | 77 | 80 | 83 | 88 | 90 |
| Dinamarca | 72 | 79 | 79 | 84 | 85 | 83 | 85 | 86 | 88 |
| Alemanha | 61 | 65 | 69 | 70 | 77 | 79 | 82 | 84 | 86 |
| Reino Unido | 58 | 63 | 65 | 70 | 71 | 75 | 78 | 81 | 83 |
| Finlândia | 55 | 57 | 57 | 64 | 71 | 74 | 76 | 80 | 82 |
| Bélgica | x | x | x | x | 58 | 67 | 70 | 71 | 77 |
| Áustria | 49 | 51 | 59 | 63 | 67 | 71 | 76 | 74 | 76 |
| Irlanda | x | 42 | 46 | 55 | 59 | 65 | 70 | 73 | 76 |
| França | 37 | 46 | 50 | x | 56 | 62 | 68 | 69 | 76 |
| Malta | x | x | x | x | 61 | 63 | 63 | 67 | 73 |
| Eslováquia | x | x | 39 | 47 | 50 | 55 | 63 | 64 | 72 |
| Eslovénia | x | x | 58 | 61 | 65 | 66 | 65 | 71 | 70 |
| Espanha | x | 47 | 52 | 55 | 57 | 60 | 64 | 66 | 69 |
| Polónia | x | x | 36 | 40 | 45 | 54 | 59 | 66 | 69 |
| Estónia | x | x | 36 | 43 | 52 | 57 | 60 | 65 | 69 |
| Hungria | x | x | 32 | 42 | 50 | 54 | 59 | 63 | 66 |
| Itália | 40 | 48 | 47 | 46 | 52 | 53 | 56 | 61 | 65 |
| República Checa | x | 24 | 30 | 30 | 39 | 43 | 52 | 60 | 64 |
| Letónia | x | x | 26 | 32 | 41 | 49 | 57 | 60 | 63 |
| Chipre | x | x | 47 | 46 | 52 | 53 | 56 | 61 | 61 |
| **Portugal** | **27** | **38** | **41** | **42** | **45** | **48** | **50** | **56** | **60** |
| Lituânia | 12 | 20 | 27 | 32 | 40 | 46 | 52 | 57 | 59 |
| Grécia | 25 | 29 | 29 | 33 | 37 | 40 | 44 | 47 | 53 |
| Roménia | x | x | 12 | x | 26 | 34 | 38 | 46 | 48 |
| Bulgária | x | x | 15 | x | 21 | 23 | 29 | 32 | 35 |

Nota(s):

* Dados relativos a computador incluem *desktop*, computador portátil e *palmtop.* Até 2007, incluiam apenas *desktop* e computador portátil.
Fonte: *EUROSTAT - Survey on ICT Usage in Households and by Individuals* (actualizado em 09/12/2010).

**Agregados domésticos com ligação à Internet na União Europeia**

(%) Agregados domésticos com pelo menos um indivíduo entre os 16 e os 74 anos

| | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|---|---|---|
| **UE27** | **x** | **x** | **41** | **48** | **49** | **54** | **60** | **65** | **70** |
| Países Baixos | 58 | 61 | 65 | 78 | 80 | 83 | 86 | 90 | 91 |
| Luxemburgo | 40 | 45 | 59 | 65 | 70 | 75 | 80 | 87 | 90 |
| Suécia | x | x | x | 73 | 77 | 79 | 84 | 86 | 88 |
| Dinamarca | 56 | 64 | 69 | 75 | 79 | 78 | 82 | 83 | 86 |
| Alemanha | 46 | 54 | 60 | 62 | 67 | 71 | 75 | 79 | 82 |
| Finlândia | 44 | 47 | 51 | 54 | 65 | 69 | 72 | 78 | 81 |
| Reino Unido | 50 | 55 | 56 | 60 | 63 | 67 | 71 | 77 | 80 |
| França | 23 | 31 | 34 | x | 41 | 49 | 62 | 63 | 74 |
| Áustria | 33 | 37 | 45 | 47 | 52 | 60 | 69 | 70 | 73 |
| Bélgica | x | x | x | 50 | 54 | 60 | 64 | 67 | 73 |
| Irlanda | x | 36 | 40 | 47 | 50 | 57 | 63 | 67 | 72 |
| Malta | x | x | x | 41 | 53 | 54 | 59 | 64 | 70 |
| Eslovénia | x | x | 47 | 48 | 54 | 58 | 59 | 64 | 68 |
| Estónia | x | x | 31 | 39 | 46 | 53 | 58 | 63 | 68 |
| Eslováquia | x | x | 23 | 23 | 27 | 46 | 58 | 62 | 67 |
| Polónia | 11 | 14 | 26 | 30 | 36 | 41 | 48 | 59 | 63 |
| Lituânia | 4 | 6 | 12 | 16 | 35 | 44 | 51 | 60 | 61 |
| República Checa | x | 15 | 19 | 19 | 29 | 35 | 46 | 54 | 61 |
| Letónia | 3 | x | 15 | 31 | 42 | 51 | 53 | 58 | 60 |
| Hungria | x | x | 14 | 22 | 32 | 38 | 48 | 55 | 60 |
| Espanha | x | 28 | 34 | 36 | 39 | 45 | 51 | 54 | 59 |
| Itália | 34 | 32 | 34 | 39 | 40 | 43 | 47 | 53 | 59 |
| Chipre | 24 | 29 | 53 | 32 | 37 | 39 | 43 | 53 | 54 |
| **Portugal** | **15** | **22** | **26** | **31** | **35** | **40** | **46** | **48** | **54** |
| Grécia | 12 | 16 | 17 | 22 | 23 | 25 | 31 | 38 | 46 |
| Roménia | x | x | 6 | x | 14 | 22 | 30 | 38 | 42 |
| Bulgária | x | x | 10 | x | 17 | 19 | 25 | 30 | 33 |

Fonte: *EUROSTAT - Survey on ICT Usage in Households and by Individuals* (actualizado em 09/12/2010).

**Agregados domésticos sem ligação à Internet por razões para tal**

(%) Agregados domésticos com pelo menos um indivíduo entre os 16 e os 74 anos, sem ligação à Internet

| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|
| Não sabe utilizar | 52 | 54 | 57 | 62 | . | 53 |
| Não precisa (não é útil, interessante, etc) | 58 | 56 | 54 | 72 | . | 46 |
| Custo do equipamento elevado | 53 | 54 | 49 | 51 | . | 26 |
| Custo do acesso elevado | 49 | 51 | 46 | 47 | . | 16 |
| Barreiras linguísticas | 33 | 33 | 36 | 34 | . | 8 |
| Não quer (conteúdo perigoso / prejudicial) | 23 | 16 | 18 | 45 | . | 7 |
| Tem acesso noutro local | 20 | 20 | 20 | 8 | . | 4 |
| Preocupações com privacidade / segurança | 12 | 9 | 10 | 9 | . | 2 |
| Incapacidade física | 2 | 2 | 2 | 3 | . | 2 |

Fonte: INE/UMIC, Inquérito à Utilização de Tecnologias de Informação e Comunicação pelas Famílias.

**Utilizadores de computador, por condição perante o trabalho**

(%) Indivíduos entre os 16 e os 74 anos, na condição perante o trabalho correspondente

| | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|---|---|---|
| Estudantes | 88 | 97 | 96 | 98 | 99 | 99 | 98 | 99 | 100 |
| Empregados | 31 | 42 | 44 | 47 | 51 | 55 | 56 | 63 | 66 |
| Desempregados | 24 | 24 | 23 | 29 | 34 | 38 | 37 | 50 | 53 |
| Reformados e outros inactivos | 5 | 5 | 5 | 7 | 9 | 11 | 12 | 15 | 20 |

Nota(s):

1) Um mesmo indivíduo pode ser contabilizado em mais do que uma das condições perante o trabalho indicadas.
Fonte: INE/UMIC, Inquérito à Utilização de Tecnologias de Informação e Comunicação pelas Famílias.

**Utilizadores de Internet (no primeiro trimestre de cada ano) na União Europeia**

(%) Indivíduos entre os 16 e os 74 anos

| | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|---|---|---|
| **UE27** | **x** | **x** | **45** | **51** | **52** | **57** | **62** | **65** | **69** |
| Suécia | 71 | 77 | 82 | 81 | 86 | 80 | 88 | 90 | 91 |
| Países Baixos | 61 | 64 | 69 | 79 | 81 | 84 | 87 | 89 | 90 |
| Luxemburgo | 40 | 53 | 65 | 69 | 71 | 78 | 81 | 86 | 90 |
| Dinamarca | 64 | 71 | 76 | 77 | 83 | 81 | 84 | 86 | 88 |
| Finlândia | 62 | 66 | 70 | 73 | 77 | 79 | 83 | 82 | 86 |
| Reino Unido | 56 | 61 | 63 | 66 | 66 | 72 | 76 | 82 | 83 |
| Alemanha | 49 | 54 | 61 | 65 | 69 | 72 | 75 | 77 | 80 |
| França | x | x | x | x | 47 | 64 | 68 | 69 | 79 |
| Bélgica | x | x | x | 58 | 62 | 67 | 69 | 75 | 78 |
| Eslováquia | x | x | 46 | 50 | 50 | 56 | 66 | 70 | 76 |
| Áustria | 37 | 41 | 52 | 55 | 61 | 67 | 71 | 72 | 74 |
| Estónia | x | x | 50 | 59 | 61 | 64 | 66 | 71 | 74 |
| Eslovénia | x | x | 37 | 47 | 51 | 53 | 56 | 62 | 68 |
| Irlanda | x | 31 | 34 | 37 | 51 | 58 | 63 | 65 | 67 |
| Letónia | x | x | 33 | 42 | 50 | 55 | 61 | 64 | 66 |
| República Checa | x | 28 | 32 | 32 | 44 | 49 | 58 | 60 | 66 |
| Espanha | 20 | 37 | 40 | 44 | 48 | 52 | 57 | 60 | 64 |
| Hungria | x | x | 28 | 37 | 45 | 52 | 59 | 59 | 62 |
| Malta | x | x | x | 38 | 38 | 45 | 49 | 58 | 62 |
| Lituânia | 18 | 24 | 29 | 34 | 42 | 49 | 53 | 58 | 60 |
| Polónia | x | x | 29 | 35 | 40 | 44 | 49 | 56 | 59 |
| Chipre | x | x | 32 | 31 | 34 | 38 | 39 | 48 | 52 |
| **Portugal** | **19** | **26** | **29** | **32** | **36** | **40** | **42** | **46** | **51** |
| Itália | 28 | 29 | 31 | 34 | 36 | 38 | 42 | 46 | 51 |
| Grécia | 15 | 16 | 20 | 22 | 29 | 33 | 38 | 42 | 44 |
| Bulgária | x | x | 16 | x | 24 | 31 | 35 | 42 | 43 |
| Roménia | x | x | 12 | x | 21 | 24 | 29 | 33 | 36 |

Fonte: *EUROSTAT - Survey on ICT Usage in Households and by Individuals* (actualizado em 09/12/2010).

