Gabinete de Estratégia e Estudos
Ministério da Economia

Temas Económicos

Número 56

Agosto de 2018

A Cibersegurança em Portugal

Gabriel Osório de Barros

Rua da Prata, nº 8 - 1149-057 Lisboa
Tel.: (351) 217921372
Fax: (351) 217921398
Web Site: www.gee.min-economia.pt

ISSN 1647-6204

Índice

Nota: O Tema Económico é da exclusiva responsabilidade do seu autor e não reflecte obrigatoriamente as posições do GEE nem do Ministério da Economia.

A Cibersegurança em Portugal[1]

Gabriel Osório de Barros *

1. Introdução

Segundo estudo da Accenture Strategy e da Oxford Economics, Portugal ocupa a 21.ª posição (entre 33 países analisados) em termos de Índice de Densidade Digital (IDD)[2] de 2017. O mesmo estudo estima que o peso da área digital no PIB é inferior a 20%, valor abaixo da média dos países desenvolvidos (28%). O estudo refere ainda que "a Economia Digital representa cerca de 28% do PIB dos países desenvolvidos, cerca de 6 vezes mais do que os 5% tradicionalmente estimados".

A concretização do Mercado Único Digital constitui uma das dez prioridades políticas da União Europeia e da Comissão Juncker. A prossecução deste desígnio exige uma maior digitalização da economia e capacitação dos cidadãos em termos de competências digitais.

Tendo em conta aquele princípio e as suas potencialidades na criação de emprego e de crescimento económico, a União Europeia apostou numa estratégia de digitalização da economia. Portugal tem procurado concretizar aquele desígnio através da Estratégia Indústria 4.0 (dirigida à digitalização da Economia), aliada à Iniciativa Nacional Competências Digitais INCoDe.2030 (procurando promover a inclusão e a literacia digitais).

Mas, se é certo que a promoção da Economia Digital apresenta grandes potencialidades para o crescimento da Economia e para o bem-estar dos cidadãos (utilizando as Tecnologias de Informação e Comunicação (TIC) para promover a qualidade do serviço prestado), este novo paradigma acarreta desafios ao nível da Cibersegurança que podem ter elevados impactos económicos.

O Regulamento Geral de Protecção de Dados (RGPD) que entrou em vigor no dia 25 de maio de 2018 introduz um novo regime em matéria de protecção de dados pessoais e constitui um passo também ao nível das questões de Cibersegurança, ao criar regras para o tratamento dos dados pessoais, definindo ainda novas regras e procedimentos do ponto de vista tecnológico. Não obstante, este é apenas um pequeno passo no que diz respeito às políticas públicas necessárias para garantir a Cibersegurança.

Adicionalmente, o inquérito sobre a percepção de Ciber-risco realizado a 1.300 executivos numa parceria entre a Marsh e a Microsoft (Fevereiro de 2018) verificou que 70% dos membros dos conselhos de administração classificam o Ciber-risco como uma das principais preocupações e apenas 14% estão confiantes na capacidade de resposta das suas empresas (Nordea, 2018)[3].

* Gabinete de Estratégia e Estudos, gabriel.barros@gee.min-economia.pt

[1] O enquadramento teórico deste documento é feito pelo Tema Económico n.º 54 do Gabinete de Estratégia e Estudos (Barros, 2018).

[2] Este Índice identifica a real penetração das tecnologias digitais em várias economias.

[3] "Cyber risk is clearly a top concern at board level, but boards are not typically well-briefed on this, or confident in their company's ability to withstand a cyberattack. The greatest perceived threat is business disruption by financially driven cybercriminals, rather than the alleged state- sponsored players behind the big global WannaCry and NotPetya cyberattacks in 2017" (Nordea, 2018)

Considerando a relevância do tema, este Tema Económico apresenta uma análise da posição de Portugal na área do Ciberespaço e das políticas públicas implementadas em termos de Cibersegurança, comparando o país com os seus principais parceiros (em especial da União Europeia (UE) e dos países da Organização para a Cooperação e Desenvolvimento Económico (OCDE)), e tem como objectivo despertar uma reflexão sobre políticas públicas que possa ser útil para os decisores políticos.

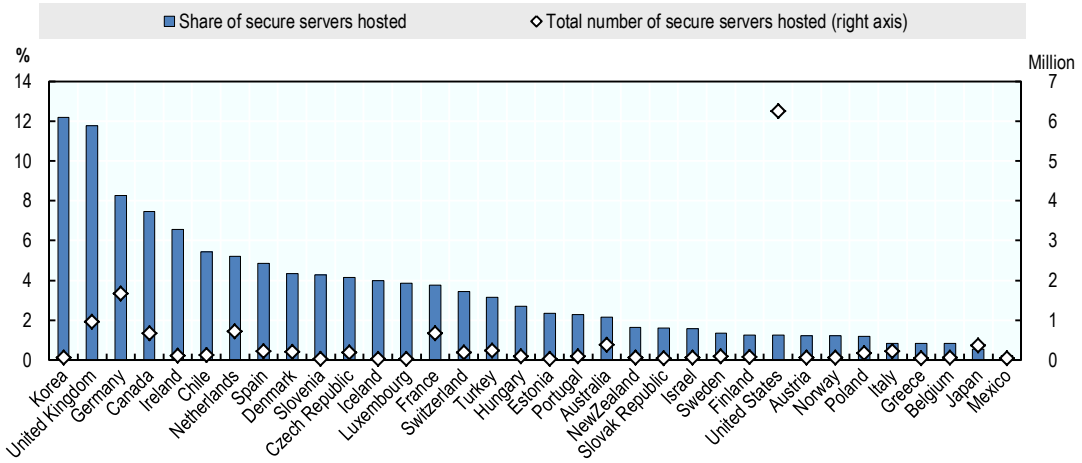
2. Enquadramento

Em Março de 2017, o número de servidores seguros hospedados na OCDE é de aproximadamente 14 milhões, representando, segundo a OCDE, 83% do número total de servidores seguros hospedados em todo o mundo. A instituição refere ainda que dos cerca de 16 milhões de servidores no mundo, apenas 10% possuem um local conhecido.

Os Estados Unidos destacam-se por representarem o maior número de servidores seguros (6,2 milhões), embora, tal como a maioria dos países, representem apenas uma pequena percentagem do total de servidores.

Portugal hospeda 85.095 servidores seguros, o que corresponde a 2,3% do total de servidores hospedados. A média destes indicadores para os 21 países da UE28 considerados é de 261.639 e 3,8%, respectivamente.

Gráfico 1 - Servidores protegidos por país de hospedagem, Março de 2017
(em % do número total de servidores protegidos e em milhões)



Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017b) - http://dx.doi.org/10.1787/888933586616

A utilização de servidores seguros é uma ajuda a prevenir ataques a contas de utilizadores. No entanto, parte da responsabilidade está do lado do utilizador que deve actuar no sentido de evitar ser atacado por *Malware*.

Segundo o *Microsoft Security Intelligence Report* (2017), a taxa de incidência de *Malware*, ou seja, a percentagem de computadores que utilizam software de segurança Microsoft e que detectaram *Malware*, software potencialmente indesejado ou uma ameaça específica durante o primeiro trimestre de 2017 foi de 9,1%.

Portugal encontra-se na 74.ª posição entre os países com maior incidência num conjunto de 109 países. Já quando considerando no conjunto dos 28 países da União Europeia (UE28), Portugal ocupa uma das mais elevadas taxas de incidência de *malware* (9.ª posição).

Tabela 1 - Taxa de incidência de *Malware* (por País)

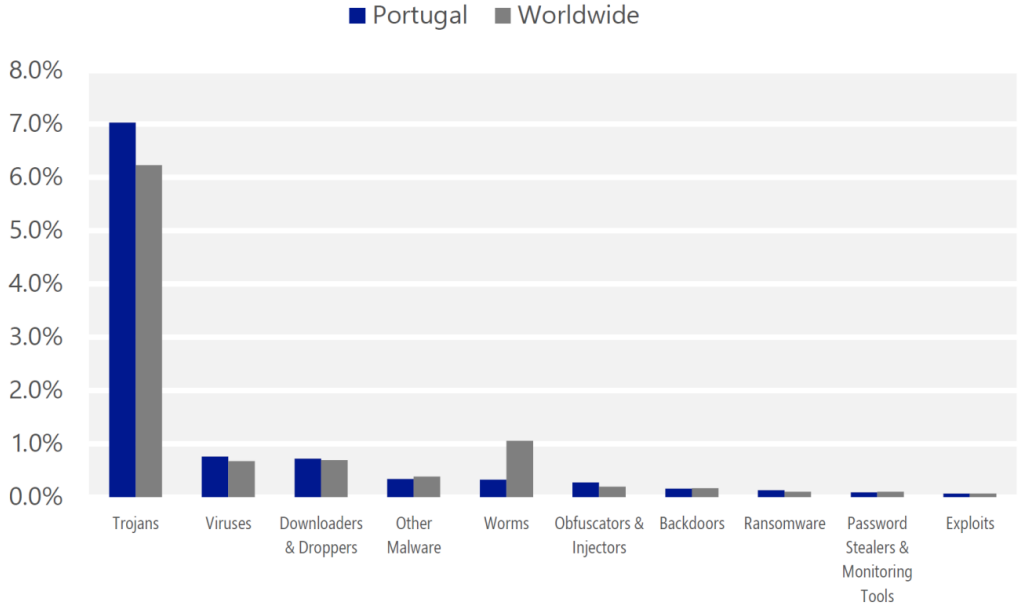
País / Região	2017T1
Worldwide	**9,1%**
Bangladesh	26,9%
Pakistan	26,3%
Cambodia	25,7%
Indonesia	24,5%
Mongolia	24,2%
Egypt	24,0%
Iraq	23,8%
Algeria	23,8%
Myanmar	23,8%
Vietnam	23,2%
Belarus	23,1%
Palestinian Authority	23,0%
Nepal	22,9%
Kazakhstan	21,8%
Tanzania	21,8%
Ukraine	21,6%
Morocco	21,2%
Moldova	21,0%
Thailand	20,2%
Armenia	20,1%
Ghana	20,0%
Côte d'Ivoire	19,9%
Senegal	19,8%
Venezuela	19,7%
Bolivia	19,5%
Tunisia	19,5%
Azerbaijan	19,2%
Philippines	18,9%
Sri Lanka	18,1%
Ecuador	17,9%
Brazil	17,7%
Jordan	17,2%
Peru	17,1%
China	17,1%
Honduras	16,9%
Kenya	16,8%
Bulgaria	16,6%
Macedonia, FYRO	16,3%
Georgia	16,0%
Nigeria	16,0%
Dominican Republic	15,9%
Saudi Arabia	15,7%
Paraguay	15,6%
Serbia	15,6%
Lebanon	15,5%
India	15,3%
Albania	15,3%
Hungary	15,3%
Oman	15,0%
Romania	15,0%
Turkey	15,0%
Bosnia and Herzegovina	14,8%
Russia	14,8%
Colombia	14,5%
El Salvador	14,4%
Guatemala	14,0%
Jamaica	13,1%
Latvia	13,0%
Lithuania	13,0%
Mexico	13,0%
Malaysia	12,9%
Kuwait	12,4%
United Arab Emirates	12,3%
Qatar	12,1%
Croatia	11,9%
Argentina	11,9%
Uruguay	11,3%
Costa Rica	11,2%
Panama	11,1%
Chile	11,0%
Slovenia	10,9%
Spain	10,8%
Taiwan	10,7%
Portugal	10,6%
Trinidad and Tobago	10,5%
Cyprus	10,4%
Greece	9,7%
South Africa	9,6%
Korea	9,3%
Estonia	9,2%
Israel	9,1%
Italy	8,9%
Malta	8,5%
Réunion	8,5%
Slovakia	8,4%
Poland	7,7%
Hong Kong SAR	7,3%
Czech Republic	7,3%
France	7,0%
Singapore	6,8%
Puerto Rico	6,6%
Belgium	5,6%
Netherlands	5,5%
Luxembourg	5,5%
Iceland	5,1%
Austria	4,8%
Canada	4,7%
Australia	4,5%
Germany	4,3%
New Zealand	4,2%
Ireland	4,2%
United Kingdom	3,8%
Denmark	3,7%
Switzerland	3,7%
United States	3,7%
Norway	3,5%
Sweden	3,5%
Finland	2,9%
Japan	2,2%

Fonte: Microsoft Security Intelligence Report (2017)

Segundo a Microsoft (2017), foi encontrado *malware* em 8,3% dos computadores em Portugal, em Março de 2017, valor que compara com uma taxa de incidência mundial de 7,8%.

O *software* malicioso mais comum em Portugal, em Março de 2017, segundo a Microsoft (2017), é os *Trojans*, identificados em mais de 7,0% dos computadores, valor substancialmente superior ao registado na média do conjunto dos países considerados. Seguem-se os Vírus, identificados em 0,8% dos computadores, e os *Downloaders & Droppers*, em 0,7% dos computadores.

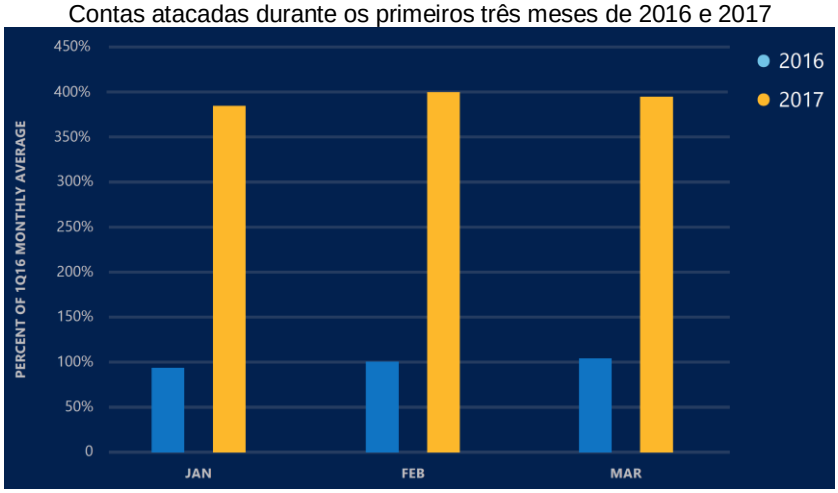
Gráfico 2 – Taxa de incidência de *software* "malicioso"
(em percentagem de todos os computadores considerados), Março de 2017



Fonte: Microsoft Security Intelligence Report (2017)

A *cloud threat intelligence* (ameaça na "nuvem") é outra das mais recentes ameaças à segurança da informação num momento em que a *cloud* se tornou a central de dados da maioria das organizações, tornando-a um alvo em crescimento para ataques. Neste tipo de ameaça, os hackers entram na "nuvem" das organizações através das credenciais de acesso roubadas a um utilizador, em grande parte devido à utilização de *passwords* fracas a que se seguem ataques de *Phishing* direccionados e violações de serviços de terceiros. Segundo a Microsoft (2017), os ataques a contas de utilizadores da nuvem aumentaram 300% no primeiro trimestre de 2017 face ao primeiro trimestre de 2016.