**Utilizadores de Internet por actividades realizadas**

(%) Indivíduos entre os 16 e os 74 anos que utilizaram Internet no primeiro trimestre de cada ano

| | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|---|---|
| **Comunicação** | | | | | | | | |
| Enviar / receber *e-mails* | 78 | 81 | 81 | 81 | 84 | 85 | 86 | 88 |
| Colocar mensagens em *chats, blogs*, *newsgroups* ou fóruns de discussão *online* ou comunicar através de mensagens escritas em tempo real (ex: *messenger*) * | . | . | . | . | . | 65 | 45 | 69 |
| Colocar conteúdo pessoal num sítio na Internet | . | . | . | . | . | 17 | 27 | 40 |
| Telefonar ou fazer chamadas de vídeo (via *webcam)*** | 10 | 11 | 10 | 16 | 22 | x | 25 | 26 |
| Desenvolver *blogs* | . | . | 7 | 10 | 14 | 11 | 14 | 14 |
| **Pesquisa de informação e utilização de serviços online** | | | | | | | | |
| Pesquisar informação de bens e serviços | 82 | 79 | 81 | 84 | 83 | 81 | 87 | 86 |
| Pesquisar informação sobre saúde | 25 | 19 | 31 | 39 | 45 | 51 | 61 | 59 |
| Ler / *download* jornais / revistas *online* | 49 | 50 | 51 | 45 | 38 | 48 | 59 | 56 |
| Jogar / *download* jogos, imagens, música | 43 | 45 | 44 | 46 | 53 | . | 44 | 44 |
| Ouvir rádio / ver TV | 23 | 27 | 28 | 30 | 36 | 41 | 42 | 50 |
| *Download* de software | 27 | 28 | 28 | 26 | 23 | 34 | 39 | 46 |
| Pesquisar informação traduzida em compras *offline* | . | . | 25 | 29 | 31 | 36 | . | 42 |
| Utilizar serviços relativos a viagens e alojamentos | 27 | 31 | 33 | 35 | 34 | 29 | 32 | 27 |
| Procurar emprego / enviar candidaturas | . | 11 | 12 | 14 | 16 | 19 | 22 | 20 |
| Jogar em rede com outras pessoas | . | . | . | . | . | 17 | 15 | 15 |
| Utilizar programas para gerir arquivos de informação (*news feeds*) / para ler novos conteúdos publicados em sítios na Internet (ex:RSS) | . | . | . | . | . | 8 | 9 | . |
| **Serviços bancários e venda de bens e serviços** | | | | | | | | |
| *Home banking* | 24 | 26 | 26 | 27 | 29 | 32 | 37 | 38 |
| Vender bens e serviços | 2 | 2 | 2 | 2 | . | . | 3 | 4 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Ligação a organismos / serviços públicos** | | | | | | | | |
| Obter informação de sítios da Internet de organismos da Administração Pública | 38 | 35 | 37 | 39 | 42 | 36 | 39 | 40 |
| Preencher / enviar *online* impressos / formulários oficiais | 20 | 26 | 28 | 32 | 33 | 31 | 35 | 33 |
| *Download* de impressos / formulários oficiais | 21 | 26 | 26 | 30 | 32 | 28 | 30 | 28 |
| Utilizar portais da Administração Pública com serviços administrativos integrados | . | 19 | 30 | 35 | 37 | 23 | 26 | 23 |
| Enviar sugestões, reclamações ou pedidos a organismos públicos | . | 6 | 8 | 9 | 11 | 10 | 11 | 8 |
| Participar em fóruns de discussão de assuntos de interesse público | . | 5 | 5 | 4 | 5 | 4 | 4 | . |
| Participar em consultas públicas *online* | . | 4 | 5 | 5 | 3 | 5 | . | . |
| **Educação / formação** | | | | | | | | |
| Consultar a Internet com o propósito de aprender | . | . | . | . | 67 | 78 | 83 | 77 |
| Procurar Informação sobre educação ou formação ou oferta de cursos | . | . | . | . | 37 | 55 | 59 | 57 |
| Frequentar cursos *online* de educação/formação (qualquer temática) | . | . | . | . | 3 | 5 | 5 | 4 |

Nota(s):

* Em 2008 e 2010, a informação sobre a "Colocação de mensagens em *chats, blogs, newsgroups* ou fóruns de discussão *online*" e sobre a "Comunicação através de mensagens escritas em tempo real (ex: *messenger*)" foi recolhida separadamente. Em 2008, os dados não consideram a colocação de mensagens em *chats*. Em 2010, os dados passam a incluir a colocação de mensagens em *websites* de redes sociais.

** Em 2008 verificou-se uma quebra de série no indicador "Telefonar ou fazer chamadas de vídeo (via *webcam*)", dado que anteriormente o indicador era "Telefonar via Internet ou videoconferência".

Fonte: INE/UMIC, Inquérito à Utilização de Tecnologias de Informação e Comunicação pelas Famílias.

**Utilizadores de Internet por horas dispendidas na Internet, por semana**

(%) Indivíduos entre os 16 e os 74 anos que utilizaram Internet no primeiro trimestre de cada ano

| | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|---|
| 1 hora ou menos | 32 | 22 | 22 | 26 | 20 | 16 | 18 |
| Mais de 1 até 5 horas | 34 | 40 | 36 | 27 | 33 | 33 | 34 |
| Mais de 5 até 10 horas | 14 | 16 | 17 | 20 | 22 | 21 | 21 |
| Mais de 10 até 20 horas | 8 | 10 | 10 | 15 | 13 | 13 | 13 |
| Mais de 20 horas | 12 | 12 | 14 | 11 | 13 | 17 | 15 |

Fonte: INE/UMIC, Inquérito à Utilização de Tecnologias de Informação e Comunicação pelas Famílias.

**Utilizadores de Internet por precauções de segurança adoptadas**

(%) Indivíduos entre os 16 e os 74 anos que utilizaram Internet no primeiro trimestre de cada ano

| | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|---|
| Instalação / actualização de anti-vírus / *firewall* | 50 | 49 | 46 | 32 | 42 | 47 | . |
| Autenticação *online* | 30 | 28 | 37 | 37 | 40 | 46 | . |

Fonte: INE/UMIC, Inquérito à Utilização de Tecnologias de Informação e Comunicação pelas Famílias.

**Utilizadores por tipos de utilização de comércio electrónico através de *browsers* da Internet, do Multibanco ou de Sistemas de Identificação por Radio Frequência**

(%) Indivíduos entre os 16 e os 74 anos

| | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|---|---|---|
| Carregamentos de telemóveis com saldo pelo Multibanco* | x | x | x | x | x | 51 | 54 | 58 | 55 |
| Utilização de Via Verde | x | x | x | x | x | x | x | 19 | 19 |
| Compra de bilhetes através de Multibanco* | x | x | x | x | x | 9 | 8 | 13 | 8 |
| Encomendas através da Internet | 2 | 2 | 3 | 4 | 5 | 6 | 6 | 10 | 10 |

Nota(s):

* Em 2010 verificou-se uma quebra de série nos indicadores "Carregamentos de telemóveis com saldo pelo Multibanco" e "Compra de bilhetes através de multibanco". Até 2009, inclusivé, os dados dizem respeito à utilização sem referência a um período temporal específico. A partir de 2010 a informação recolhida refere-se à utilização no primeiro trimestre do ano.

Fonte: INE/UMIC, Inquérito à Utilização de Tecnologias de Informação e Comunicação pelas Famílias.

**Utilizadores que efectuaram encomendas pela Internet nos últimos três meses por valor de encomendas efectuadas**

(%) Indivíduos entre os 16 e os 74 anos que realizaram comércio electrónico

| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 * |
|---|---|---|---|---|---|---|
| Até 30 € | 14 | 14 | 17 | 13 | 10 | 7 |
| Mais de 30 € até 100€ | 38 | 39 | 34 | 29 | 32 | 31 |
| Mais de 100 até 300€ | 24 | 26 | 27 | 30 | 31 | 26 |
| Mais de 300 € | 24 | 21 | 22 | 26 | 28 | 34 |

Nota(s):

* Até 2009, inclusivé, os dados dizem respeito a encomendas efectuadas no primeiro trimestre de cada ano. Em 2010 a informação recolhida refere-se a a encomendas efectuadas nos últimos 12 meses (no ano anterior, portanto). Assim, em 2010 as percentagens foram calculadas tendo como denominador o número de indivíduos que realizaram comércio electrónico no ano anterior, enquanto até 2009, inclusivé, as percentagens calculadas eram relativas aos indivíduos que realizaram comércio electrónico no primeiro trimestre de cada ano.

Fonte: INE/UMIC, Inquérito à Utilização de Tecnologias de Informação e Comunicação pelas Famílias.

**Utilizadores de computador**

(%) Indivíduos entre os 10 e os 15 anos

| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|
| Utilizadores de computador | 91 | 91 | 94 | 97 | . | 96 |

Fonte: INE/UMIC, Inquérito à Utilização de Tecnologias de Informação e Comunicação pelas Famílias.

**Utilizadores de computador por frequência de utilização**

(%) Indivíduos entre os 10 e os 15 anos que utilizaram computador no primeiro trimestre de cada ano

| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|
| Todos ou quase todos os dias | 51 | 55 | 59 | 68 | . | 80 |
| Pelo menos uma vez por semana | 42 | 37 | 33 | 27 | . | 19 |
| Menos de uma vez por semana | 7 | 8 | 8 | 4 | . | 2§ |

Fonte: INE/UMIC, Inquérito à Utilização de Tecnologias de Informação e Comunicação pelas Famílias.

**Utilizadores de Internet**

(%) Indivíduos entre os 10 e os 15 anos

| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|
| Utilizadores de Internet | 74 | 75 | 83 | 93 | . | 91 |

Fonte: INE/UMIC, Inquérito à Utilização de Tecnologias de Informação e Comunicação pelas Famílias.

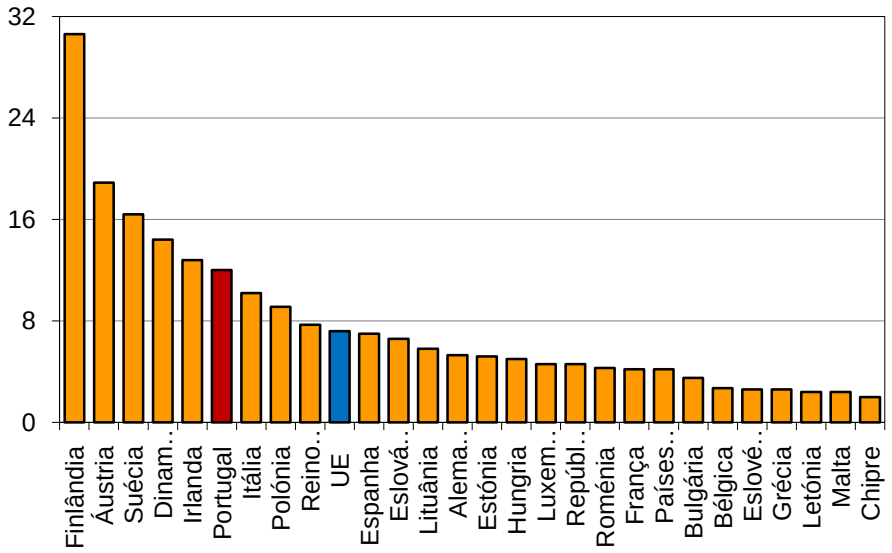
A maioria dos cidadãos da UE mostrou preocupação com questões de protecção de dados. Dois terços dos participantes da pesquisa disseram estar preocupados sobre se as organizações que lidavam com os seus dados pessoais lidariam com estes dados de forma adequada (64%).

- O nível de preocupação com a protecção de dados só mudou um pouco desde o início da Década de 1990. Desde então, o número flutuou, antes de voltar - em 2008 - para o nível início de 1991 (68%).
- Cidadãos da UE consideram que os seus dados pessoais são melhor protegidos por serviços médicos, os médicos e instituições públicas. A partir de uma lista de organizações públicas e privadas, cidadãos da UE colocaram mais confiança em serviços médicos, os médicos e a polícia para proteger os seus dados pessoais.
- Os maiores níveis de desconfiança estavam relacionados com as empresas de encomendas por correio.

**Telecomunicações e Prestadores**

**Penetração na População de Banda Larga Móvel nos Estados Membros da EU - Serviços Dedicados a Dados (placas, modems, chaves)**
1 de Janeiro de 2011, (%)

| | % |
|---|---|
| Finlândia | 30,6 |
| Áustria | 18,9 |
| Suécia | 16,4 |
| Dinamarca | 14,4 |
| Irlanda | 12,8 |
| **Portugal** | **12,0** |
| Itália | 10,2 |
| Polónia | 9,1 |
| Reino Unido | 7,7 |
| **UE** | **7,2** |
| Espanha | 7,0 |
| Eslováquia | 6,6 |
| Lituânia | 5,8 |
| Alemanha | 5,3 |
| Estónia | 5,2 |
| Hungria | 5,0 |
| Luxemburgo | 4,6 |
| República Checa | 4,6 |
| Roménia | 4,3 |
| França | 4,2 |
| Países Baixos | 4,2 |
| Bulgária | 3,5 |
| Bélgica | 2,7 |
| Eslovénia | 2,6 |
| Grécia | 2,6 |
| Letónia | 2,4 |
| Malta | 2,4 |
| Chipre | 2,0 |




**Fonte:** COCOM, DG INFSO, Comissão Europeia, Junho de 2011

**Número de prestadores em actividade**

4.º Trimestre de cada ano, Número de prestadores

| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|
| Número de ISP registados | 39 | 38 | 42 | 54 | 50 | 51 |
| Número de ISP em actividade | 30 | 28 | 34 | 37 | 35 | 35 |

Fonte(s): ICP-ANACOM.

**Número de clientes do serviço de acesso fixo à Internet**

4.º Trimestre de cada ano, Milhares de clientes

| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|
| **Total de clientes** | **1 436** | **1 580** | **1 612** | **1 676** | **1 898** | **2 104** |
| Residenciais | 1 222 | 1 327 | 1 355 | x | x | x |
| Não residenciais | 214 | 253 | 256 | x | x | x |
| **Clientes com acesso ADSL** | **673** | **882** | **892** | **947** | **1 060** | **1 069** |
| Residenciais | 502 | 674 | 679 | 767 | 857 | 861 |
| Não residenciais | 171 | 208 | 213 | 180 | 202 | 208 |
| **Clientes com acesso modem cabo** | **490** | **538** | **606** | **663** | **750** | **852** |
| Residenciais | 467 | 511 | 579 | 640 | 723 | 817 |
| Não residenciais | 23 | 26 | 27 | 23 | 28 | 35 |
| **Clientes com outros acessos** | **3** | **5** | **15** | **26** | **55** | **154** |
| Residenciais | 0 | 2 | 11 | 22 | 51 | 146 |
| Não residenciais | 3 | 3 | 3 | 4 | 4 | 7 |
| **Clientes com acesso *dial-up*** | **271** | **156** | **99** | **41** | **33** | **29** |

Fonte(s): ICP-ANACOM.

**Penetração da banda larga de acesso fixo na população nos Estados Membros da União Europeia**

4.º Trimestre de cada ano, Número de clientes (residenciais e não residenciais) por 100 habitantes

| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|
| **UE27** | **11** | **16** | **23** | **25** | **27** | **26** |
| Países Baixos | 25 | 32 | 34 | 36 | 38 | 39 |
| Dinamarca | 25 | 32 | 36 | 37 | 38 | 39 |
| Luxemburgo | 14 | 21 | 25 | 29 | 32 | 33 |
| França | 15 | 20 | 25 | 28 | 30 | 33 |
| Alemanha | 13 | 18 | 24 | 28 | 30 | 32 |
| Suécia | 20 | 26 | 31 | 31 | 32 | 32 |
| Reino Unido | 16 | 22 | 26 | 28 | 30 | 32 |
| Bélgica | 18 | 23 | 26 | 28 | 29 | 31 |
| Malta | 11 | 12 | 17 | 24 | 27 | 30 |
| Finlândia | 22 | 27 | 31 | 31 | 29 | 29 |
| Estónia | 12 | 17 | 21 | 25 | 26 | 27 |
| Chipre | 4 | 7 | 14 | 18 | 22 | 24 |
| Eslovénia | 9 | 13 | 17 | 21 | 23 | 24 |
| Áustria | 14 | 17 | 20 | 21 | 23 | 24 |
| Espanha | 12 | 15 | 18 | 20 | 22 | 24 |
| Irlanda | 7 | 12 | 17 | 20 | 22 | 23 |
| Itália | 12 | 14 | 17 | 19 | 21 | 22 |
| República Checa | 6 | 11 | 15 | 17 | 19 | 22 |
| Hungria | 6 | 10 | 14 | 16 | 19 | 21 |
| Lituânia | 6 | 9 | 14 | 18 | 19 | 21 |
| **Portugal** | **11** | **14** | **15** | **17** | **19** | **21** |
| Grécia | 1 | 4 | 9 | 13 | 17 | 20 |
| Letónia | 4 | 9 | 15 | 17 | 19 | 19 |
| Eslováquia | 2 | 5 | 9 | 11 | 15 | 17 |
| Polónia | 2 | 5 | 8 | 12 | 14 | 16 |
| Bulgária | x | x | 8 | 11 | 13 | 15 |
| Roménia | x | x | 10 | 12 | 13 | 14 |

Fonte(s): OCDE; COCOM, DG INFSO, Comissão Europeia

**Empresas que Receberam Encomendas Online**

% das empresas

| | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 ⊥ | 2010 |
|---|---|---|---|---|---|---|---|---|
| % das empresas | 3 | 6 | 9 | 7 | 9 | 19 | 15 | 19 |

⊥ Quebra de série de 2008 para 2009, resultante de harmonização na União Europeia, que incluiu o alargamento das actividades económicas consideradas na inquirição, nomeadamente por ter passado a abranger "restauração" e "electricidade, gás e vapor, fornecimento de água, saneamento, gestão de resíduos", entre outras.

**Fonte**: Agência para a Sociedade do Conhecimento, IP

**Empresas que preencheram e enviaram formulários electrónicos à Administração Pública pela Internet**

% das empresas (PMEs e Grande Empresas, s/ sector financeiro)

| | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|---|---|
| % das empresas | 43 | 50 | 52 | 54 | 66 | 68 | 69 | 64 |

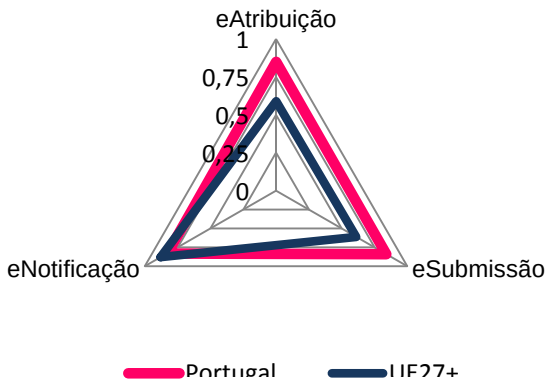
**Fonte**: EUROSTAT

**Processo Pré-atribuição de Compras Públicas Electrónicas**

2010, (%)

| Processo pré-atribuição de compras públicas electrónicas | Portugal | UE27+ |
|---|---|---|
| *eAtribuição* | 85% | 59% |
| eSubmissão | 84% | 61% |
| eNotificação | 83% | 88% |

Fonte: *eGov Benchmarking Report 2010, DGINFSO, EC*



**Número de declarações de Imposto de Rendimento sobre Pessoas Singulares (IRS) submetidas pela Internet**

Milhões de declarações

| | ≤2003* | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|---|---|
| Número de declarações de IRS submetidas pela Internet | 0,534 | 0,952 | 1,733 | 2,277 | 2,933 | 3,394 | 3,810 | 4,181 |

* Valor acumulado.
**Fonte:** Direcção-Geral de Impostos.

**Número de declarações de Imposto de valor Acrescentado (IVA) submetidas pela Internet**

Milhões de declarações

| | ≤2003* | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|---|---|
| Número de declarações de IVA submetidas pela Internet | 1,224 | 2,897 | 3,632 | 3,851 | 3,871 | 3,852 | 3,737 | 3,698 |

* Valor acumulado.
**Fonte:** Direcção-Geral de Impostos.