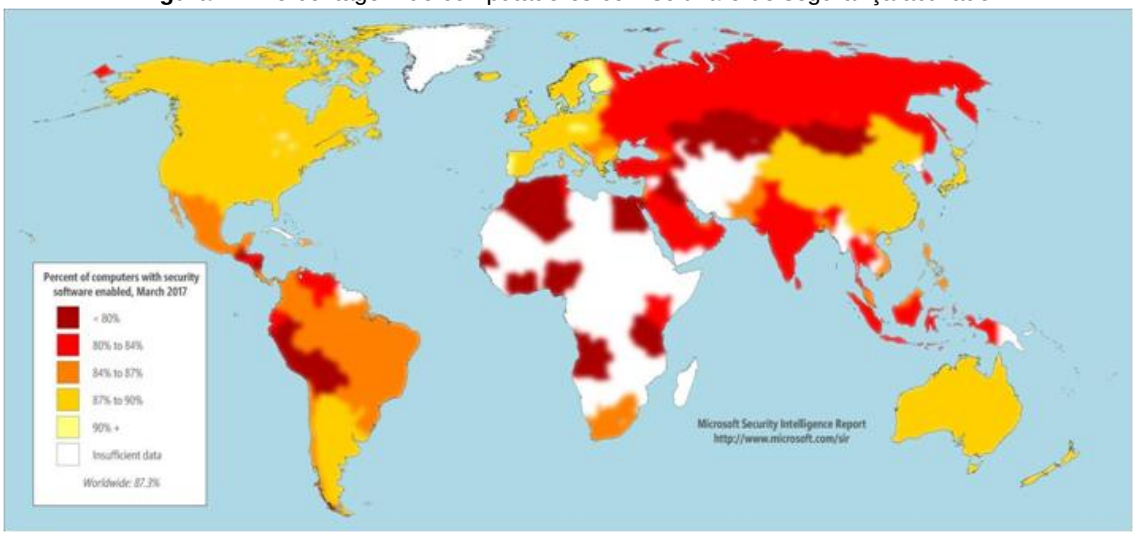
Gráfico 3 - *Cloud threat intelligence*
Contas atacadas durante os primeiros três meses de 2016 e 2017



Fonte: Microsoft Security Intelligence Report (2017)

Ainda assim, convém referir que Portugal regista uma percentagem elevada de computadores com software de segurança activado. A figura seguinte apresenta informação para um conjunto de países sendo que em qualquer deles se verifica que mais de 73% dos computadores se encontravam protegidos em Março de 2017. Os países que apresentam percentagens superiores de computadores protegidos com software de segurança são a Finlândia (92,2%), Portugal (90,3%) e Dinamarca (90,2%). Pelo contrário, os países que apresentam percentagens inferiores são o Peru (78,3%), a Venezuela (80,4%) e a Turquia (80,6%).

Figura 1 – Percentagem de computadores com *software* de segurança activado



Fonte: Microsoft Security Intelligence Report (2017)

Em termos de custos do Cibercrime, segundo o Website Builder Expert (2017), "*it can be next to impossible to quantify the exact cost of cybercrime on a country, so the next best option for us was to look at which populations were the biggest and smallest victims of cybercrime*".

Neste sentido, e segundo os resultados obtidos pelo estudo, Portugal é o o 8.º país da UE com maior risco de Cibercrime e o 3.º maior "EU Country most at risk of Cybercrime" e o 3.º país da UE maior vítima de Cibercrimes.

Tabela 2 - Países da UE em maior risco de cibercrime

EU COUNTRY	CYBERCRIME VULNERABILITY SCORE				
1. MALTA (MOST VULNERABLE)	42%	11. SLOVENIA	38%	21. SWEDEN	32%
2. GREECE	41%	12. CROATIA	37%	22. ITALY	31%
3. ROMANIA	41%	13. DENMARK	36%	23. FRANCE	31%
4. SLOVAKIA	40%	14. LATVIA	35%	24. UK	31%
5. SPAIN	40%	15. CZECH REP	35%	25. NETHERLANDS	30%
6. LITHUANIA	39%	16. POLAND	34%	26. GERMANY	30%
7. CYPRUS	39%	17. IRELAND	33%	27. ESTONIA	30%
8. PORTUGAL	39%	18. LUXEMBOURG	32%	28. FINLAND (LEAST VULNERABLE)	29%
9. HUNGARY	39%	19. AUSTRIA	32%		
10. BULGARIA	38%	20. BELGIUM	32%		

Fonte: Website Builder Expert (2017)

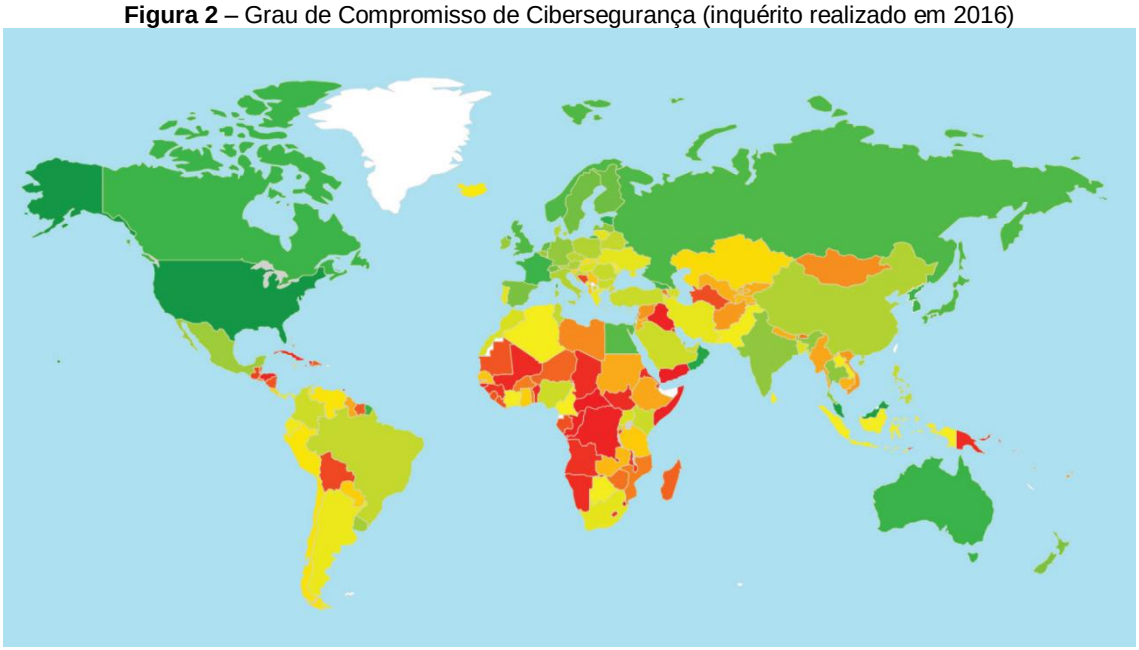
Tabela 3 – Maiores vítimas de crimes cibernéticos entre os países da UE

	% OF POPULATION WHO HAVE EXPERIENCED CYBERCRIME	ANNUAL AVERAGE MALWARE ENCOUNTER RATE	CYBERCRIME VICTIMHOOD RATING
1. ROMANIA	18%	28%	23%
2. NETHERLANDS	27%	14%	21%
3. PORTUGAL	15%	24%	20%
4. POLAND	16%	23%	20%
5. ITALY	17%	21%	19%

Fonte: Website Builder Expert (2017)

Em termos de grau de compromisso com a Cibersegurança, segundo o ITU (2017), Portugal encontra-se classificado no 22.º lugar entre os países da UE28 (62.º lugar entre os 193 países do mundo considerados).

Figura 2 – Grau de Compromisso de Cibersegurança (inquérito realizado em 2016)



Level of commitment: from Green (highest) to Red (lowest)
Fonte: Global Cybersecurity Index 2017 (ITU, 2017)

Segundo a mesma fonte, as áreas críticas em que Portugal se encontra em pior posição em termos de Cibersegurança são as seguintes: (i) formação, (ii) normas para profissionais, (iii) estratégia ao nível das organizações, (iv) definição de métricas, (v) órgãos de definição de padrões, (vi) boas práticas, (vii) programas de I&D na área, (viii) acordos bilaterais, (ix) acordos multilaterais e (x) parcerias público-privadas.

Tabela 4 – Resultados de Portugal no Índice (inquérito realizado em 2016)

	Cybercriminal legislation	Cybersecurity legislation	Cybersecurity training	**LEGAL MEASURES**	National CERT/CIRT/CSIRT	Government CERT/CIRT/CSIRT	Sectoral CERT/CIRT/CSIRT	Standards for organizations	Standards for professionals	Child online protection	**TECHNICAL MEASURES**	Strategy	Responsible agency	Cybersecurity metrics	**ORGANIZATIONAL MEASURES**	Standardization bodies	Cybersecurity good practices	R&D programmes	Public awareness campaigns	Professional training courses	Education programmes	Incentive mechanisms	Home-grown industry	**CAPACITY BUILDING**	Bilateral agreements	Multilateral agreements	International participation	Public-private partnerships	Interagency partnerships	**COOPERATION**	GCI
Portugal																														

Fonte: Global Cybersecurity Index 2017 (ITU, 2017)

Em suma, não obstante Portugal registar uma percentagem elevada de computadores com *software* de segurança activado, o país apresenta uma taxa de incidência de *malware* acima da média e é um dos países da UE com maior risco e maior incidência de Cibercrime. Por si só, esta situação justifica uma análise mais detalhada.

3. A utilização de TIC e a Cibersegurança em Portugal

No presente capítulo, iremos analisar os principais indicadores que permitem avaliar Portugal quanto à utilização das TIC, ao Comércio Electrónico e à Cibersegurança, quer em relação aos cidadãos que em relação às empresas.

3.1. Os Cidadãos

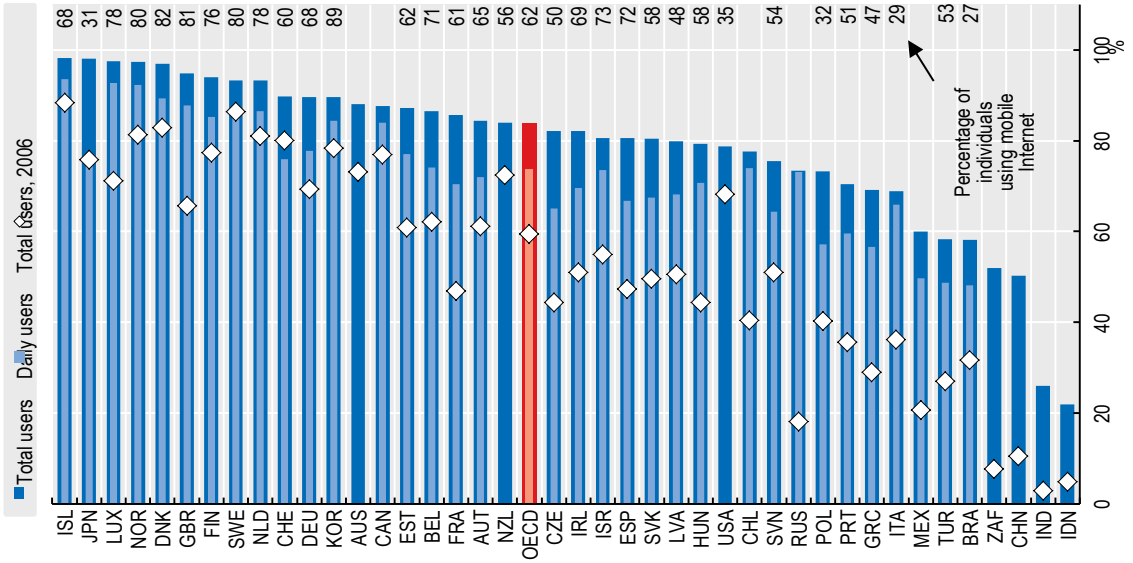
3.1.1. A utilização das TIC

Sendo a internet uma ferramenta cada vez mais comum no dia-a-dia das pessoas, verifica-se que as taxas de utilização nos países da OCDE aumentaram em média 24,4 p.p. entre 2006 (59,4%) e 2016 (83,8%). Portugal encontra-se abaixo da média da OCDE (70,4 p.p.), embora tenha registado um dos maiores aumentos desde 2006 (34,8 p.p.).

Em termos de utilizadores diários de internet, Portugal regista um dos piores resultados (59,5%) comparativamente com os países para os quais a informação se encontra disponível, abaixo da média da OCDE (73,7%) e apenas acima do Brasil (48,1%), Turquia (48,7%), México (49,7%), Grécia (56,7%) e Polónia (57,2%).

Apenas 51% das pessoas utilizam internet móvel através, por exemplo, de telemóveis/*smartphones*, abaixo da média da OCDE (62%) e, em especial, dos países que lideram a lista: Coreia (89%), Dinamarca (82%), Reino Unido (81%), Noruega (80%) e Suécia (80%).

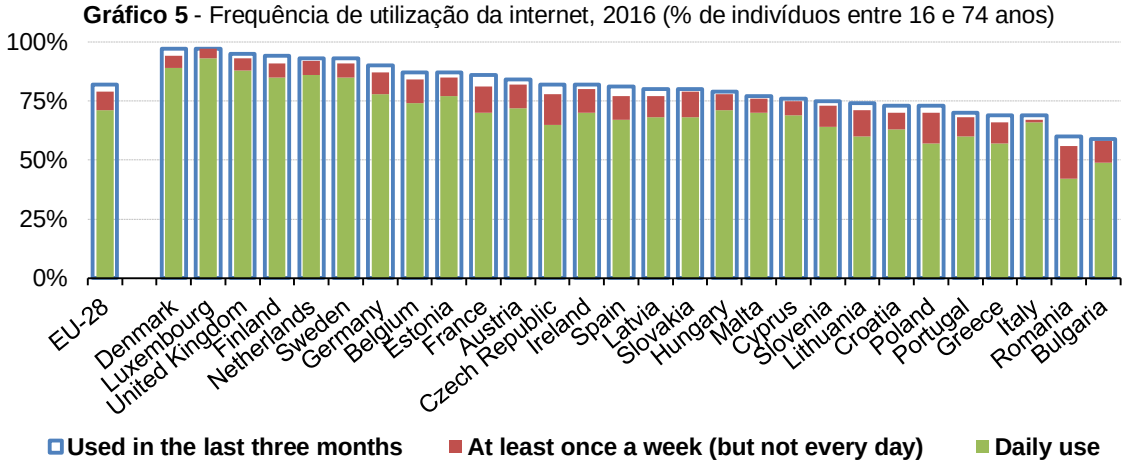
Gráfico 4 - Usuários de Internet (total, diários e móveis), 2016 (% de população de 16 a 74 anos)



Fonte: OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation (OCDE, 2017a) - http://dx.doi.org/10.1787/888933620037

Também quando comparando com a UE28 Portugal regista um dos valores mais baixos no que respeita à frequência de utilização de internet por pessoas entre os 16 e os 74 anos nos últimos 3 meses, muito abaixo da média (82%) e apenas à frente de 4 países (Grécia e Itália, ambos com 69%, Roménia com 60% e Bulgária com 59%). Destas pessoas, cerca de 86% utiliza a internet diariamente, representando, como tínhamos visto no gráfico anterior, 60% das pessoas entre os 16 e os 74 anos (71% no caso da UE28).