**Negócio Electrónico em todas as empresas nos Países da União Europeia**

(PMEs e Grandes Empresas, s/ sector financeiro)
2010, 1º trimestre,
(%)

| | Integração de processos internos | Integração com clientes/fornecedores e Gestão da Cadeia de Valor | Recepção de encomendas online no ano anterior (≥1% de todas as encomendas) | Utilização da Internet para interagir com serviços públicos | Utilização da Internet para serviços bancários e financeiros |
|---|---|---|---|---|---|
| Alemanha | 32 | 65 | 22 | 68 | |
| Áustria | 25 | 39 | 14 | 75 | 88 |
| Bélgica | 40 | 57 | 26 | 77 | |
| Bulgária | 11 | 38 | 4 | 64 | 58 |
| Chipre | 17 | 14 | 7 | 74 | 63 |
| Dinamarca | 29 | 50 | 25 | 92 | |
| Eslováquia | 17 | 54 | 7 | 88 | 90 |
| Eslovénia | 21 | 67 | 10 | 88 | 93 |
| Espanha | 22 | 44 | 12 | 67 | 87 |
| Estónia | 7 | 42 | 10 | 80 | 94 |
| **UE27** | **22** | **51** | **14** | **75** | **82** |
| Finlândia | 28 | 49 | 16 | 96 | |
| França | 24 | 59 | 12 | 78 | 78 |

| | | | | | |
|---|---|---|---|---|---|
| Grécia | 36 | 25 | 9 | 77 | 70 |
| Hungria | 8 | 51 | 8 | 71 | 79 |
| Irlanda | 20 | 34 | 21 | 87 | 85 |
| Itália | 22 | 63 | 4 | 84 | 87 |
| Letónia | 8 | 55 | 6 | 72 | |
| Lituânia | 11 | 63 | 22 | 95 | 93 |
| Luxemburgo | 21 | 62 | 14 | 90 | 82 |
| Malta | 18 | 50 | 16 | 77 | 81 |
| Países Baixos | 22 | 72 | 22 | 95 | 91 |
| Polónia | 11 | 49 | 8 | 89 | 85 |
| **Portugal** | **26** | **46** | **19** | **75** | **77** |
| Reino Unido | 6 | 23 | 15 | 67 | |
| República Checa | 21 | 23 | 20 | 89 | 87 |
| Roménia | 19 | 34 | 6 | 50 | 58 |
| Suécia | 35 | 42 | 24 | 90 | |

**Fonte:** EUROSTAT

**Formação e educação**

Todas as escolas públicas do ensino básico e secundário estão ligadas à Internet em banda larga desde 2006.

- O número de computadores ligados à Internet nos estabelecimentos de ensino mais que septuplicou de 2004/2005 para 2008/2009. As escolas tinham em 2008/2009 cerca do dobro de computadores desktop e 18 vezes mais computadores portáteis do que apenas dois anos antes, em 2006/2007.
- Em 2008/2009 o número de alunos por computador ligado à Internet no conjunto das escolas do ensino básico e secundário foi 2,3, tendo decrescido para menos de 1/7 do que era em 2004/2005, quando o número de alunos por computador com ligação à Internet era 16,1. Esta evolução positiva é ainda mais acentuada no ensino público: de 2004/2005 para 2008/2009 o número de alunos por computador com ligação à Internet passou de 18,2 para 2,2, isto é decresceu para menos de 1/8 do que era em 2004/2005. A situação é agora melhor no ensino público do que no privado, quando em 2004/2005 o privado tinha mais do dobro de computadores por aluno.

**Confiança em organizações**

*Nota: Os dados seguintes resultam de uma compilação de dados da Osterman Research*

- Nos últimos cinco anos. Empresas de pesquisa de mercado e de opinião foram os únicos a ter visto uma diminuição contínua nos níveis de confiança 1991-2008.
- Os entrevistados tenderam a ver os níveis de protecção de dados baixos no seu próprio país. Nem sequer metade dos entrevistados (48%) considerou que os seus dados foram adequadamente protegidos.
- A maioria teme que a legislação nacional não conseguirá lidar com o crescente número de dados pessoais na Internet (54%). A grande maioria também sentiu que os seus concidadãos tinham baixos níveis de consciência sobre a protecção de dados (77%).

- Os cidadãos da UE estavam muito bem informados sobre alguns dos dados existentes normas de protecção, ainda havia algumas lacunas de informação considerável:

Os entrevistados foram apresentados com uma lista de direitos dos cidadãos europeus têm com as organizações que mantêm os seus dados, tais como o direito de tomar medidas legais em caso de abuso de informação pessoal ou de ser indemnizado pelos danos resultantes. Cada um dos direitos enumerados era familiar para a maioria dos entrevistados. No entanto, apenas um quarto dos entrevistados sabiam que os cidadãos europeus desfrutaram de todos esses direitos (27%).

- Além disso, apenas 29% dos entrevistados sabiam que os dados sensíveis, como informações sobre origem racial ou étnica, opiniões políticas, etc., recebiam protecção jurídica especial. A pequena minoria (17%) tinha ouvido falar que os dados pessoais só podem ser transferidos para fora da UE para países que garantissem um nível adequado de protecção de dados.
- As autoridades nacionais de protecção de dados eram relativamente desconhecidas para a maioria dos cidadãos da EU. Em média, apenas 28% dos entrevistados disseram que tinham ouvido falar da existência de tais instituições no seu país. Grécia e Hungria tinham os níveis mais altos de reconhecimento (51% e 46%, respectivamente). A consciência de tais instituições em toda a UE tem-se mantido inalterada ao longo dos últimos cinco anos.
- A maioria dos utilizadores de Internet europeus sente-se desconfortável ao transmitir seus dados pessoais na Internet: 82% dos utilizadores de Internet argumentou que a transmissão de dados através da Web não era suficientemente segura. No entanto, apenas uma minoria de utilizadores da Internet disseram que usaram ferramentas e tecnologias que aumentaram a segurança dos dados na rede, ou seja, firewalls ou filtragem de e-mail (22%).
- Aos olhos da maioria dos cidadãos da UE, a luta contra o terrorismo internacional é uma razão aceitável para restringir direitos de protecção de dados. A maioria dos entrevistados concordou que deveria ser possível monitorizar dados de passageiros de voo (82%), as chamadas telefónicas (72%) e Internet e o uso de cartão de crédito (75% e 69%, respectivamente) quando este serviu para combater o terrorismo.
- No entanto, a maioria dos entrevistados revia-se a favor de leis mais relaxadas na protecção de dados, se isso estiver dentro de limites claramente definidos: cerca de um terço dos entrevistados salientou que apenas suspeitos devem ser monitorizados (27% -35%) e aproximadamente uma em cada cinco pessoas (14% -21%) queria excepções ainda mais rigorosas.
- Desde 2003, o número de cidadãos que aprova a monitorização do uso da Internet e das chamadas telefónicas das pessoas aumentou em cerca de 12 pontos percentuais.

# *3* Research Design: Os Enquadramentos Legal e Governamental

Quase todos os aspectos da Governação da Internet têm um componente legal, mas a formulação de uma resposta legal ao rápido desenvolvimento da Internet ainda está muito pouco desenvolvida. As duas abordagens prevalecentes dos aspectos legais da Internet são:

- A abordagem "direito real" (em oposição a "direito virtual" ou "ciberdireito"), segunda a qual o tratamento a ser recebido pela Internet não é essencialmente diferente daquele recebido pelas tecnologias de telecomunicações anteriores.
  Embora mais rápida e mais abrangente, a Internet continua a envolver comunicação à distância entre indivíduos, e portanto as regras legais existentes podem ser aplicadas.
- A abordagem "ciberdireito", que se baseia na presunção de que a Internet introduz novos tipos de relacionamentos sociais no ciberespaço.

Consequentemente, coloca-se a necessidade de formular novas "ciberleis" para o ciberespaço. Um dos argumentos desta abordagem é que o volume e velocidade tremendos das comunicações facilitadas pela Interne, sendo global e, até certo ponto, anónima, dificulta a aplicação das regras legais existentes.

Embora ambas as abordagens tenham elementos válidos, a abordagem do direito real vem ganhando predominância tanto na análise teórica como em termos de políticas e directrizes [Parlamento Europeu (2011)]. O pensamento geral é que uma parte considerável da legislação existente pode ser aplicada à Internet. Em certos casos, contudo, como a protecção de marcas registadas, por exemplo, as regras do direito real teriam de ser adaptadas para poderem ser aplicadas ao mundo virtual. Outros casos, como o spam, devem ser regulamentados por regras novas, concebidas especificamente. A analogia "mundo real" mais próxima do spam é a correspondência publicitária, que não é ilegal.

## 3.1.1 A dimensão legal

**Factores de sucesso**

Algumas directivas de legislação nacionais e convenções internacionais vinculam juridicamente as organizações a colocar em prática medidas de segurança local. Como resultado, os gestores da organização, em virtude desta delegação de autoridade, têm uma obrigação em relação às medidas de segurança (mas não uma obrigação em termos de resultados). A pessoa jurídica que é culpada de um lapso de segurança levando a uma infracção pode ter um responsabilidade penal, civil ou de natureza administrativa.

Legislação adequada sobre o processamento de dados tem como resultado o reforço da confiança dos parceiros económicos na estrutura nacional, contribuindo para o desenvolvimento económico do país. Para além disso, ajudando a criar um contexto favorável

para a troca de dados em conformidade com a lei, torna-se o primeiro factor para a adopção de informação e comunicação baseada em serviços por parte do público em geral.

Legislação de segurança e a própria segurança podem ser vistas como duas alavancas da economia nacional. Sistemas de cibersegurança concebidos em termos de confiança e qualidade, lançam as bases para o desenvolvimento de uma economia de serviços.

### 3.1.2 Fortalecimento e aplicação de legislação

No presente momento, o cibercrime não é bem controlado, como fica claro quando se examina as estatísticas anuais produzidos pelo Computer Security Institute (CSI) ou a Computer Emergency and Response Team (CERT).

Significa isto que medidas de segurança postas em prática por organizações tendem a fornecer protecção para um determinado ambiente, num contexto particular, mas são impotentes para impedir actividades criminosas através da Internet [Parlamento Europeu (2011)].

As razões para este estado de coisas estão relacionadas, em particular, com o seguinte:

- A natureza do crime cibernético (automação, *malware* inteligente, activação remota);
- A facilidade e impunidade com que os hackers podem usurpar identidades de utilizadores legítimos, impedindo assim a capacidade do sistema jurídico para identificar os autores do acto criminoso.
- A necessidade de resolver questões de competência, antes de realizar uma investigação.
- Falta de recursos humanos e recursos materiais nos serviços responsáveis pelo anti-cibercrime.
- A natureza transnacional do crime virtual, o que exige burocracia e atrasos naturais para a assistência e cooperação internacionais e judiciárias, impondo atrasos que estão em desacordo com a velocidade dos atacantes.
- A ausência de categorias apropriadas para os crimes, em algumas jurisdições.
- A definição inadequada e a natureza transitória da maioria das evidências relacionadas a TI.

Por todas estas razões, o sistema jurídico continua sendo ineficaz no contexto da internet. Além disso, assim como existem paraísos fiscais, também existem paraísos cibernéticos, onde a "lei e a ordem" tendem a ser, por incapacidade ou conluio, permissivas (porque é que foram reportados muitos ataques aos EUA, vindos da Coreia do Norte?). A proliferação de crimes informáticos não é necessariamente um sinal de que não há leis suficientes. As leis existentes já cobrem muitas das actividades de TI dos criminosos e *hackers*. Ainda assim, novas legislações, nascidas da necessidade de definir um quadro jurídico adequado adaptado para o uso de novas tecnologias, são necessárias para complementar muitas das leis existentes, que naturalmente, já se aplicariam ao ciberespaço [Parlamento Europeu (2011)]..

### 3.1.3 Combate à cibercriminalidade, respeitando a privacidade digital: um compromisso complicado

Os meios necessários para combater o flagelo internacional crescente de crimes cibernéticos exigem um quadro legal que tenha sido harmonizado a nível internacional e possa ser

aplicado de forma eficaz, juntamente com os meios equilibrados para uma verdadeira cooperação internacional ao nível das autoridades policiais e da justiça.

Os governos nacionais têm importantes responsabilidades na garantia de segurança cibernética. Isto é particularmente verdadeiro para a definição do quadro jurídico adequado, ou seja, aquele que é uniforme e efectivo, para a promoção de uma cultura de segurança que irá respeitar o direito dos indivíduos à privacidade digital, e simultaneamente reforçar os esforços para combater o cibercrime.

A luta contra o cibercrime deve ter como objectivo principal a protecção dos indivíduos, organizações e países, tendo em conta os princípios fundamentais da democracia.

As ferramentas usadas para combater o cibercrime são potencialmente hostis aos direitos humanos, e podem comprometer a privacidade das informações pessoais. Observatórios e/ou uma cúpula de monitorização estatal são essenciais para que os abusos de poder e de posição sejam evitados [Parlamento Europeu (2011)]..

## 3.1.4 As Recomendações Legislativas ao Nível internacional

## 3.1.5 OCDE e as linhas orientadoras

Atenda-se à transcrição e tradução das linhas orientadoras da Organização de Cooperação e de Desenvolvimento Económicos, cujo conteúdo, quase 10 anos depois, permanece actual e com uma vigência fortalecida.

### *3.1.5.1 Consciencialização*

***Os participantes devem estar conscientes da necessidade de segurança dos sistemas e das redes de informação.***

*A consciencialização dos riscos e dos mecanismos de salvaguarda disponíveis é a primeira linha de defesa da segurança dos sistemas e das redes de informação. Os sistemas e as redes de informação podem estar expostos a riscos internos e externos. Os participantes devem compreender que as falhas de segurança se podem repercutir em danos significativos para os sistemas e as redes de informação sob o seu controlo. Devem também estar conscientes do dano potencial que pode ser causado a outros em consequência da inter-conectividade e interdependência. Os participantes devem estar conscientes das configurações e das actualizações disponíveis para os seus sistemas, do seu lugar dentro das redes, das boas práticas que podem implementar para melhorar a segurança, e das necessidades de outros participantes.*

### *3.1.5.2 Responsabilidade*

***Os participantes são responsáveis pela segurança dos sistemas e das redes de informação.***

*Os participantes dependem de sistemas e redes de informação interligados a nível local e global e devem compreender a sua responsabilidade na salvaguarda da segurança desses sistemas e redes de informação. Devem ser responsáveis de uma maneira apropriada ao papel de cada um. Os participantes devem rever regularmente as suas políticas, práticas, medidas e procedimentos e avaliar se estão adaptados ao seu ambiente. Aqueles que desenvolvem, concebem e fornecem produtos e serviços devem tomar em conta a segurança*

*dos sistemas e das redes e distribuirem de maneira oportuna informação apropriada incluindo actualizações de modo a que os utilizadores sejam capazes de compreender melhor as funcionalidades de segurança dos produtos e serviços e as suas responsabilidades em relação a este assunto.*

#### *3.1.5.3 Reacção*

***Os participantes devem agir com prontidão e em cooperação de forma a prevenir, detectar e reagir a acidentes de segurança.***

*Tendo em conta a inter-conectividade dos sistemas e das redes de informação, assim como a propensão dos danos se alastrarem rápida e massivamente, os participantes devem reagir com prontidão e num espírito de cooperação aos incidentes de segurança. Eles devem partilhar informação sobre as ameaças e as vulnerabilidades de modo apropriado e implementar os procedimentos para uma cooperação rápida e eficaz a fim de prevenir e detectar os incidentes de segurança e lhes dar resposta. Sempre que permitido, tal pode envolver a partilha de informação e a cooperação transfronteiriça.*

#### *3.1.5.4 Ética*

***Os participantes devem respeitar os interesses legítimos dos outros.***

*Devido à omnipresença dos sistemas e das redes de informação nas nossas sociedades, os participantes devem estar conscientes de que a sua acção ou inacção pode prejudicar outros. É, portanto, indispensável manter uma conduta ética e os participantes devem esforçar-se por desenvolver e adoptar melhores práticas e promover uma conduta que reconheça as necessidades de segurança e que respeite os interesses legítimos dos outros.*

#### *3.1.5.5 Democracia*

***A segurança dos sistemas e das redes de informação devem ser compatíveis com os valores essenciais de uma sociedade democrática.***

*A segurança deve ser implementada de forma consistente com os valores reconhecidos pelas sociedades democráticas, nomeadamente a liberdade de intercâmbio de pensamentos e de ideias, o livre fluxo de informação, a confidencialidade da informação e da comunicação, a protecção adequada da informação de carácter pessoal, a abertura e a transparência.*

#### *3.1.5.6 Avaliação do risco*

***Os participantes devem levar a cabo avaliações de risco.***

*A avaliação do risco identifica ameaças e vulnerabilidades e deve ser suficientemente ampla de forma a abranger os factores chave, internos e externos, tais como tecnologia, factores humanos e físicos, políticas e serviços prestados por terceiras partes com implicações de segurança. A avaliação do risco permitirá determinar o nível aceitável de risco e facilitará a selecção dos controlos apropriados para a gestão o risco de danos potenciais aos sistemas e redes de informação à luz natureza e importância da informação a ser protegida. Devido à crescente inter-conectividade dos sistemas de informação, a avaliação do risco deve ter em conta o dano possível que pode ter origem ou ser causado por outros participantes.*

#### *3.1.5.7 Concepção e implementação da segurança.*

***Os participantes devem incorporar a segurança como um elemento essencial dos sistemas e das redes de informação.***

*Os sistemas, as redes e as políticas devem ser concebidas, implementadas e coordenadas de forma apropriada de modo a optimizar a segurança. Um enfoque maior mas não exclusivo deste esforço deve ser a concepção e a adopção de medidas de protecção e de soluções apropriadas a fim de prevenir ou evitar os possíveis danos devidos às ameaças e vulnerabilidades identificadas. As medidas de protecção e as soluções devem ser de âmbito técnico e não-técnico e ser proporcionais ao valor da informação nos sistemas e redes de informação da organização. A segurança deve ser um elemento fundamental do conjunto dos produtos, serviços, sistemas e redes e parte integrante da concepção e arquitectura dos sistemas. Para o utilizador final, a concepção e a implementação da segurança consistem essencialmente na selecção e configuração dos produtos e serviços para os seus sistemas.*

#### *3.1.5.8 Gestão da segurança*

***Os participantes devem adoptar uma aproximação integral da gestão da segurança.***

*A gestão da segurança deve estar baseada na avaliação dos riscos e ser dinâmica e global de forma a cobrir todos os níveis de actividade dos participantes e todos os aspectos das suas operações. Deve incluir possíveis respostas antecipadas às ameaças emergentes e considerar a prevenção, detecção e resposta a incidentes que afectem a segurança, a recuperação de sistemas, a manutenção permanente, a revisão e a auditoria. As políticas, práticas, medidas e procedimentos de segurança de redes e sistemas de informação devem ser coordenados e integrados de forma a criar um sistema coerente de segurança. Os requisitos da gestão de segurança dependem do nível de participação, do papel desempenhado pelos participantes, dos riscos em jogo e dos requisitos do sistema.*

#### *3.1.5.9 Reavaliação*

***Os participantes devem proceder a revisões e reavaliações da segurança dos sistemas e das redes de informação e fazer as modificações apropriadas nas suas políticas, práticas, medidas e procedimentos de segurança.***

*Vulnerabilidades e ameaças novas e evolutivas estão permanentemente a ser descobertas. Os participantes devem rever, reavaliar e modificar todos os aspectos da segurança de modo contínuo de forma a poder fazer face a estes riscos evolutivos.*

### 3.1.6 Legislação cibercrime Internacional

Além da directiva europeia de 1995, outras leis para a protecção de informações pessoais foram aplicadas, em vários países, ao longo dos anos:

- Alemanha: Lei de 21 de Janeiro de 1977
- Argentina: Lei sobre a protecção das informações pessoais, 1996
- Áustria: Lei de 18 de Outubro de 1978
- Austrália: Lei sobre privacidade, 1978
- Bélgica: Lei de 08 Dezembro de 1992
- Canadá: Lei sobre a protecção de informação privada, 1982
- Dinamarca: Lei de 08 de Junho de 1978
- Espanha: Lei de 29 de Outubro de 1992
- Estados Unidos: Lei sobre as liberdades de protecção individual, de 1974; Lei de bases de dados de informações privadas, 1988
- Finlândia: Lei de 30 de Abril de 1987

- França: Lei sobre tecnologia da informação e liberdade de 06 de Janeiro de 1978, alterada em 2004
- Grécia: Lei de 26 de Março de 1997
- Hungria: Lei sobre a protecção das informações pessoais e à comunicação de informação pública, 1992
- Irlanda: Lei de 13 Julho de 1988
- Islândia: Lei sobre a gravação de informação pessoal, 1981
- Israel: Lei sobre a protecção da privacidade, 1981, 1985, 1996; Lei sobre a protecção de informação na administração de 1986
- Itália: Lei de 31 de Dezembro de 1996
- Japão: Lei sobre a protecção de informações pessoais, 1988
- Luxemburgo: Lei de 31 de Março de 1979
- Noruega: Lei de registos de dados pessoais, 1978
- Nova Zelândia: lei sobre a informação oficial de 1982
- Holanda: Lei de 28 de Dezembro de 1988
- Polónia: Lei sobre a protecção das informações pessoais, 1997
- Portugal: Lei de 29 de Abril de 1991
- República Checa: Lei sobre a protecção das informações, 1995
- Reino Unido: Lei de 12 de Julho de 1988
- Rússia: A lei federal sobre a informatização, informação e protecção de informações
- Eslovénia: Lei sobre a protecção da informação, 1990
- Suécia: 11 de Maio de 1973
- Suíça: A lei federal sobre a protecção de informação, 1992
- Taiwan: Lei sobre a protecção da informação, 1995

A primeira convenção internacional criada para atender o carácter internacional do cibercrime foi o Conselho da Europa "Convenção sobre o Cibercrime" (Conselho da Europa [2001]), adoptado em Bruxelas em 23 de Novembro de 2001, que entrou em vigor em Julho de 2004 (após a sua ratificação por cinco dos países signatários, em que pelo menos três dos quais tiveram que ser do Conselho da Europa). A convenção contém os seguintes pontos.

**Direito penal material:**

- Crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos;
- Crimes informáticos;
- Infracções relacionadas com violações dos direitos de autor e direitos conexos.