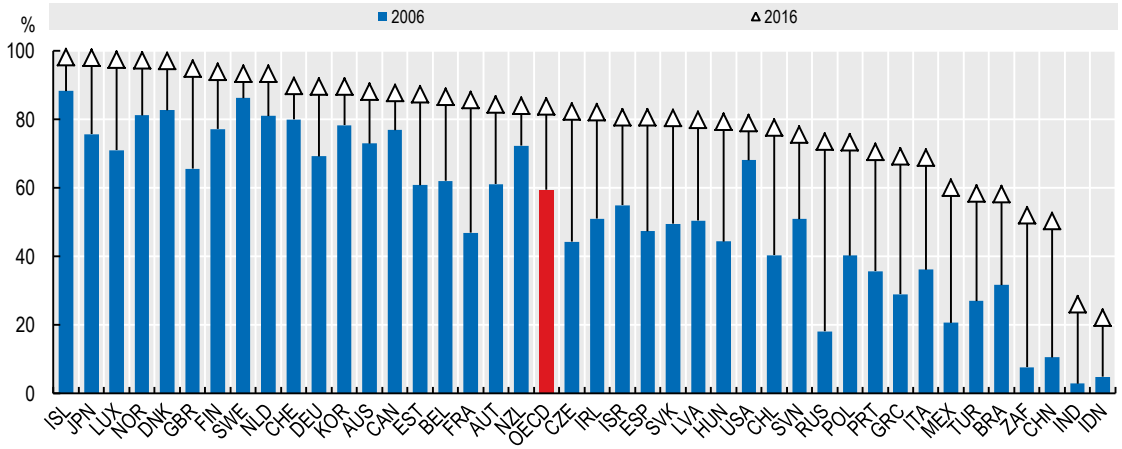
Gráfico 5 - Frequência de utilização da internet, 2016 (% de indivíduos entre 16 e 74 anos)



Fonte: Eurostat (online data codes: isoc_ci_ifp_iu and isoc_ci_ifp_fu)

Apesar da evolução positiva registada, Portugal apresenta ainda um atraso na percentagem de utilizadores de internet. Dos 22 países da UE28 considerados no gráfico seguinte, Portugal foi o segundo em que a percentagem de utilizadores de internet mais aumentou de 2006 para 2016 (98%), apenas ultrapassado peça Grécia (139%). Embora a percentagem de utilizadores tenha aumentado de 35,6% para 70,4%, Portugal encontra-se abaixo da média da OCDE (83,8%).

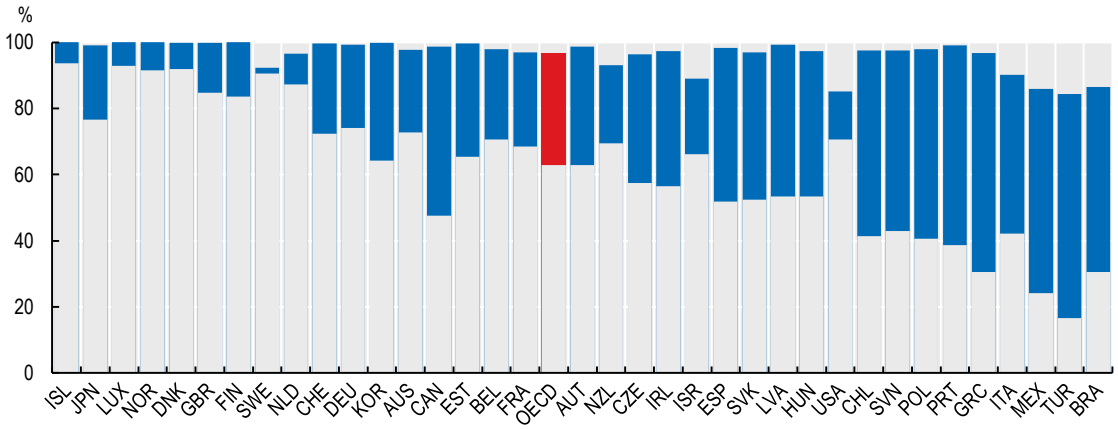
Gráfico 6 - Diferença na percentagem de utilizadores de internet entre 2006 e 2016



Fonte: OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation (OCDE, 2017a) - http://dx.doi.org/10.1787/888933617928

No mesmo grupo de países, Portugal apresenta o segundo maior gap entre a percentagem de utilizadores com idade entre os 16 e os 24 anos e a percentagem de utilizadores com idade entre os 55 e os 74 anos (60,6 p.p.). A Grécia apresenta o maior gap (66,3 p.p.). Ainda assim, a população mais jovem (dos 16 aos 24 anos) apresenta uma percentagem de utilizadores muito elevada (99,1%), acima da média da OCDE (96,5%). Desta forma, podemos verificar que, a manter-se esta tendência, Portugal deverá evoluir de forma muito positiva a este nível.

Gráfico 7 – Gap percentual entre utilizadores de internet nas faixas etárias dos 16 aos 24 anos e dos 55 aos 74 anos (2016)



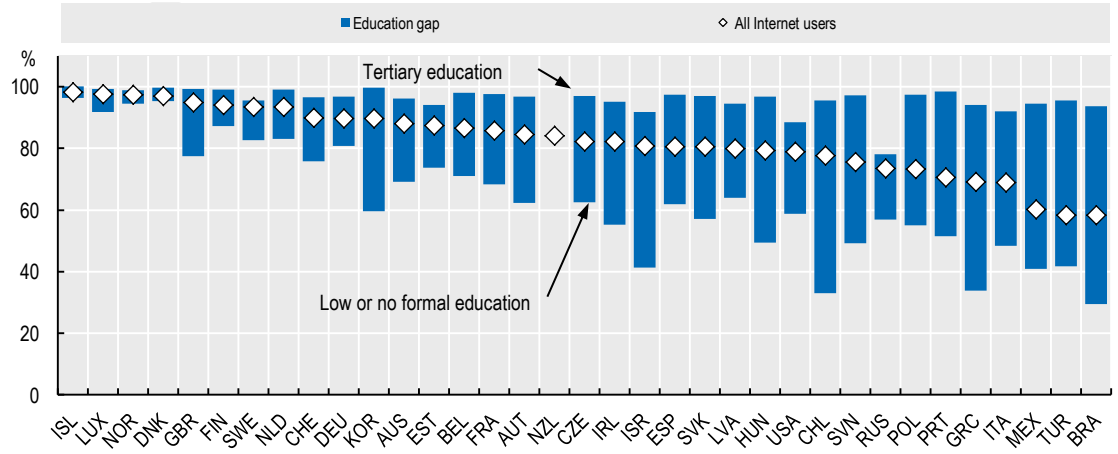
Fonte: OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation (OCDE, 2017a) - http://dx.doi.org/10.1787/888933617947

A adesão à internet está intimamente ligada ao nível de educação dos cidadãos. Em Portugal, tal como na maioria dos países da OCDE (com excepção dos Estados Unidos da América), a proporção de utilizadores de Internet com educação superior é superior a 90% (98,4%) em 2016, sendo o 9.º país entre os considerados no gráfico seguinte e o 6.º da UE entre 22 países para os quais existe informação (atrás da Dinamarca, Luxemburgo, Reino Unido, Finlândia e Holanda).

No entanto, Portugal apresenta uma grande diferença neste indicador quando considerando os cidadãos com menos instrução, sendo a percentagem de utilizadores da Internet entre indivíduos com pouca ou nenhuma escolaridade de 51,5%. Desta forma, o país obtém o 5.º pior resultado entre os 22 países da UE considerados (apenas à frente da Hungria, Eslovénia, Itália e Grécia), sendo um dos países em que a diferença na adesão à Internet entre pessoas com alta e baixa escolaridade é maior, atingindo os 46,9 p.p..

Tal como constata a OCDE, face a estes resultados, verifica-se que as pessoas com baixa escolaridade são um foco potencial para estratégias de promoção da inclusão digital. Por outro lado, o cada vez maior nível educacional registado em Portugal permite antecipar uma diminuição deste gap no futuro.

Gráfico 8 – *Gap* no uso da Internet por nível educacional, 2016 (% da população em cada categoria)

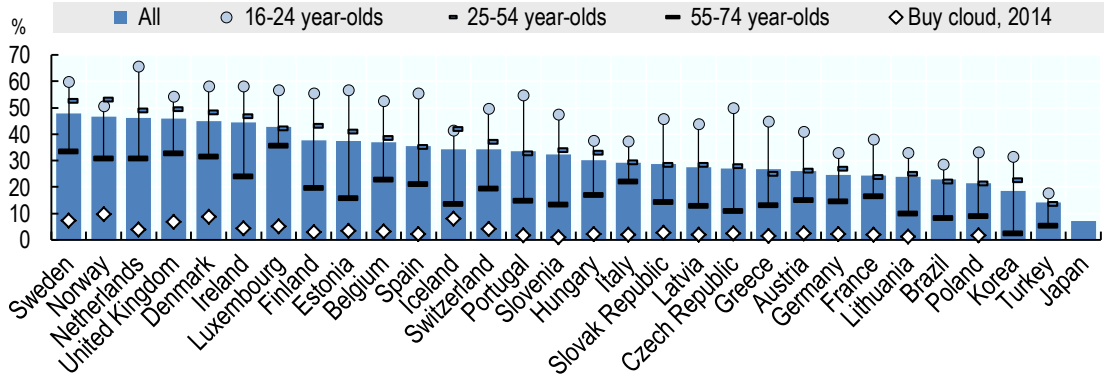


Fonte: OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation (OCDE, 2017a) - http://dx.doi.org/10.1787/888933620056

À semelhante da generalidade dos países, Portugal registou um aumento significativo na utilização de serviços de *cloud computing*[4] por utilizadores da internet (31,8p.p. entre 2014 e 2016). Apesar daquele aumento, em 2016, o *cloud computing* em Portugal foi utilizado por apenas 33,5% dos utilizadores de internet, atrás de países da UE28 como a Suécia (47,8%), a Holanda (46,1%), o Reino Unido (45,8%), a Bélgica (36,9%) ou Espanha (35,5%).

Entre os utilizadores destacaram-se os do grupo etário entre os 16 e os 24 anos de idade (54,6%), sendo esta a faixa etária em que Portugal fica melhor posicionado na comparação com os outros países seleccionados.

Gráfico 9 – Uso de *cloud computing* por indivíduos em países seleccionados da OCDE, por faixa etária, 2016 (% de usuários da Internet)

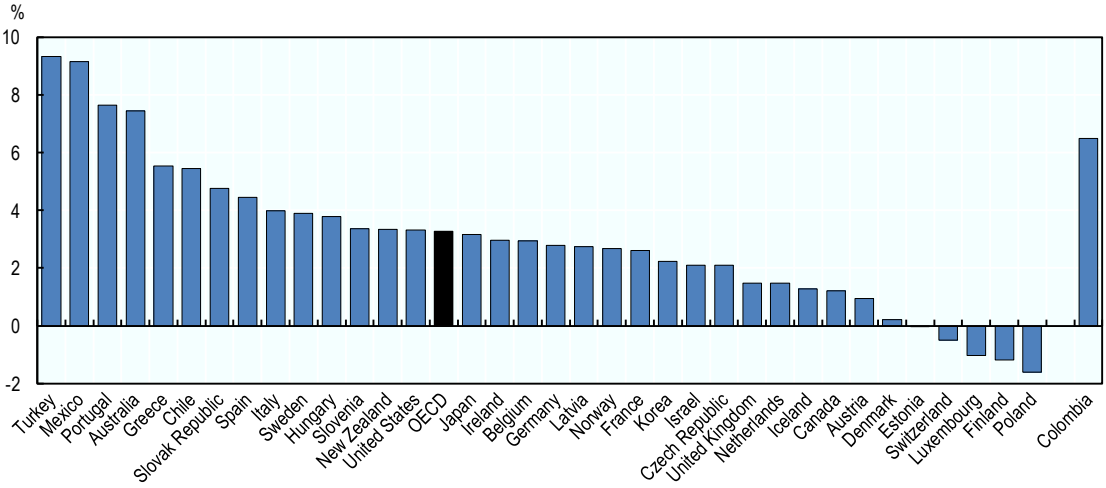


Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017b) - http://dx.doi.org/10.1787/888933585647

As ligações de banda larga permitem identificar o nível de acesso das famílias a serviços e à informação.

O número de assinaturas de banda larga fixa aumentou em quase todos os países da OCDE, tendo em média aumentado 3,28% entre Dezembro de 2015 e Dezembro de 2016. Portugal apresenta o 3.º maior aumento (7,64%), apenas atrás da Turquia e do México.

Gráfico 10 – Assinaturas de banda larga fixa por 100 habitantes (aumento percentual, Dezembro de 2015 a Dezembro de 2016)



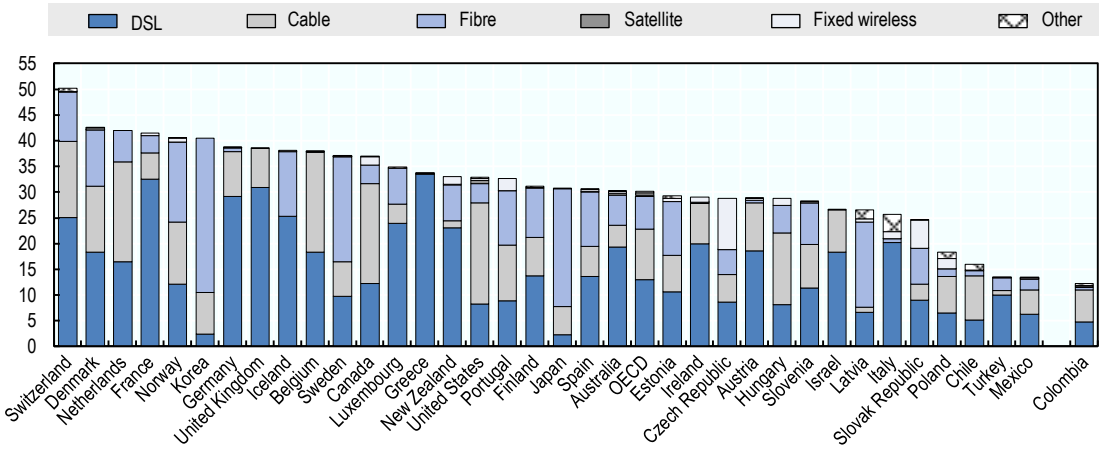
Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017b) - http://dx.doi.org/10.1787/888933585210

[4] O chamado *cloud computing* é um espaço de armazenamento virtual que permite a gravação de diverso tipo de ficheiros e de *software* e a sua partilha com outros utilizadores.