**O direito processual:**

- *Preservação expedita de computador e tráfego de dados e divulgação rápida dos últimos às autoridades competentes;*
- *Preservação e manutenção da integridade dos dados do computador por um período de tempo tão longo quanto necessário para permitir às autoridades competentes para buscar a sua divulgação;*
- *Ordem de produção;*
- *Busca e apreensão de dados informáticos armazenados;*
- *Recolha em tempo real de dados informáticos;*

- *A adequada protecção dos direitos humanos e liberdades.*

*Cada Estado tem de adoptar as medidas legislativas e outras necessárias para estabelecer a jurisdição sobre as seguintes infracções, sem prejuízo de seu direito interno:*

- *Quando cometido intencionalmente, o acesso a toda ou qualquer parte de um sistema de computador sem direito;*
- *Quando cometido intencionalmente, a interceptação, sem direito de não-pública as transmissões de dados para, de ou dentro de um sistema de computador.*

*[Parlamento Europeu, tratados (2009, 2010, 2011)]*

### 3.1.7 O valor económico da legislação

Organizações devem dotar-se de meios adequados de segurança e controlo.

O valor económico dos investimentos necessários para garantir um nível mínimo de segurança (protecção física e legal) varia de acordo com o potencial da organização e eventuais perdas e os riscos à sua reputação e imagem. Legislação é, portanto, um factor endógeno de segurança.

Os Fornecedores de email devem ter uma abordagem mais pró-activa na monitorização do spam e identificar a fonte, de forma que acções apropriadas possam ser tomadas pelos ISPs originários.

As listas de reputação têm sem dúvida um papel fulcral e deverão ser incluídas no âmbito legal. Um pouco como as agências de rating, estas listas acabam por ter um poder desmesurado na na gestão das redes mundiais.

Os Fornecedores deveriam automatizar os processos de denúncia de abusos, possivelmente adoptando o formato de denúncia de abuso (ARF).

Os fornecedores devem procurar soluções de colaboração para combater o spam, como muitos, mas não todos, já fazem. Por exemplo, notificando ISPs que originam spam e discutindo medidas preventivas com eles são iniciativas que teoricamente irão ajudar a debelar mais spam na fonte.

Além disso, relatórios encaminhados para as autoridades podem ajudar estas a tomar as medidas legais ou a desenvolver as políticas adequadas para lidar com tais fontes (ENISA [2010]).

Decisores políticos e autoridades reguladoras poderiam ajudar os esforços de prevenção de spam por clarificar os conflitos aparentes entre filtragem de spam, privacidade e obrigação de entregar.

Os dados claramente indiciam uma necessidade dos governos legislarem favoravelmente contra o Impacto causado, quer pelo spam, quer por outros tipos de fraudes de internet (vírus, *bots*, *phishing*, etc.)

Iniciativas recentes do Governo Norte-americano, adicionáveis à já existente legislação na Austrália e Japão (bem como o Programa Conjunto na Alemanha, aqui explanado),

conseguiram que todos os prestadores (ISPs) se juntassem numa Solução. Iniciativas estas que tem obtido resultados notáveis.

Portugal, já com a legislação adequada, requer uma iniciativa similar à alemã, encabeçada (ou gerida) por uma entidade autónoma (talvez a ANACOMou o CEDRT.pt) que conseguisse comprometer todos (ou pelo menos os maiores) ISPs a operar em Portugal.

## 3.2 As Recomendações legislativas existentes ao Nível Europeu

### 3.2.1 Recomendações da ENISA

A ENISA, em conjunto com autoridades europeias, identificou uma série de contra-medidas que devem ser considerados em termos nacionais e à escala da EU, e que visam:

- Coordenação pan-europeia para o comércio transfronteiriço de riscos;
- A colaboração com as autoridades nacionais para a protecção de infra-estrutura crítica;
- Promoção de iniciativas regulatórias que complementem, apoiem e incentivem a organização das medidas de resiliência;
- A nível da EU, a monitorização e sistemas de alerta precoce sobre ameaças externas;
- A criação ou participação em planos de emergência nacionais relacionados com infra-estrutura;
- A identificação dos níveis de resiliência necessários a infra-estruturas críticas;
- A focalização nas interdependências de infra-estruturas - com foco na identificação de questões práticas e para a mitigação de risco;
- Acompanhar a exposição de plataformas tecnológicas e mitigá-los a nível da UE;

Os desafios e as contra-medidas discutidas podem desempenhar um papel importante na eliminação dos obstáculos todos os operadores de rede, independentemente da sua dimensão e maturidade, terá que enfrentar em diversos casos. As medidas propostas podem ajudar os gestores de Fornecedores de rede a aumentar a suar resiliência e a compreender as tendências na mitigação.

### 3.2.2 Recomendações da OCDE

> *O CONSELHO, considerando*
>
> *A Recomendação do Conselho em relação com As Linhas Orientadoras que regulam a privacidade da vida privada e dos fluxos transfronteiriços de dados de carácter pessoal, de 23 de Setembro de 1980 [C(80)58(Final)];*

*A Declaração sobre os fluxos transfronteiriços de dados adoptada pelos Países Membros da OCDE de 11 de Abril de 1985 [Anexo a C(85)139];*

*A Recomendação do Conselho relativa às Linhas Orientadoras para a Política de Criptografia de 27 de Março de 1997 [C(97)62/FINAL];*

*A Declaração Ministerial sobre a Protecção da Privacidade em Redes Globais de 7-9 de Dezembro de 1998 [Anexo a C(98)177/FINAL];*

*A Declaração Ministerial sobre a Autenticação para o Comércio Electrónico de 7-9 de Dezembro de 1998 [Anexo a C(98)177/FINAL];*

*E reconhecendo que:*

*Os sistemas e as redes de informação são cada vez mais utilizados e de maior valor para os governos, as empresas, outras organizações e utilizadores individuais;*

*O papel cada vez mais importante que os sistemas e as redes de informação jogam na estabilidade e na eficiência das economias nacionais, do comércio internacional, assim como na vida social, cultural e política, e o acentuação da dependência neles impõem esforços especiais para proteger e promover a confiança neles;*

*Os sistemas e as redes de informação e a sua expansão à escala mundial são acompanhados de novos riscos e em número crescente;*

*Os dados e as informações arquivados e transmitidos através de sistemas e de redes de informação são sujeitos a ameaças em resultado dos vários meios de acesso e uso não autorizado, de apropriação abusiva, de alteração, de transmissão de código malicioso, de impedimento de serviço ou de destruição e requerem as salvaguardas apropriadas;*

*É necessário aumentar a consciencialização dos riscos para os sistemas e redes de informação, bem como das políticas, práticas, medidas e procedimentos disponíveis para dar resposta a esses riscos e, também, de encorajar comportamentos apropriados como um passo crucial para o desenvolvimento de uma cultura de segurança;*

*É necessário rever as políticas, as práticas, as medidas e os procedimentos actuais para ajudar a garantir que estes respondam de forma adequada aos desafios, em constante evolução, que são colocados por ameaças aos sistemas e redes de informação;*

*Há um interesse comum na promoção da segurança dos sistemas e das redes de informação através de uma cultura de segurança que incentive a coordenação e a cooperação internacional com vista a dar resposta aos desafios colocados pelos potenciais prejuízos que as falhas de segurança são susceptíveis de causar às economias nacionais, ao comércio internacional e à participação na vida social, cultural e política.*

*Reconhecendo também que:*

*As Linhas Orientadoras para a Segurança dos Sistemas e das Redes de Informação: Para uma Cultura de Segurança, em anexo à presente Recomendação, são de aplicação voluntária e não afectam os direitos soberanos dos Estados;*

*Estas linhas orientadoras não pretendem sugerir que existe uma solução única, qualquer que ela seja, em matéria de segurança ou quais as políticas, as práticas, as medidas e os procedimentos apropriados para uma determinada situação, mas sim fornecer um quadro mais geral de princípios que promova junto dos participantes um melhor entendimento de como podem beneficiar e contribuir para o desenvolvimento de uma cultura de segurança;*

*PRECONIZA a aplicação destas Linhas Orientadoras para a Segurança dos Sistemas e das Redes de Informação aos governos, empresas, outras organizações e utilizadores individuais que desenvolvam, possuam, forneçam, giram, mantenham e utilizem sistemas e redes de informação;*

*RECOMENDA aos países membros que:*

*Estabeleçam novas políticas, práticas, medidas e procedimentos, ou alterem as existentes, de forma a reflectirem e a tomarem em conta as Linhas Orientadoras para a Segurança dos Sistemas e das Redes de Informação: Para uma Cultura de Segurança, adoptando e promovendo uma cultura de segurança tal como exposto nas Linhas Orientadoras;*

*Consultem, coordenem e cooperem a nível nacional e internacional para implementarem estas Linhas Orientadoras;*

*Disseminem estas Linhas Orientadoras pelos sectores público e privado, incluindo governos, empresas, outras organizações e utilizadores individuais por forma a promover uma cultura de segurança e a encorajar todas as partes interessadas a serem responsáveis e a tomarem todos os passos necessários para implementarem estas Linhas Orientadoras de uma maneira apropriada com o papel de cada um;*

*Tornem estas Linhas Orientadoras disponíveis a países não-membros o mais rapidamente possível e de forma apropriada;*

*Revejam estas Linhas Orientadoras cada cinco anos de modo a promoverem a cooperação internacional sobre as questões relacionadas com a segurança dos sistemas e das redes de informação;*

*[OCDE (2010)]*

## 3.3 Legislação portuguesa afecta ou afectável ao Problema

No caso português, e equivalente em muitos países europeus, a legislação contra o Cibercrime está em estágios muito pouco avançados, direi mesmo redutores, não estando patente a

abrangência deste segmento com outras peças sociais, como sejam os direitos de liberdade de expressão, os acordos de serviços, entre outros.