Ao contrário da Turquia e do México, Portugal não apresenta um nível tão reduzido em termos de taxa de penetração, segundo os valores registados em Dezembro de 2016. Neste aspecto, Portugal regista uma taxa de penetração de 32,7%, acima da média da OCDE (30,1%). Portugal, encontra-se, assim, na 10.ª posição entre os 22 países da UE28 pertencentes à OCDE. Desagregando aquele valor, verifica-se uma maior incidência da banda larga por cabo (10,8 p.p.) e por fibra (10,5 p.p.).

Também a este nível, podemos registar uma evolução positiva do acesso à banda larga pelos cidadãos em Portugal.

Gráfico 11 – Assinaturas de banda larga fixa por 100 habitantes
(por tecnologia, Dezembro de 2016)

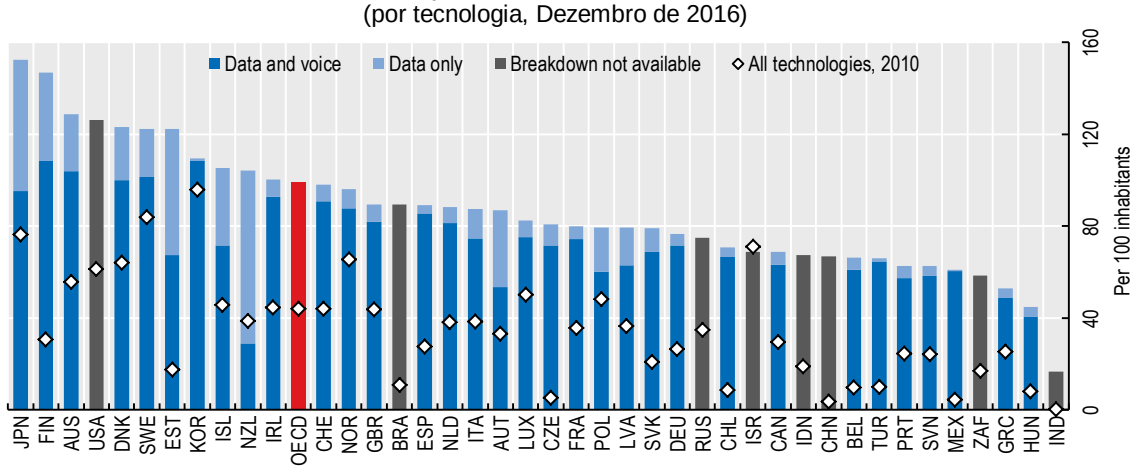


Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017b) - http://dx.doi.org/10.1787/888933585191

Já no que diz respeito ao acesso móvel, considerando informação do referido mês, a penetração da banda larga móvel na área da OCDE encontra-se em 99,25% (quase uma assinatura de banda larga móvel por habitante). Portugal regista um dos valores mais reduzidos (62,7%), apenas à frente de 3 países da UE28 que fazem parte da OCDE (Eslovénia, Grécia e Hungria), sendo a maior parte das subscrições de dados e voz (57,3 p.p.).

Apesar de Portugal ainda apresentar um atraso nesta área, há que salientar a evolução positiva registada. De facto, a taxa de penetração na banda larga móvel aumentou 158% entre 2010 (24,3%) e 2016 (62,7%), acima da média da OCDE (126%).

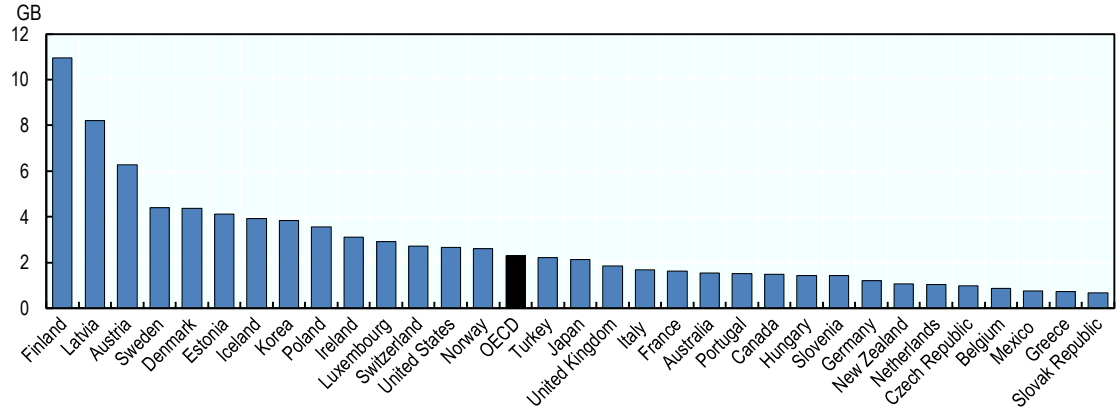
Gráfico 12 – Penetração da banda larga móvel por 100 habitantes
(por tecnologia, Dezembro de 2016)



Fonte: OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation (OCDE, 2017a) - http://dx.doi.org/10.1787/888933619923

A quantidade de tráfego que os cidadãos utilizam é também um factor importante quando avaliamos o seu acesso à internet. Em termos de volume de dados utilizados, a OCDE refere uma tendência para aumento dos plafonds de dados incluídos nos tarifários e o consequente aumento de utilização de dados. Portugal regista uma média de 1,52 GB por mês por subscrição de banda larga, um valor reduzido e que se situa abaixo da média da OCDE (2,30 GB) mas, ainda assim, acima de países como a Alemanha (1,21 GB) ou a Bélgica (0,86 GB).

Gráfico 13 – Uso de dados móveis por assinatura de banda larga móvel, 2016
(Gigabytes por mês)

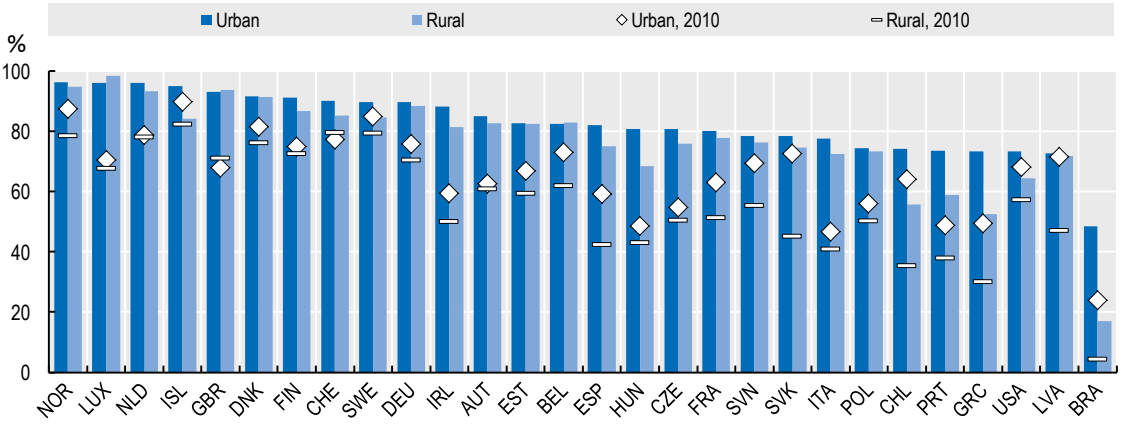


Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017b) - http://dx.doi.org/10.1787/888933585343

Ainda ao nível das ligações de banda larga, registam-se disparidades no acesso entre zonas rurais e urbanas. Portugal apresenta um dos maiores hiatos (14,6 p.p.), a seguir ao Brasil (31,5 p.p.), Grécia (20,9 p.p.) e Chile (18,6 p.p.).

Portugal é, igualmente, o 4.º país em que o *gap* mais aumentou desde 2010, em resultado de um maior aumento registado nas zonas urbanas. Ainda assim, a percentagem de família com ligações de banda larga (fixa e móvel) é das mais reduzidas da OCDE (em particular no que respeita à móvel) - 5.º pior em termos de zonas urbanas (73,5 p.p.) e 4.º pior em termos de zonas rurais (58,8 p.p.).

Gráfico 14 – Agregados familiares com ligações de banda larga, urbanos e rurais, 2010 e 2016
(% de agregados familiares em cada categoria)



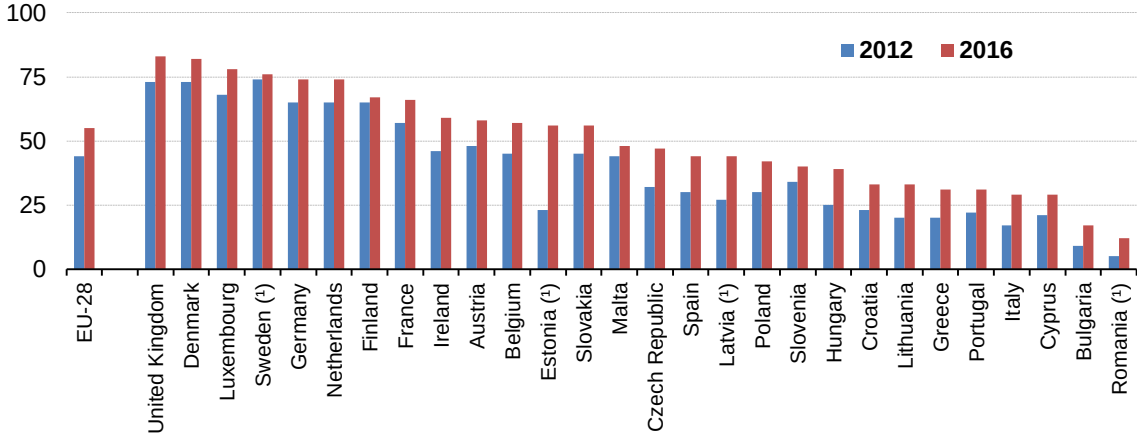
Fonte: OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation (OCDE, 2017a) - http://dx.doi.org/10.1787/888933619942

3.1.2. O Comércio Electrónico

Entraremos agora no subcapítulo em que faremos referência ao ponto de situação das principais questões ligadas ao comércio electrónico por parte dos cidadãos.

Em Portugal, em 2016, apenas 31% das pessoas com idade entre os 16 e os 74 anos encomendaram bens ou serviços pela internet para uso privado nos 12 meses anteriores ao inquérito (55% na média da UE28). Entre 2012 e 2016, aquela percentagem apenas aumentou 9,0 p.p. (11,0 p.p. na média da UE28), tendo o país passado da 22.ª para a 24.ª posição a este respeito.

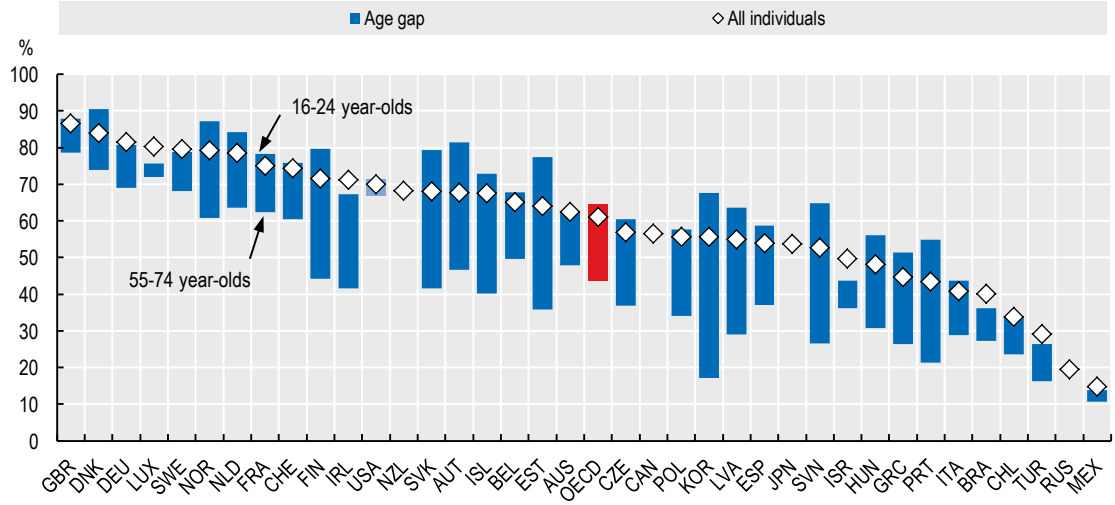
Gráfico 15 – Indivíduos que encomendaram bens ou serviços pela internet para uso privado nos 12 meses anteriores ao inquérito, 2012 e 2016 (% de indivíduos entre 16 e 74 anos)



(1) Break in series
Fonte: Eurostat (online data code: isoc_ec_ibuy)

Dos utilizadores de internet, 61,1% adquiriram *online* nos 12 meses anteriores ao inquérito, novamente destacando-se o peso da faixa etária entre os 16 e os 24 anos (54,9%). Entre os países da OCDE seleccionados, Portugal é um dos piores classificados, encontrando-se muito abaixo da média dos países (61,1%), numa lista liderada pelo Reino Unido (86,5%), Dinamarca (83,9%) e Alemanha (81,5%). Ainda assim, o país progrediu positivamente face a 2010 (mais 16,0 p.p.).

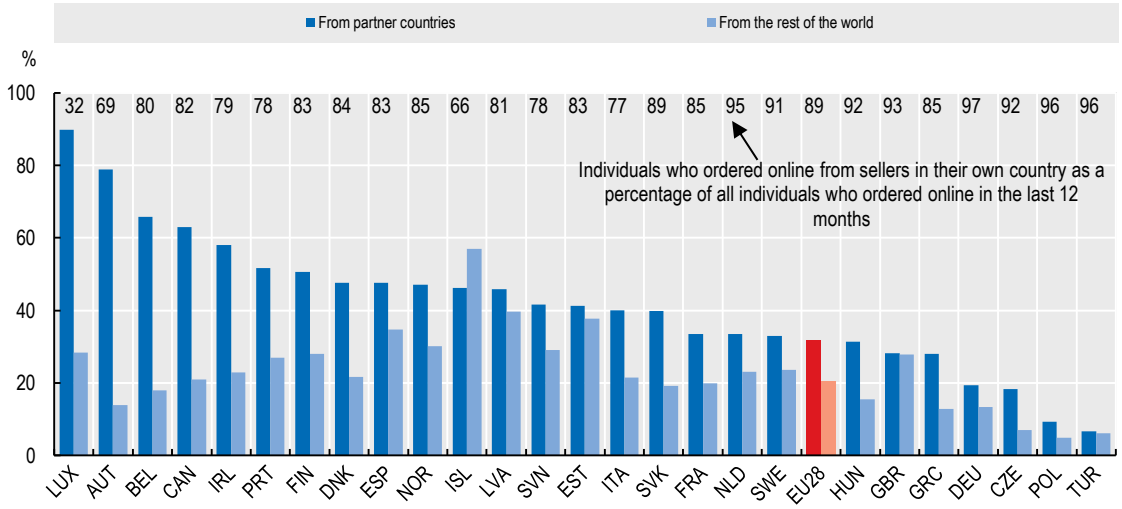
Gráfico 16 – Indivíduos que compraram *online* nos últimos 12 meses, por idade, 2016 (% de usuários da Internet em cada faixa etária)



Fonte: OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation (OCDE, 2017a) - http://dx.doi.org/10.1787/888933620113

Os consumidores portugueses preferem fazer compras *online* a vendedores nacionais em vez de adquirirem a vendedores estrangeiros. De facto, em 2016, 78,4% das pessoas que compraram *online* nos últimos 12 meses fizeram-no vendedores portugueses (89,1% na média da UE28).No mesmo ano, 52% dos compradores portugueses *online* encomendaram a um vendedor localizado num país parceiro, encontrando-se o país na 5.ª posição face aos países da UE28. Apenas 27% dos compradores *online* adquiriram a vendedores do resto do mundo.

Gráfico 17 – Indivíduos que compraram *online* no mercado interno e externo, 2016
(% de indivíduos que encomendaram produtos ou serviços pela Internet nos últimos 12 meses)



Fonte: OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation (OCDE, 2017a) - http://dx.doi.org/10.1787/888933620170

3.1.3. A Cibersegurança

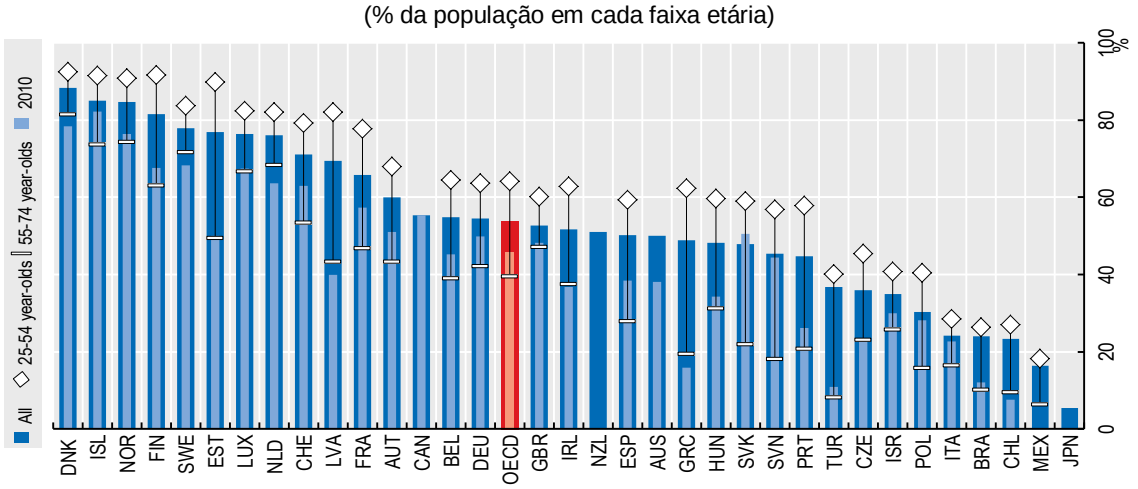
Nesta presente subsecção abordaremos as questões da Cibersegurança que se colocam aos cidadãos, nomeadamente no momento de decidir a forma de lidar com organismos públicos ou de definir o tipo de informação que estão dispostos a disponibilizar *online*.

Em Portugal, a percentagem de pessoas entre os 16 e os 74 anos que utilizam a Internet para interagir com as autoridades públicas foi de 44,7% em 2016, abaixo da média dos países da OCDE (53,8%). Segundo a OCDE (2017a), para a diferença registada entre os vários países contribuem, entre outros factores, a diferença na percentagem de utilizadores de internet e a disponibilidade de serviços de *e-government*.

Não obstante, Portugal registou um aumento significativo entre 2010 e 2016, sendo o 5.º país da OCDE com maior aumento (18,6 p.p.) entre os países para os quais existe informação disponível, apenas atrás da Grécia (33,1%), Letónia (29,5%), Estónia (26,9%) e Turquia (25,9%).

Em Portugal, aquela utilização destaca-se no grupo etário dos 25 aos 54 anos (57,7%), seguido do grupo etário entre os 16 e os 24 anos (48,4%) e, no final, o grupo etário dos 55 aos 74 anos (20,6%). Em qualquer dos casos, este último grupo encontra-se sempre abaixo da média.

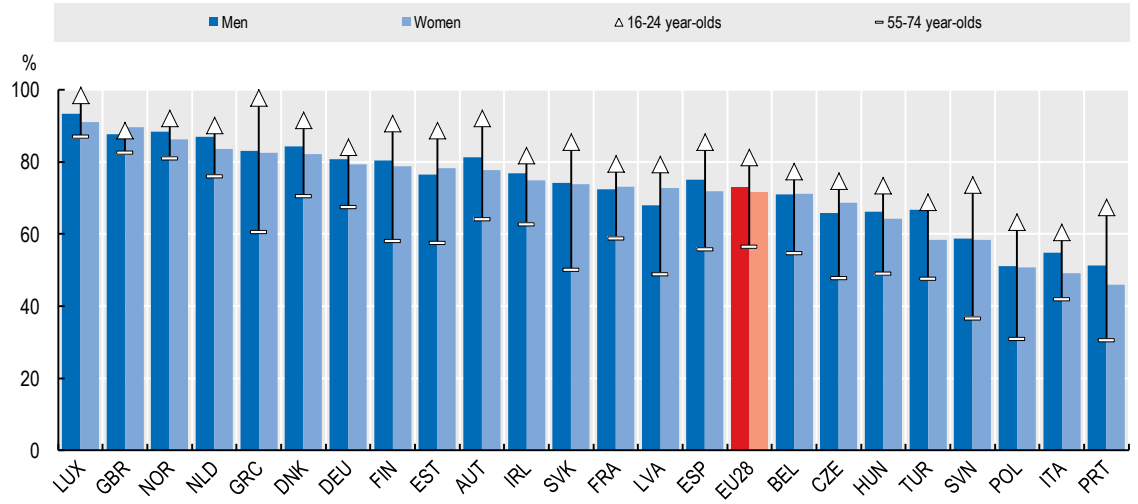
Gráfico 18 – Indivíduos que usam a Internet para interagir com autoridades públicas, por idade, 2016 (% da população em cada faixa etária)



Fonte: OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation (OCDE, 2017a) - http://dx.doi.org/10.1787/888933620208

Em 2016, apenas 51,3% dos homens e 45,9% das mulheres utilizadores de internet em Portugal forneceram algum tipo de informação pessoal *online* nos últimos 12 meses, sendo o pior resultado entre os países da UE28 com um valor muito abaixo da média (72,9% e 71,6%, respectivamente). Para este resultado contribui particularmente o grupo etário entre os 55 e os 74 anos em que apenas 30% forneceram informação *online*.

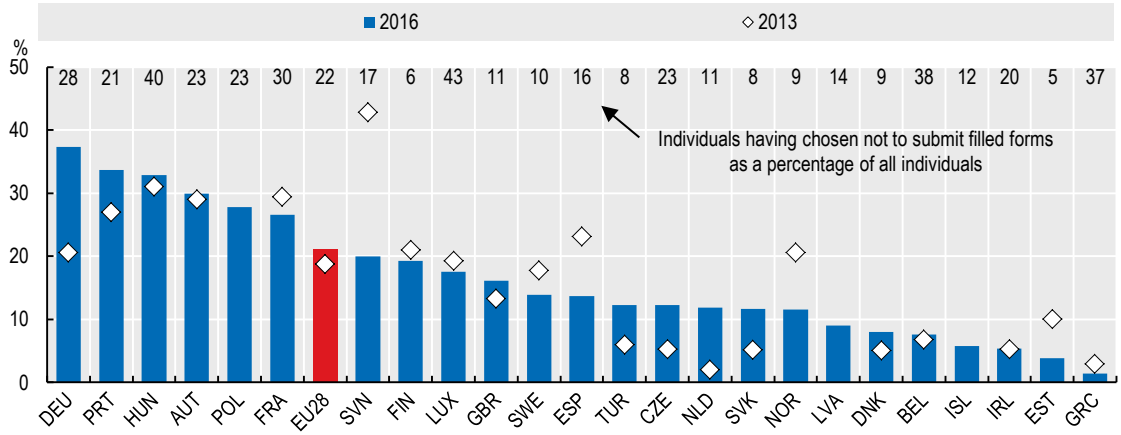
Gráfico 19 – Indivíduos que forneceram informações pessoais pela Internet nos últimos 12 meses, por sexo e idade, 2016 (% de usuários da Internet em cada grupo)



Fonte: OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation (OCDE, 2017a) - http://dx.doi.org/10.1787/888933620284

Um motivo frequentemente referido para o não envio de formulários oficiais *online* são as preocupações com a protecção e a segurança dos dados pessoais, sendo Portugal o 2.º país, em 2016, em que uma percentagem maior de pessoas refere essa justificação (33,7%), apenas atrás da Alemanha (37,4%) e acima da média da UE28 (21,1%).

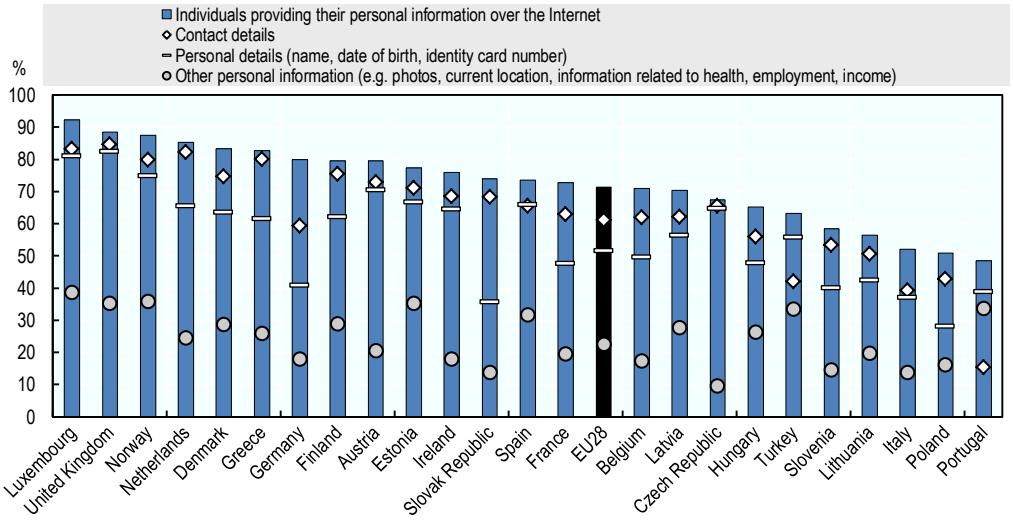
Gráfico 20 – Indivíduos que não submeteram formulários oficiais *online* devido a preocupações com privacidade e segurança, 2016 (% de indivíduos que optaram por não enviar *online*)



Fonte: OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation (OCDE, 2017a) - http://dx.doi.org/10.1787/888933620227

Portugal é o país em que os cidadãos menos fornecem os seus dados pessoais e a sua informação de contacto pela internet (48,6% e 15,2%, respectivamente, que compara com 71,4% e 61,1% na UE28). No que diz respeito às pessoas que fornecem detalhes pessoais (nome, data de nascimento, número do documento de identidade), Portugal ocupa a 21.ª posição em 24 países da UE28 (com 38,8%, o que compara com 51,6% na UE28). Em sentido inverso, Portugal destaca-se na percentagem de pessoas que forneceram na internet outras informações pessoais tais como fotografias, dados de localização e informações sobre sua saúde e rendimento, a qual atinge os 33,5% (22,4% na UE28), colocando Portugal na 5.ª posição entre 24 países da UE28.

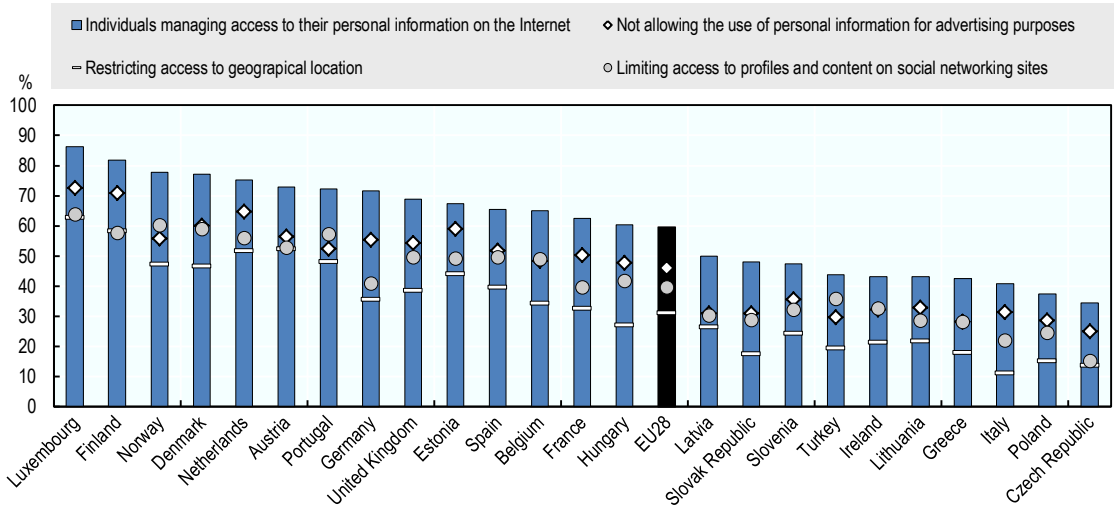
Gráfico 21 – Indivíduos que fornecem informações pessoais pela Internet, 2016 (% de indivíduos que usaram a Internet durante o último ano)



Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017b) - http://dx.doi.org/10.1787/888933586502

Em Portugal, 72,3% das pessoas que utilizam internet controlam o acesso à sua informação pessoal, acima da média dos países referidos (59,5%). Esse controlo passa por limitar o acesso aos perfis e conteúdos nas redes sociais (57,2%), impedindo a utilização para efeitos de publicidade (52,2%) e/ou restringir o acesso à informação da localização geográfica (48,0%) – respectivamente 39,5%, 46,0% e 31,1% na média dos países da UE28.