| Tipo de Documento | Código | Titulo | Data de Entrada em Vigor | Aplicável a |
|---|---|---|---|---|
| Norma | ISO 9001:2008 | Sistema de Gestão da Qualidade. Requisitos | Nov.2008 | Toda a organização |
| Lei do Código do Trabalho | Lei nº7/2009 de 12 de Fevereiro | Aprova a revisão do Código do Trabalho | 12-02-2009 | Recursos Humanos: contratos de Trabalho/ acordos de confidencialidade |
| Lei da Segurança e saúde no trabalho | Lei nº102/2009 de 10 de Setembro | Regime jurídico da promoção da segurança e saúde no trabalho | 10-09-2009 | Toda a organização. |
| Lei das Comunicações Electrónicas | LEI N.º 5/2004, DE 10 DE FEVEREIRO | Regime jurídico aplicável às redes e serviços de comunicações electrónicas. | 11-02-2004 | Comunicações Electrónicas |
| Lei das Comunicações Electrónicas | LEI N.º 35/2008, DE 28 DE JULHO | Segunda alteração à Lei n.º 5/2004, de 10 de Fevereiro (Lei das Comunicações Electrónicas) | 29-07-2008 | Comunicações Electrónicas |
| Lei das Comunicações Electrónicas | LEI N.º 32/2009, DE 9 DE JULHO | Legislar sobre o regime de acesso aberto às infra - estruturas aptas ao alojamento de redes de comunicações electrónicas e a estabelecer o regime de impugnação dos actos do ICP | 10-07-2009 | Comunicações Electrónicas |

| | | | | |
|---|---|---|---|---|
| | | -ANACOM aplicáveis no âmbito do regime de construção, acesso e instalação de redes e infra - estruturas de comunicações electrónicas. | | |
| Lei das Comunicações Electrónicas | D.L. n.º 176/2007 | Alteração à Lei nº 5/2004, de 10 de Fevereiro | 11-02-2007 | Comunicações Electrónicas |
| Lei de Protecção de Dados Pessoais | LEI N.º 41/2004, DE 18 DE AGOSTO | Transpõe para a ordem jurídica nacional a Directiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas | 19-08-2004 | Dados Pessoais |
| Lei de Protecção de Dados Pessoais | DECRETO-LEI N.º 7/2004, DE 7 DE JANEIRO | Transpõe para a ordem jurídica nacional a Directiva 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho de 2000, relativa a certos aspectos legais dos serviços da sociedade da informação, em especial do comércio electrónico, no mercado interno. [Artigo 22º - Comunicações não solicitadas] | 07-01-2004 | Dados Pessoais |
| Lei de Protecção de Dados Pessoais | LEI N.º 67/98, DE 26 DE OUTUBRO | Transpõe para a ordem jurídica portuguesa a Directiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados | 27-10-1998 | Dados Pessoais |

| | | | | |
|---|---|---|---|---|
| Lei de Protecção de Dados Pessoais | LEI N.º 32/2008, DE 17 DE JULHO | Transpõe para a ordem jurídica interna a Directiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações | 18-07-2008 | Dados Pessoais |
| Leis do Comércio Electrónico | DECRETO-LEI N.º 7/2004, DE 7 DE JANEIRO | Transpõe para a ordem jurídica nacional a Directiva 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho de 2000, relativa a certos aspectos legais dos serviços da sociedade da informação, em especial do comércio electrónico, no mercado interno | 07-01-2004 | Comércio Electrónico |
| Leis do Comércio Electrónico | DECRETO-LEI N.º 62/2009, DE 10 DE MARÇO | Alteração ao Decreto -Lei n.º 7/2004, de 7 de Janeiro | 31-05-2009 | Comércio Electrónico |
| Leis do Comércio Electrónico | LEI N.º 7/2003, DE 9 DE MAIO | Transposição da Directiva nº 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho | 09-05-2003 | Comércio Electrónico |
| Leis do Comércio Electrónico (Assinatura Electrónica) | DECRETO-LEI N.º 290-D/99, DE 2 DE AGOSTO | Aprova o regime jurídico dos documentos electrónicos e da assinatura digital | 03-08-1999 | Assinatura Electrónica |
| Leis do Comércio Electrónico (Assinatura Electrónica) | DECRETO-LEI N.º 62/2003, DE 3 DE ABRIL | O presente decreto-lei transpõe para a ordem jurídica interna a Directiva n.o 1999/93/CE, do Parlamento Europeu e do Conselho, de 13 de Dezembro, relativa a um quadro legal comunitário para as assinaturas electrónicas. | 04-04-2003 | Assinatura Electrónica |
| Leis do | Decreto-Lei | O Decreto-Lei n.o 62/2003, | 06-07-2004 | Assinatura |

| | | | | |
|---|---|---|---|---|
| Comércio Electrónico (Assinatura Electrónica) | n.o 165/2004<br>de 6 de Julho | de 3 de Abril, procurou compatibilizar o regime jurídico da assinatura digital, estabelecido no Decreto-Lei n.o 290-D/99, de 2 de Agosto, com a Directiva n.o 1999/93/CE, do Parlamento Europeu e do Conselho, de 13 de Dezembro, relativa a um quadro legal comunitário para as assinaturas electrónicas. | | Electrónica |
| Leis do Comércio Electrónico (Assinatura Electrónica) | DECRETO REGULAMENTAR N.º 25/2004, DE 15 DE JULHO | O presente diploma regulamenta o Decreto-Lei nº290-D/99, de 2 de Agosto, com a redacção que lhe foi dada pelo Decreto-Lei nº62/2003, de 3 de Abril. | 16-07-2004 | Assinatura Electrónica |
| Leis do Comércio Electrónico (Assinatura Electrónica) | DECRETO-LEI N.º 88/2009, DE 9 DE ABRIL | Alteração ao Decreto -Lei n.º 290 -D/99, de 2 de Agosto | 10-04-2009 | Assinatura Electrónica |
| Leis do Comércio Electrónico (Dados Pessoais) | LEI N.º 41/2004, DE 18 DE AGOSTO | Transpõe para a ordem jurídica<br>nacional a Directiva nº2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas, com excepção do seu artigo 13.o, referente a comunicações não solicitadas. | 19-08-2044 | Dados Pessoais |
| Leis do Comércio Electrónico (Dados Pessoais) | LEI N.º 67/98, DE 26 DE OUTUBRO | Transpõe para a ordem jurídica portuguesa a Directiva nº 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados). | 27-10-1998 | Dados Pessoais |

| | | | | |
|---|---|---|---|---|
| Legislação Comunitária<br>(Comunicações Electrónicas) | REGULAMENTO (CE) N.º 1211/2009 DO PARLAMENTO EUROPEU E DO CONSELHO, DE 25.11.2009 | Regulamento (CE) n.º 1211/2009 do Parlamento Europeu e do Conselho, de 25 de Novembro de 2009, que cria o Organismo de Reguladores Europeus das Comunicações Electrónicas (ORECE) e o Gabinete. | 18-12-2009 | Comunicações Electrónicas |
| Legislação Comunitária<br>(Comunicações Electrónicas) | RECTIFICAÇÃO AO REGULAMENTO (CE) N.º 1211/2009, DE 1.4.2010 | Regulamento (CE) n.º 1211/2009 do Parlamento Europeu e do Conselho, de 25 de Novembro de 2009, que cria o Organismo de Reguladores Europeus das Comunicações Electrónicas (ORECE) e o Gabinete. | 01-04-2010 | Comunicações Electrónicas |
| Legislação Comunitária<br>(Comunicações Electrónicas) | DIRECTIVA 2006/24/CE DO PARLAMENTO EUROPEU E DO CONSELHO, DE 15.3.2006 | Directiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações e que altera a Directiva 2002/58/CE. | 13-04-2006 | Comunicações Electrónicas |
| Legislação Comunitária<br>(Comunicações Electrónicas) | DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, OF 25.11.2009 | Amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. | 18-12-2009 | Comunicações Electrónicas |

| | | | | |
|---|---|---|---|---|
| Legislação Comunitária<br>(Segurança dos Sistemas e Redes de Informação) | REGULAMENTO (CE) N.º 717/2007 DO PARLAMENTO EUROPEU E DO CONSELHO, DE 27.6.2007 | Regulamento relativo à itinerância nas redes telefónicas móveis públicas da Comunidade e que altera a Directiva 2002/21/CE. | 29-06-2007 | Segurança dos Sistemas e Redes de Informação |
| Legislação Comunitária<br>(Segurança dos Sistemas e Redes de Informação) | DIRECTIVA 2002/58/CE PARLAMENTO EUROPEU E DO CONSELHO, DE 12.7.2002 | Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas - Directiva relativa à privacidade e às comunicações electrónicas. | 31-07-2002 | Segurança dos Sistemas e Redes de Informação |
| Legislação Comunitária<br>(Segurança dos Sistemas e Redes de Informação) | DIRECTIVA 2006/24/CE DO PARLAMENTO EUROPEU E DO CONSELHO, DE 15.3.2006 | Directiva relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE. | 13-04-2006 | Segurança dos Sistemas e Redes de Informação |
| Legislação Comunitária<br>(Segurança dos Sistemas e Redes de Informação) | DIRECTIVA 95/46/CE DO PARLAMENTO EUROPEU E DO CONSELHO, DE 24.10.1995 | Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. | 24-10-1995 | Segurança dos Sistemas e Redes de Informação |

Tabela 3-1 Documentação Legal relacionada com a segurança informática

# 4 *Research Design: Case studies* de utilização de sistemas de reputação

Os *case studies* seleccionados, pela sua abrangência, são: técnicas de anti-spam, mercados online e Web-of-trust.

> *Nota: O conteúdo deste sub-capítulo tem por base Internet Governance [Kurbalija, Gelbstein (2005)]*.

### 4.1.1 Técnicas de Anti-Spam

A utilização de reputação para detectar quem (ou o quê) envia spam (e *phishing*, e outro *malware*) alavanca a filtragem em geral, tornando-a muito mais eficiente. De facto, na actualidade, todas as empresas fornecedoras de produtos de anti-spam, com alguma maturidade e conceituadas, utilizam os mecanismos de reputação como a principal ferramenta para filtragem, detecção e monitorização dos seus sistemas.

Os mecanismos de reputação representam uma forma dinâmica e eficiente para prever se o remetente é confiável ou a mensagem é spam.

A evolução das listas negras e brancas tradicionais, conforme explicado abaixo, à formulação de vários parâmetros, permite aumentar a capacidade de filtragem. Para além deste factor, permite aquilo que se chama de "Zero-Hour blocking", ou seja ser preventivo e debelar potenciais perigos só com base na comunicação, sem atender ao conteúdo da mensagem. Basta para tal que se compare a reputação do emissor, com listas de reputação devidamente credenciadas e capazes, e assim atribuir-lhe um qualquer tipo de pontuação que, em conjugação com outros factores, permitirá aferir fielmente a natureza das suas intenções.

Isto é particularmente valioso em face da crescente utilização de zombies como agentes de spam, que são imprevisíveis e operam por períodos curtos (não se conseguindo, por isso, detectar com base na frequência (envio massivo de spam). A origem do ataque pode mudar frequentemente, tornando o ataque mais difícil de parar recorrendo a listas negras tradicionais.

Existem várias soluções de reputação para anti-spam disponíveis no mercado, cada uma olhando para um conjunto diferente de propriedades sobre as quais a reputação é calculada.

Essencialmente, estas soluções olham para o comportamento do remetente ao longo do tempo para prever a sua "confiabilidade"; o remetente é identificado por, por exemplo, um endereço IP, um domínio, ou a mensagem em si, portanto oferecendo diferentes níveis de granularidade de filtragem.

Sistemas de reputação podem ser usados em conjunto com mecanismos que tentam avaliar a identidade do remetente. Tal é crítico para adequar o sistema ao utilizador.

As soluções de reputação podem usar informações diversas como, por exemplo, os participantes, muitas vezes no contexto de uma comunidade ou rede social, comportamentos promíscuos nas redes, queixas de outrem e, o mais usual, *spamtraps* (listas de e-mail cujo objectivo é capturar o spam, analisar e determinar padrões, tendências, remetentes, etc.).