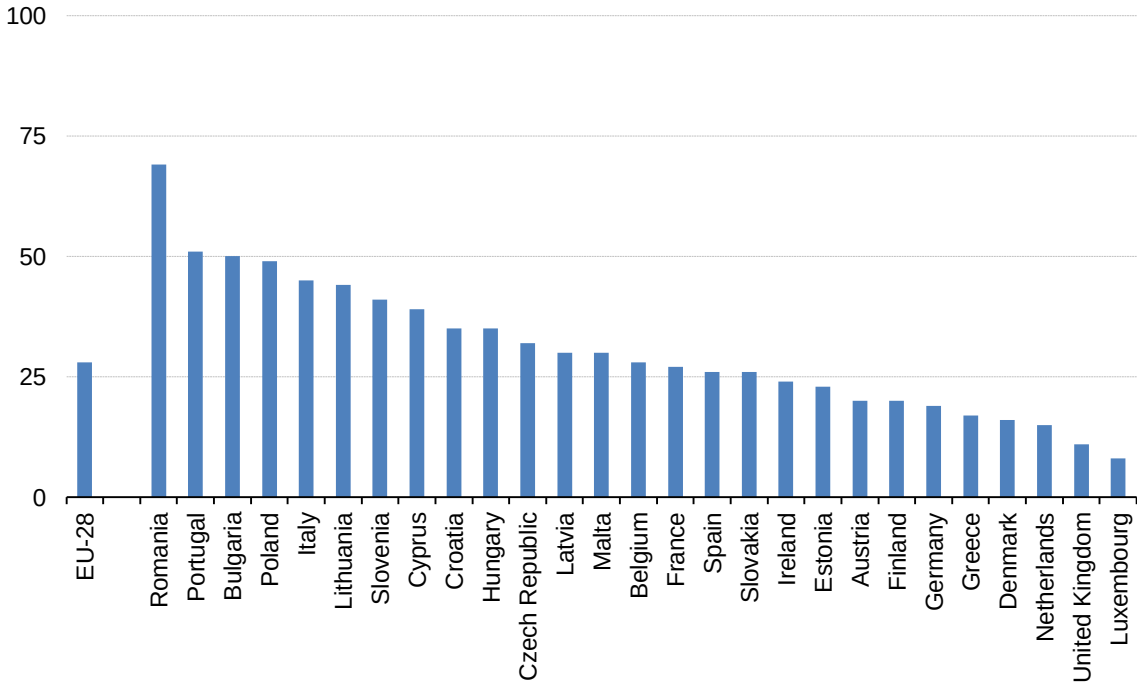
Gráfica 22 – Indivíduos que geriram o uso das suas informações pessoais pela Internet, 2016 (% de indivíduos que usaram a Internet no último ano)



Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017b) - http://dx.doi.org/10.1787/888933586578

Em 2016, Portugal foi o segundo país (a seguir à Roménia) em que mais pessoas (que utilizaram a internet nos 12 meses anteriores ao inquérito) se recusaram a facultar informações pessoais através da internet (51%), muito acima da média da UE28 (28%). Este valor varia entre 8% no Luxemburgo e 69% na Roménia.

Gráfico 23 – Proporção de indivíduos que não forneceram nenhuma informação pessoal na Internet, 2016 (% de pessoas que usaram internet no último ano)

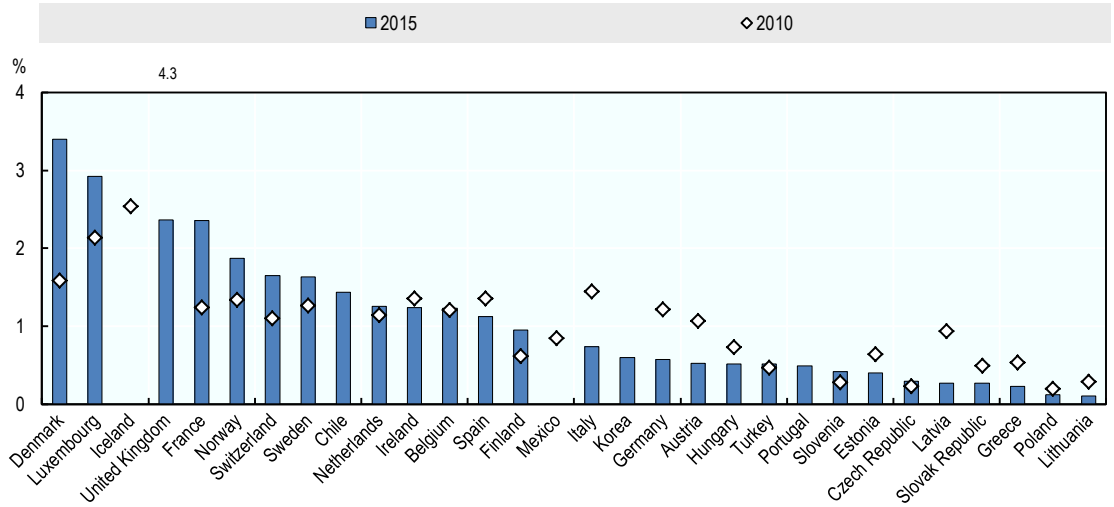


Fonte: Eurostat (online data code: isoc_cisci_prv)

No que se refere a indivíduos que sofreram perdas financeiras devido a pagamentos *online* fraudulentos, verifica-se que não existem valores disponíveis para Portugal para 2010. Relativamente a 2015, verifica-se que 0,49% dos portugueses sofreram perdas devido a pagamentos fraudulentos *online*, ocupando a 20ª posição entre os 28 países para os quais esta informação se encontra disponível.

O facto de em Portugal haver um menor número de pessoas afectadas por este tipo de fraude está associado ao menor número de utilizadores.

Gráfico 24 – Indivíduos que sofreram perdas financeiras devido a pagamentos *online* fraudulentos nos últimos três meses (% de todos os indivíduos)

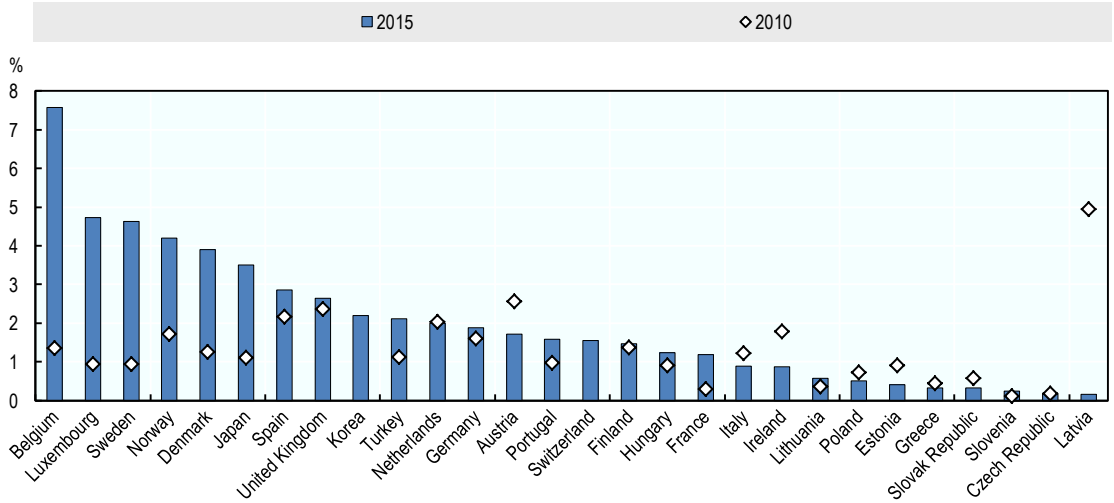


Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017b) - http://dx.doi.org/10.1787/888933586540

Relativamente a perdas em consequência de *phising*/*pharming*, a percentagem de pessoas afectadas em Portugal aumentou 63% entre 2010 (0,97%) e 2015 (1,58%). Esta evolução segue a tendência da maioria dos países referidos no gráfico seguinte, com destaque para o crescimento deste fenómeno verificado na Bélgica (458%), Luxemburgo (404%) e Suécia (391%). Em sentido contrário, destacam-se a Letónia (-97%), a Estónia (-55%) e a Irlanda (-50%).

Novamente, a relativamente baixa percentagem de pessoas atingidas em Portugal deve-se à ainda reduzida utilização das TIC por uma percentagem significativa da população.

Gráfico 25 – Indivíduos que sofreram uma perda financeira de *phishing*/*pharming* nos últimos três meses (% de todos os indivíduos)



Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017b) - http://dx.doi.org/10.1787/888933586559

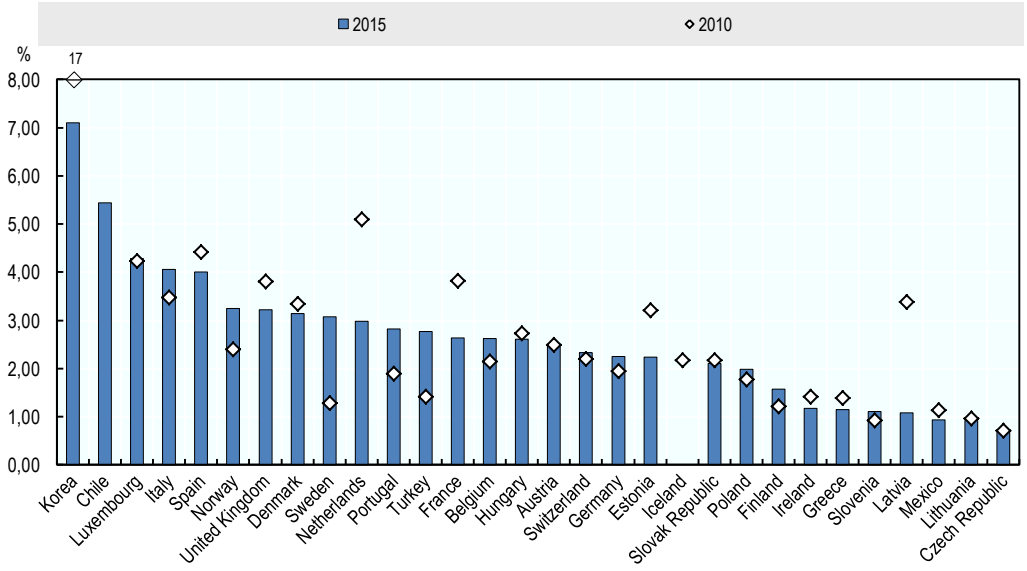
Outra preocupação relevante prende-se com o tratamento de grandes quantidades de informação pessoal, nomeadamente através de "*data mining*", o que pode pôr em risco a privacidade.

Em Portugal, em 2015, cerca de 2,8% das pessoas relataram ter sofrido uma violação de privacidade[5] nos últimos três meses. Portugal foi o 2.º país da UE28 em que este valor mais aumentou entre 2010 e 2015 (49%), logo a seguir à Suécia (139%). Entre os países da UE28 em que mais diminuiu encontram-se a Letónia (-68%) e a Holanda (-42%).

Em comparação com os 30 países da OCDE para os quais é fornecida esta informação, Portugal ocupava a 11.ª posição em 2015, piorando significativamente face a 2010 (19.ª posição) em termos de percentagem de indivíduos que sofreram violações de privacidade[6]. Face aos 23 países da UE28 considerados, Portugal ocupava o 8.º lugar em 2015 depois de ocupar o 15.º lugar em 2010.

Para esta evolução, é importante referir a cada vez maior disponibilização de dados que é realizada hoje em dia em diversas situações, razão pela é particularmente relevante o Regulamento Geral de Protecção de Dados que recentemente entrou em vigor.

Gráfico 26 – Indivíduos que sofreram violações de privacidade nos últimos três meses
(% de todos os indivíduos)



Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017b) - http://dx.doi.org/10.1787/888933586483

Em Portugal, em 2016, 55,7% das pessoas estavam preocupados com o registo das suas actividades *online* com o objectivo de realizar publicidade direccionada (61,1% na média dos países da UE28). Entre as pessoas que referiram estar preocupadas, a maioria refere estar "muito preocupada" (24,9%, o 3.º maior entre os 19 países da UE28 considerados) e "um pouco preocupada" (30,8%).

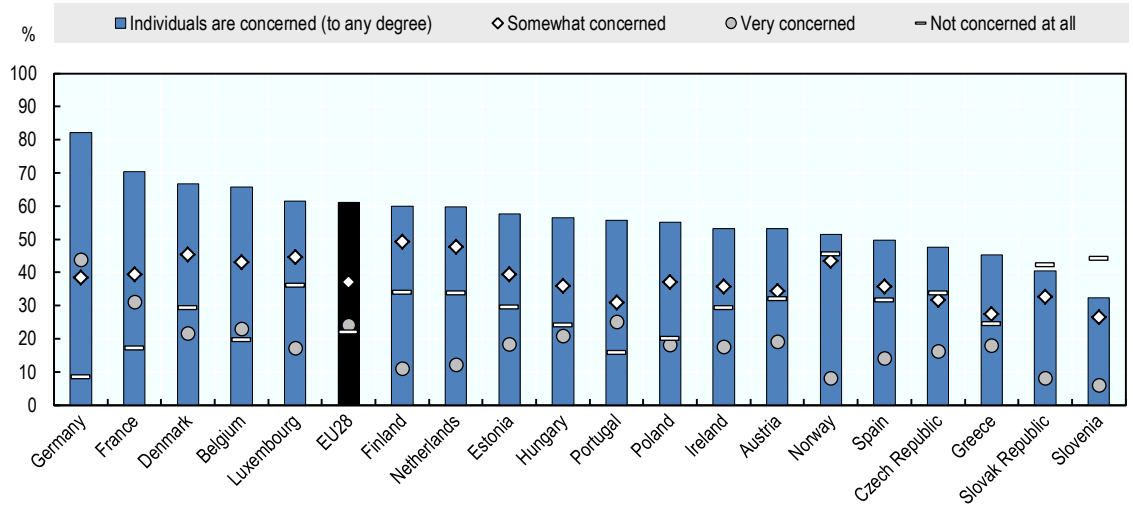
Os países em que mais pessoas referiram estar preocupadas (muito ou pouco) foram a Alemanha (82,1%), França (70,4%) e Dinamarca (66,7%).

Finalmente, os países em que menos de 20% das pessoas referem não estar de forma alguma preocupadas são a Alemanha (8,5%), Portugal (15,7%) e França (17,2%).

[5] Violação da confidencialidade de dados pessoais como resultado de actividades maliciosas ou perdas acidentais

[6] Uma posição mas próxima do topo da lista significa uma pior classificação a este respeito.

Gráfico 27 – Preocupações sobre as atividades *online* gravadas para fornecer publicidade por medida, 2016 (%de indivíduos)

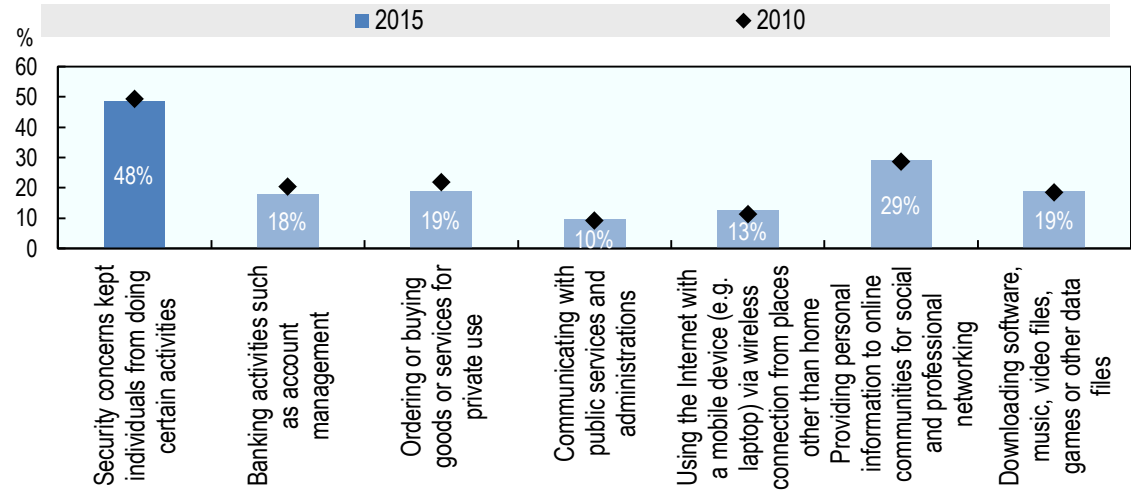


Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017b) - http://dx.doi.org/10.1787/888933586331

Muitos utilizadores de internet têm vindo a evitar executar actividades *online*. Os principais motivos apresentados são as preocupações de segurança (48,4%), com o fornecimento de informações pessoais em comunidades *online* para *networking* social e profissional (28,9%), com a encomenda ou compra de bens ou serviços para uso privado (18,9%) e com o download de software, música, arquivos de vídeo, jogos ou outros arquivos de dados (18,7%). Regista-se o facto de estas preocupações se terem mantido relativamente constantes em 2015 face a 2010.

As preocupações com a privacidade e com a segurança digital afastam os consumidores da utilização das TIC e do *e-commerce*, razão pela qual se torna mais relevante garantir a Cibersegurança.

Gráfico 28 – Preocupações de segurança impediram os usuários da Internet de realizar certas actividades (% de pessoas que usaram a Internet no último ano)



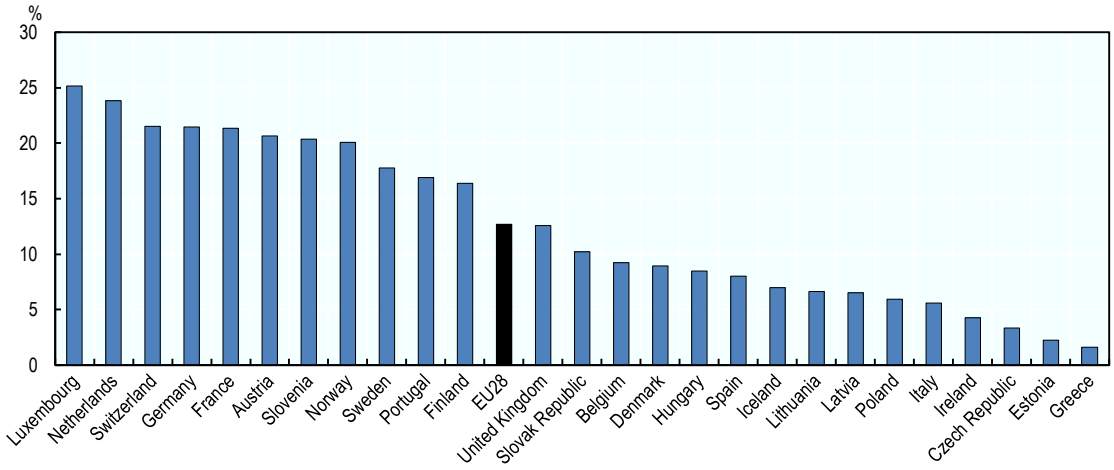
Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017b) - http://dx.doi.org/10.1787/888933586350

Segundo a OCDE, as actividades mais frequentes foram relacionadas com o risco de uso indevido de dados pessoais e de perdas económicas, nomeadamente através do roubo de identidade.

Em Portugal, em 2014, 16,9% das pessoas não usaram serviços de *cloud computing* devido a preocupações com privacidade ou segurança. Este valor é superior à média dos países da UE28 (12,7%), colocando Portugal na 8.ª posição em 26 países da UE28 considerados.

Ainda assim, alguns países da UE28 registam percentagens superiores de cidadãos que evitam utilizar *cloud computing* por receio quanto à segurança e privacidade: Luxemburgo (25,2%), Holanda (23,8%), Alemanha (21,5%), France (21,4%), Áustria (20,7%), Eslovénia (20,4%) e Suécia (17,8%).

Gráfico 29 – Preocupações com segurança e privacidade impediram indivíduos de usar computação em nuvem, 2014 (% de indivíduos)

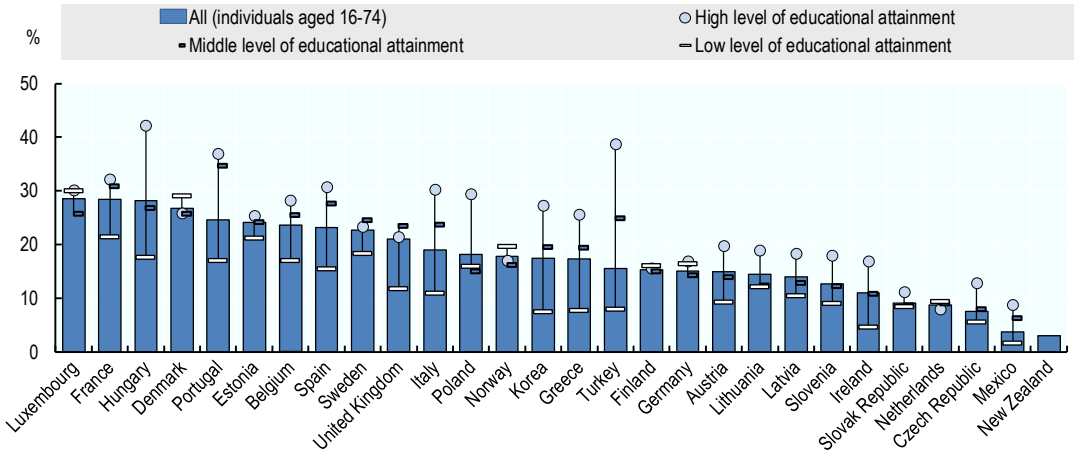


Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017b) - http://dx.doi.org/10.1787/888933586369

Em 2015, em termos de incidentes de segurança, 24,6% das pessoas em Portugal (entre os 16 e os 74 anos) refere ter sofrido incidentes de segurança digital, registando o 5.º pior resultado entre os 23 países da UE28 considerados.

De uma forma geral, ocorrem maiores incidentes a pessoas com maiores níveis de ensino por serem aquelas que mais utilizam as TIC e que por isso estão mais expostas a estes riscos: 36,9% no caso das pessoas com ensino superior, 34,6% nas pessoas com ensino média e 16,9% das pessoas baixo nível de ensino.

Gráfico 30 – Incidentes de segurança digital sofridos por indivíduos, 2015 ou posterior (% de todos os indivíduos e por nível de habilitações literárias)



Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017b) - http://dx.doi.org/10.1787/888933586445

3.2. As Empresas

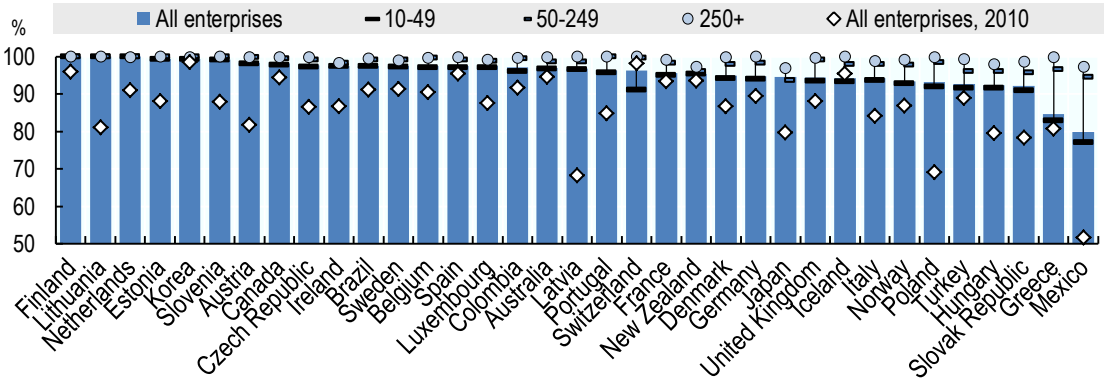
3.2.1. A utilização das TIC

Abordaremos, agora a utilização de TIC por parte das empresas.

Em Portugal, grande parte das empresas faz uso das TIC e, em 2016, 96,3% das empresas tinham conexão de banda larga, acima dos 84,7% registados em 2010 (mais 11,6 p.p., sendo este o 9.º maior aumento entre os países da OCDE) e à frente de países como França, Alemanha ou Reino Unido.

Destacam-se as empresas com mais de 250 funcionários (100,0%) e as empresas com entre 50 e 249 funcionários (99,9%), sendo as empresas com menos de 50 funcionários as que dispõe menos de conexões de banda larga (95,6%).

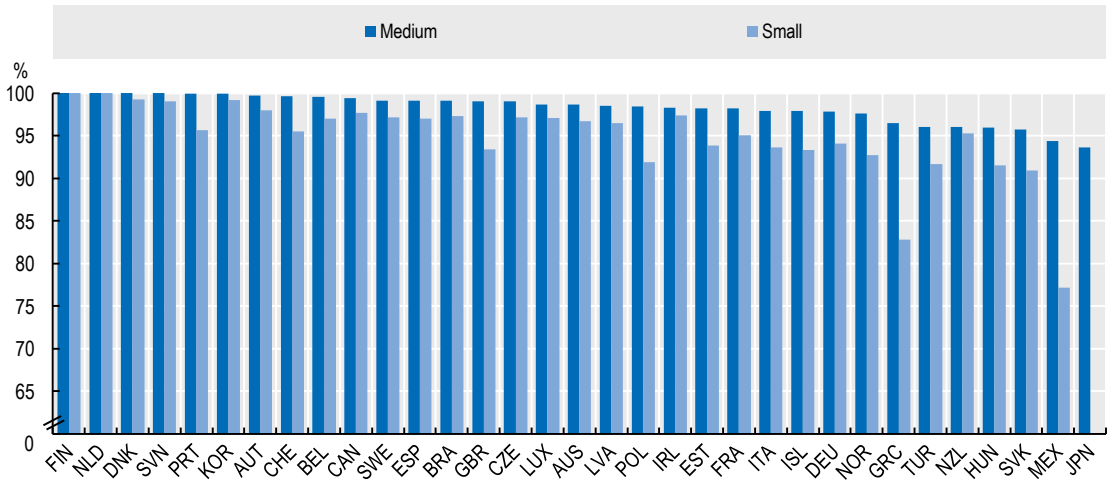
Gráfico 31 – Conectividade de banda larga nas empresas, por dimensão, 2016
(% de empresas por cada classe de dimensão do emprego)



Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017b) - http://dx.doi.org/10.1787/888933585419

Considerando a diferença entre as pequenas e médias empresas no que respeita ao acesso a banda larga (fixa e móvel), verifica-se que a maior penetração da banda larga diminuiu a diferença entre aquelas empresas. Em Portugal, a diferença entre pequenas e médias empresas com banda larga diminuiu de 9,1 p.p. em 2010 para 4,3 p.p. em 2016.

Gráfico 32 – Pequenas e médias empresas com acesso por banda larga, fixa ou móvel, 2016
(% de empresas em cada classe de dimensão do emprego)

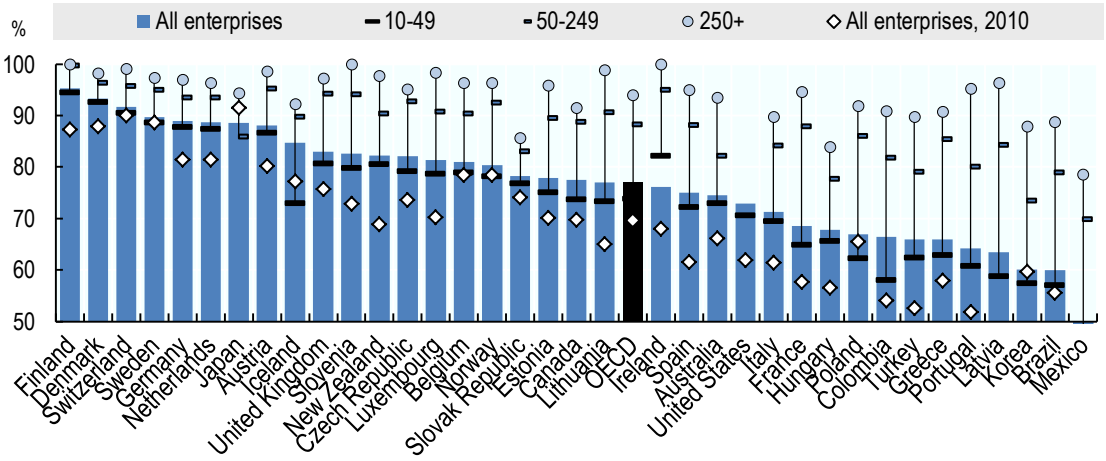


Fonte: OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation (OCDE, 2017a) - http://dx.doi.org/10.1787/888933619961

Em 2016, cerca de 64,2% das empresas portuguesas tinham um *site* ou página, em comparação com 51,9% em 2010 (77,0% e 64,2%, respectivamente, na OCDE). Nos países da UE28 considerados no gráfico seguinte, o progresso face a 2010 foi particularmente significativo na Letónia (15,1 p.p.), Espanha (13 p.p.) e Portugal (12,3 p.p.). Ainda assim, Portugal ocupa a 22.ª posição entre os 23 países da UE28 para os quais existe informação, apenas à frente da Letónia (63,5%).

A presença na web através de *sites* é menor entre as pequenas empresas (60,8%) que nas médias empresas (80,1%) e que nas grandes empresas (95,2%), tal como se verificou também para o acesso à banda larga.

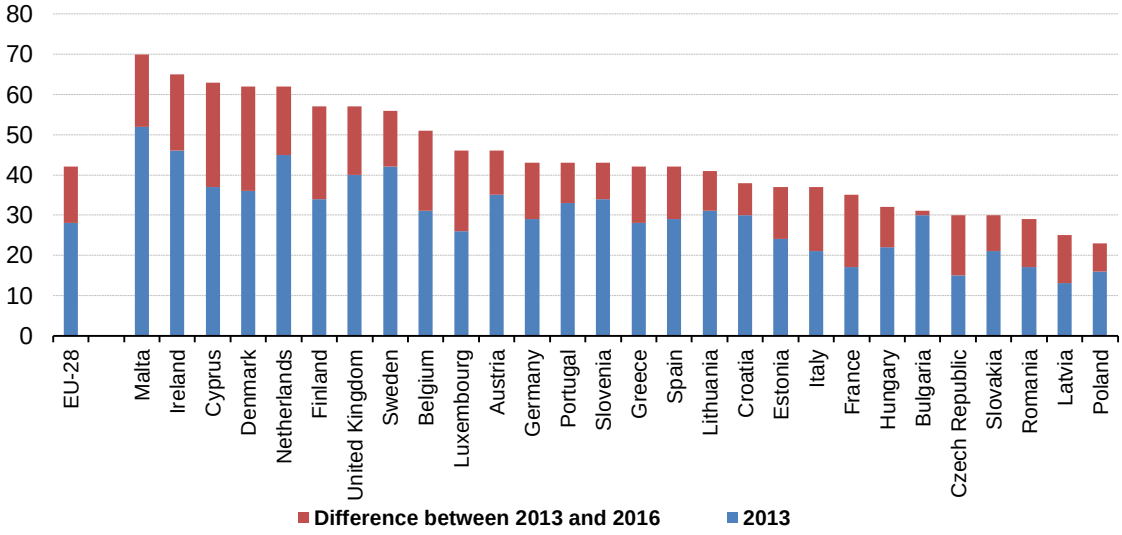
Gráfico 33 – Empresas com um *website* ou *home page*, por dimensão de empresa, 2016
(% de empresas em cada classe de dimensão do emprego)



Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017b) - http://dx.doi.org/10.1787/888933585438

Em Portugal, 43% das empresas utilizaram as redes sociais em 2016, encontrando-se na 13.ª posição entre os países da EU28 numa lista liderada por Malta (70%), Irlanda (65%), Chipre (63%), Dinamarca (62%) e Holanda (62%). A este respeito, Portugal desceu 2 posições face a 2013, ano em que ocupava a 11.ª posição, ocupando a 21.ª posição entre os países com maior aumento no uso empresarial das redes sociais entre 2013 e 2016. Parece, assim, haver um abrandamento na utilização de redes sociais pelas empresas.