Outros parâmetros a observar e recolher podem incluir:

- Volume de tráfego de e-mail.
- Tipo de tráfego (por exemplo, contínuo vs esporádico).
- Conformidade com os regulamentos (por exemplo, o CANSPAM nos EUA).
- E-mail com parâmetros inválidos ou mal formados.
- Resposta a pedidos de cancelamento.
- Feedback dos *spamtraps*.
- Feedback dos relatórios de utilizador.
- Filtragem e triagem de conteúdo.

Esta informação agregada, e colectada ao longo do tempo faz a reputação do remetente.

Uma Avaliação baixa da reputação do utilizador (ou o endereço IP ou domínio ou a rede) pode levar a mensagem a ser julgada como spam quando estiver a ser filtrada.

Os mecanismos de reputação que observam o remetente são tipicamente baseados em entidades centrais de monitorização baseando-se em alguns dos parâmetros listados acima. Como uma alternativa para estes modelos centralizados, um sistema de reputação distribuído envolve os participantes na partilha da reputação e em seguida calcula a pontuação de reputação localmente.

### 4.1.2 Mercados on-line

Os membros de um mercado on-line estão autorizados a vender e comprar itens dentro de uma comunidade arbitrária.

A responsabilidade do comércio dentro da comunidade é, habitualmente, delegada nos membros envolvidos. Depois que um item ter sido vendido, o vendedor e o comprador têm que trocar o artigo adquirido e ao pagamento de uma forma justa. As maiorias dos itens são bens físicos que podem ser trocados directamente entre os utilizadores, ou através de um serviço de transporte de carga que é oferecido por muitos Fornecedores.

Na maioria dos casos de mercados online, tanto o vendedor como o comprador e são expostos a alguns riscos: O risco para o comprador é que o item não seja compatível com a descrição de venda, ou que o item não seja devidamente entregue, apesar do pagamento; o risco para o vendedor é que o seu item é enviado para um comprador (desconhecido), mas o pagamento não efectuado durante ou depois do processo.

Muitas das trocas são bem sucedidas, no entanto, das 303,809 queixas de fraudes de internet, relatadas ao Internet Crime Complaint Center, dos EUA, e em 2010, 14,4% foram casos de fraudes no pagamento ou entrega de mercadoria, 7,6% foram casos de pagamentos antecipados por compras, 5,9% foram casos de fraudes em leilões, e 5,3% foram casos com cartões de crédito [I3C, Internet Crime Report (2010)].

Isto é claramente um factor que pode dificultar o desenvolvimento dos mercados on-line; e a gestão de reputação pode ajudar a mitigar esses riscos.

Depois de cada transacção, os utilizadores podem fornecer comentários e / ou pontuação relativa à operação. Estas pontuações são adicionadas a reputação dos utilizadores, e podem ser consultados durante outras operações, dando aos pares envolvidos uma forma de avaliar o risco que estão a tomar e, em geral, aumentando confiança nos mercados online.

### 4.1.3 Web-of-trust (Autenticação de Chave Pública)

Um dos problemas mais importantes do público é a autenticação com criptografia de chave pública, isto é, como se sabe que um a chave de autenticação que diz: "Esta é a chave do Rui", na verdade pertence ao Rui? A menos que o proprietário aceda ao par de chaves público / privado, não há nenhuma maneira de conferir, estando na posse apenas da chave pública. [Kurbalija, Gelbstein (2005)].

Para gerir este problema de privacidade, PGP ("Pretty Good") usa um conceito de um "apresentador" ou "terceiro de confiança" que, como intermediário, e da confiança do utilizador potencial da chave pública, atesta a validade da chave como "pertencente ao Rui". Em contraste com uma Public Key Infrastructure (PKI), que é um sistema para apoiar a terceiros introdução de chaves públicas, através de uma hierarquia de Autoridades Certificadoras, o PGP usa um web-of-trust.

Deve ser salientado que web-of-trust está listado aqui como um sistema de reputação, como um sistema que agrega opiniões subjectivas (também objectivas, sempre que possível) quanto à validade de uma afirmação (por exemplo, o David é um vendedor de confiança, o endereço IP que a Cláudia usa é um endereço usado por *spammers*, ou x é a chave pública da Patrícia).

Por outras palavras, dizer que uma web-of-trust, como a PGP, é um sistema de reputação não implica que a web-of-trust faça uma afirmação quanto à "confiabilidade" da pessoa.

#### 4.1.3.1 Em web-of-trust, sistema de PGP

No PGP, um utilizador pode ter confiança 'completa' ou 'marginal' (parcial) num apresentador. PGP também permite que cada chave pública possa ter mais que um apresentador. Como resultado, o utilizador pode então formar regras do género: "Eu vou aceitar uma chave pública como válida apenas se tiver sido introduzida por pelo menos:

a) um apresentador totalmente confiável ou
b) três apresentadores parcialmente confiáveis ".

PGP permite a formação de tais regras e automatiza o processamento de validade chave usando essas regras. Como tal, o PGP usa uma reputação sistémica, e agrega uma série de opiniões para formar confiança. Se considerarmos um sistema de reputação como uma rede de entidades que avalia opiniões um do outro, então podemos assumir que PGP

Implementa um sistema de reputação descentralizado. Eis algumas características deste sistema:

- Entidades são identificadas pelos seus endereços de correio electrónico.
- Assinar uma chave representa a opinião do signatário que a chave a ser assinada é válido, ou seja, é realmente propriedade da pessoa com o alegado e-mail.

# 5 *Case Study* sobre reputação online: o exemplo da BP

Em 20 de Abril de 2010, um dos piores derramamentos de petróleo na história começou com uma explosão na plataforma de perfuração Transocean Deepwater Horizon, utilizada pela British Petroleum (BP). Até o final dos dois primeiros meses, BP sofria prejuízos enormes devido a este desastre: perdeu mais de 67 bilhões (USD) em capitalização nas primeiras seis semanas. E se isto não era um forte indício de que a sua reputação estava a ser muito afectada, o que dizer dos boicotes à empresa, que obrigaram muitos postos de abastecimento a cobrir os logótipos para conseguirem vender? A BP precisava de um milagre – um milagre de gestão da Reputação Online

**Métodos desonestos que envolvam a gestão da reputação online**
Reconhecendo que o aumento da cobertura pelos media, e principalmente o número de comentários e *posts* na Internet estavam a crescer muito rapidamente, a BP agiu rapidamente para mitigar os danos … na sua reputação.

O primeiro passo no seu caminho para a recuperação foi uma enorme campanha pay-per-click, através do Google AdWords. A BP comprou termos de busca relevantes, tais como "oil spill", e "top kill", gastando cerca de 3,7 milhões (USD) num mês (aproximadamente 65 vezes o seu volume de publicidade normal).
Esta iniciativa gerou bastantes crítica como, por exemplo, Pamela Seiple, especialista em Internet Marketing para o blog HubSpot, que escreveu: “Os críticos estão a bater na estratégia PPC (pay-per-click) da BP, considerando-a antiética, uma vez que empurra para baixo outros resultados da pesquisa”. Ela acrescentou: “Em vez de gastar tanto dinheiro em palavras-chave altamente competitivas numa campanha de pay-per-click, A BP poderia ter feito melhor se impulsionasse a sua imagem através da atribuição de dinheiro para os esforços de recuperação do derramamento de óleo."
O resto do esforço da BP no controlo da sua reputação residiu em controlar opiniões públicas. Por exemplo, The Gulf of Mexico Foundation (GMF), que descreve os seus objectivos como “garantir uma qualidade de vida sustentável para os moradores e visitantes do litoral do Golfo", foi destaque na primeira página do NY Times, com a citação do seu director executivo, Quenton R. Dokken, minimizando a gravidade da catástrofe:. "O céu não está a cair. Nós certamente pisámos um buraco e vamos ter que trabalhar para sair dele, mas não é o fim do Golfo do México" - Em nenhum lugar do artigo era mencionado que a GMF é fortemente apoiado pela indústria do petróleo -.
Noutro exemplo, a AmericaWetland Foundation (AWF) apresentou-se nos media oferecendo-se “como um árbitro neutro, trazendo para a mesa os interesses diversos, de procura e estabelecimento de soluções para garantir a sustentabilidade do ambiente costeiro da Louisiana e as actividades económicas que lá ocorrem, para o grande benefício da nação." - Na verdade, a AWF é financiada por "Um grupo de empresas petrolíferas como a BP, Shell, ExxonMobil, Citgo, (…)”.A AWF patrocinou um vídeo com a actriz Sandra Bullock pedindo ao contribuinte americano para pagar "um plano para restaurar Golfo dos Estados Unidos (…) para as futuras gerações." Bullock rapidamente se afastou da campanha quando soube do patrocínio da indústria do petróleo à AWF, e o vídeo parece ser difícil de encontrar agora na

internet ".
Ainda noutro exemplo, o Dauphin Island Sea Lab no Alabama foi amplamente relatado em Março de 2011 com o argumento de que as mortes em massa de golfinhos no Golfo seriam uma reacção a um influxo de água fria por um escoamento de neve fora do comum. No entanto, a BP doou US $ 5 milhões para o Sea Lab em Julho de 2011 e os cientistas da Administração Nacional Oceanográfica e Atmosférica frisaram que os golfinhos evitam a água fria e que as mortes destes estariam provavelmente relacionadas com o derrame.

As implicações morais e éticas são claras. Na era do acesso instantâneo, os mecanismos de Online Reputation Management e Search Engine Optimization das empresas são os reis da percepção do público, porque o grau de preocupação do público médio raramente se estende além da primeira página de resultados de uma pesquisa.

Um estudo de 2004 por Bernard J. Jansen e Amanda Spink [citado por Kabay, M.E (2011)], intitulado "Como estamos na busca na World Wide Web?" relatou que a percentagem de utilizadores que visualizavam apenas a primeira página de resultados em motores de busca, aumentou de 29% em 1997 para 73% em 2002.

Certamente existe ética nas Relações Públicas digitais das empresas, mas casos como o da BP representam a exploração, engano e manipulação que paira no mundo digital.

E se pensarmos que é preciso muito dinheiro e poder para manipular a informação deste modo, pensemos também que quanto menor é a importância do caso, da empresa, ou mesmo da pessoa, menos custará decerto manipular a informação. Ainda mais se equacionarmos que são as primeiras impressões (antes de se conterem os danos) que ficam nas mentes dos leitores, em especial num mundo onde as notícias fluem muito rapidamente e que o destaque a cada notícia não dura mais que uns dias.

Até o final de 2010, a BP registou um aumento de 30% de lucros no quarto trimestre, em relação a 2009 – Afinal compensa!

MITIGAÇÃO DO MALWARE PARA O DESENVOLVIMENTO EMPRESARIAL EM PORTUGAL

**Rui Diogo Duarte Mendes Serra**

**Lisboa, 2011**

ISCTE Business School
Instituto Universitário de Lisboa