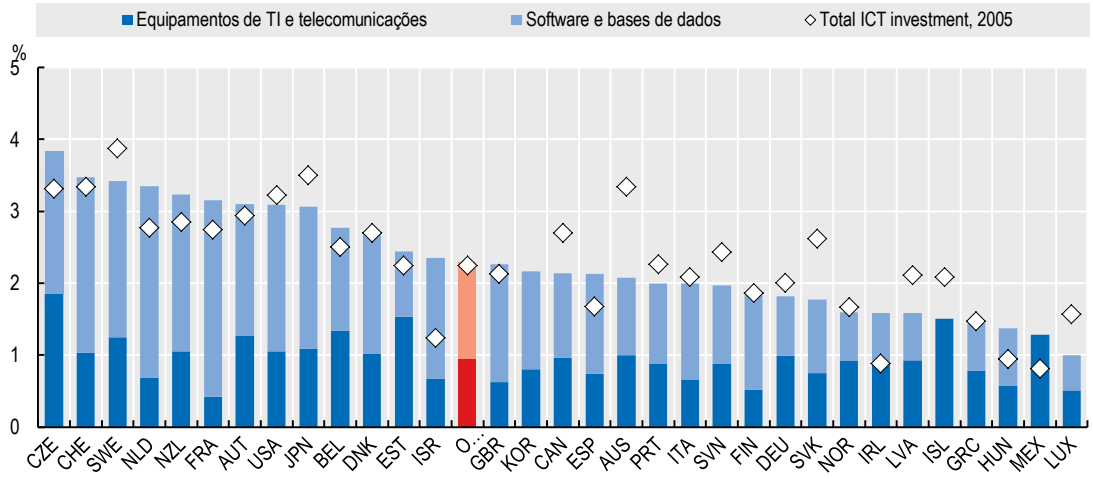
Gráfico 34 – Empresas que utilizam redes sociais, 2013 e 2016 (% de empresas)



Fonte: Eurostat (online data code: isoc_cismt)

Apesar de, entre 2005 e 2015, o investimento da OCDE em activos de TIC ter permanecido praticamente inalterado (passou de 2,2% para 2,3% do PIB), Portugal registou uma degradação deste indicador (de 2,3% para 2,0% do PIB).

Gráfico 35 - Investimento em TIC, por activos, 2015
(em percentagem do PIB)



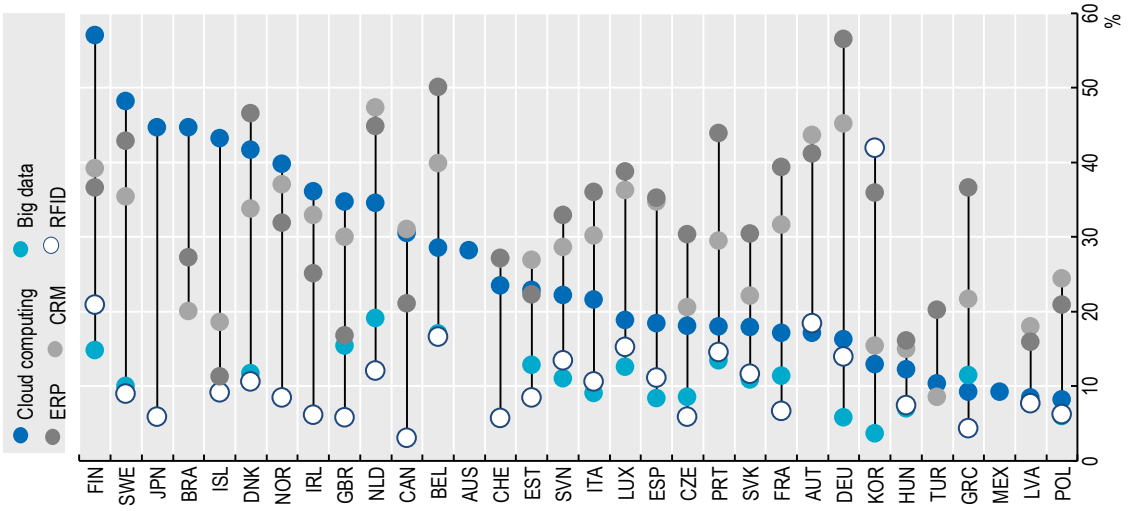
Fonte: OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation (OCDE, 2017a) - http://dx.doi.org/10.1787/888933618384

Apesar de uma parte substancial da economia actual seja desenvolvida através das TIC, os países integram estas ferramentas de forma diferente nos seus processos de negócio. Considerando empresas com mais de 10 pessoas empregadas, Portugal é o 21.º país (ex aequo com a Eslováquia) em 32 no que respeita à utilização de *Cloud Computing*, verificando-se que apenas 17,9% das empresas utilizam aquela ferramenta.

Também ao nível de *Customer Relationship Management* (CRM) Portugal ocupa apenas a 16.ª posição (entre 29 países para os quais existe informação), abrangendo 20,5% das empresas. Relativamente à adopção da análise de *Big Data*, em Portugal abrangeu 8,5% das empresas (5.ª posição entre 20 países).

Quanto à proporção de empresas que utilizam *Radio-Frequency Identification* (RFID), Portugal encontra-se na 6.ª posição entre 28 países (14,5% das empresas utilizam identificação por radiofrequência). Portugal é um dos países (5.º entre 29) em que uma maior percentagem das empresas (43,8%) adopta *Enterprise Resource Planning*.

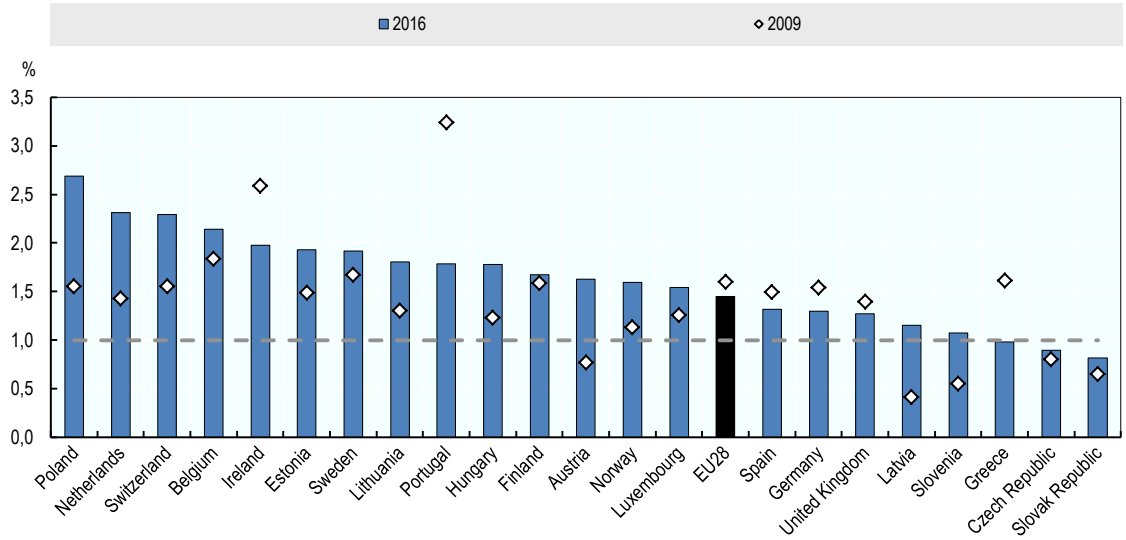
Gráfico 36 - Difusão de ferramentas e actividades de TIC em empresas, por tecnologia, 2016
(% das empresas com 10 ou mais pessoas empregadas)



Fonte: OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation (OCDE, 2017a) - http://dx.doi.org/10.1787/888933619581

Quanto à taxa média de vagas nos serviços de TIC face ao total do sector empresarial, verifica-se que Portugal registou a maior diminuição (-45%) de 2009 para 2016 (de 3,24% para 1,79%). Os maiores aumentos foram registados pela Letónia (183%), Áustria (112%) e Eslovénia (97%). Quando comparando com os 22 países da UE28 considerados, Portugal ocupa, em 2016, a 9.ª posição (1ª posição em 2009).

Gráfico 37 – Taxas médias de lugares vagos nos serviços de TIC relativamente ao total do sector empresarial (média anual das taxas trimestrais)



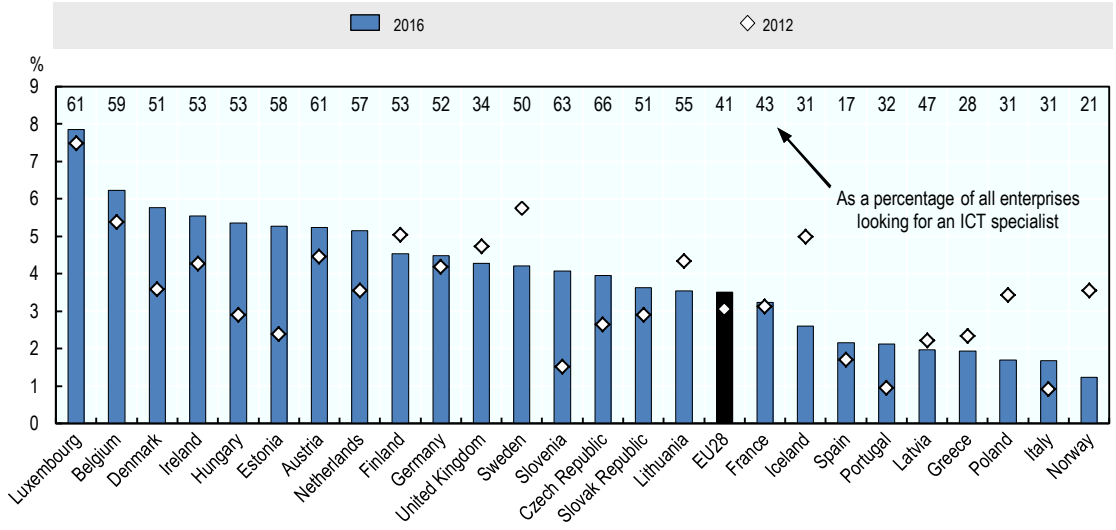
Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017b) - http://dx.doi.org/10.1787/888933585742

Em termos de especialistas em TIC, 32,0% das empresas portuguesas à procura destes quadros (2,1% do total de empresas) refere ter dificuldade em contratar. Verifica-se que mais empresas se deparam com esta dificuldade quando comparando com o ano de 2012 (0,9% do total de empresas), indicando que o aumento da procura não terá sido acompanhado pelo aumento da oferta (provocando a redução no número de vagas disponíveis referido no gráfico anterior).

Face aos 25 países da UE28 considerados no gráfico seguinte, Portugal ocupa a 20.ª posição mostrando que, ainda assim, é relativamente fácil de encontrar pessoas com esta especialização no país.

Lideram a lista dos países com maior percentagem de empresas à procura de especialistas em TIC e com dificuldade em contratar o Luxemburgo (61%), a Bélgica (59%) e a Dinamarca (51%), fixando-se a média de UE28 em 41%.

Gráfico 38 – Empresas que reportaram vagas difíceis de preencher para especialistas em TIC (% de todas as empresas)

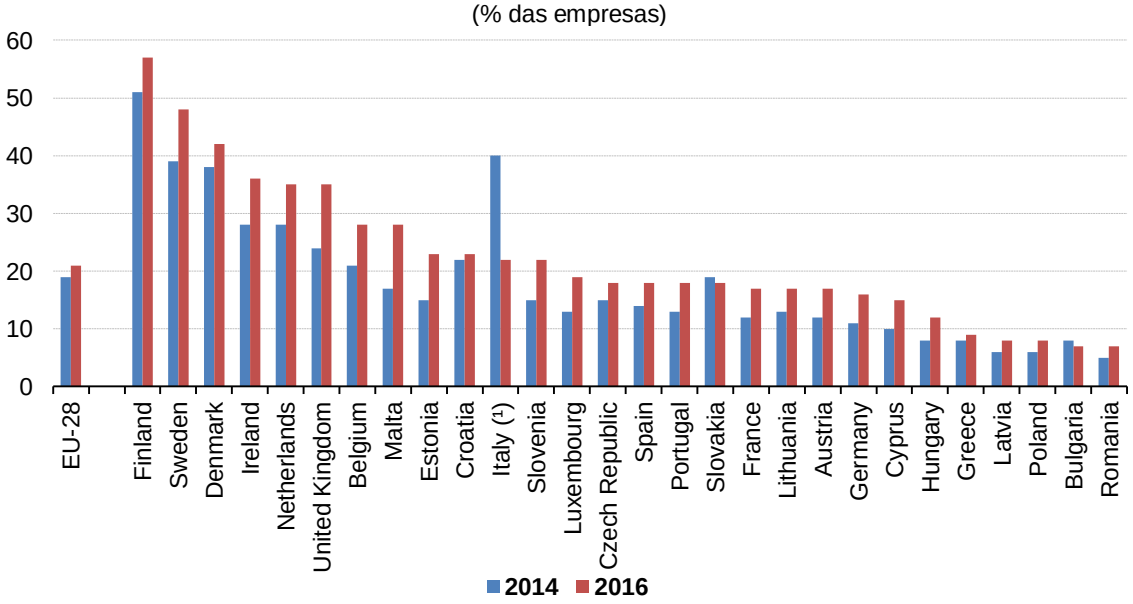


Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017b) - http://dx.doi.org/10.1787/888933585723

Cada vez mais empresas utilizam serviços de *cloud computing*, como resposta à cada vez maior digitalização da economia.

A percentagem de empresas em Portugal que utilizam serviços de *cloud computing* aumentou 5 p.p. entre 2014 e 2016 (de 13% para 18%). Portugal ocupa a 16.ª posição entre os países da UE28, subindo um lugar face a 2014. Apesar de Portugal se ter aproximado da média da UE28 (que passou de 19% em 2014 para 21% em 2016), continua abaixo. Nas 3 primeiras posições, acima de 40%, encontram-se a Finlândia (57%), a Suécia (48%) e a Dinamarca (42%). Em sentido contrário, com menos de 10%, encontram-se a Grécia (9%), Letónia (8%), Polónia (8%), Bulgária (7%) e Roménia (7%).

Gráfico 39 – Empresas que utilizam serviços de *cloud computing*, 2014 e 2016 (% das empresas)



Fonte: Eurostat (online data code: isoc_cicce_use)

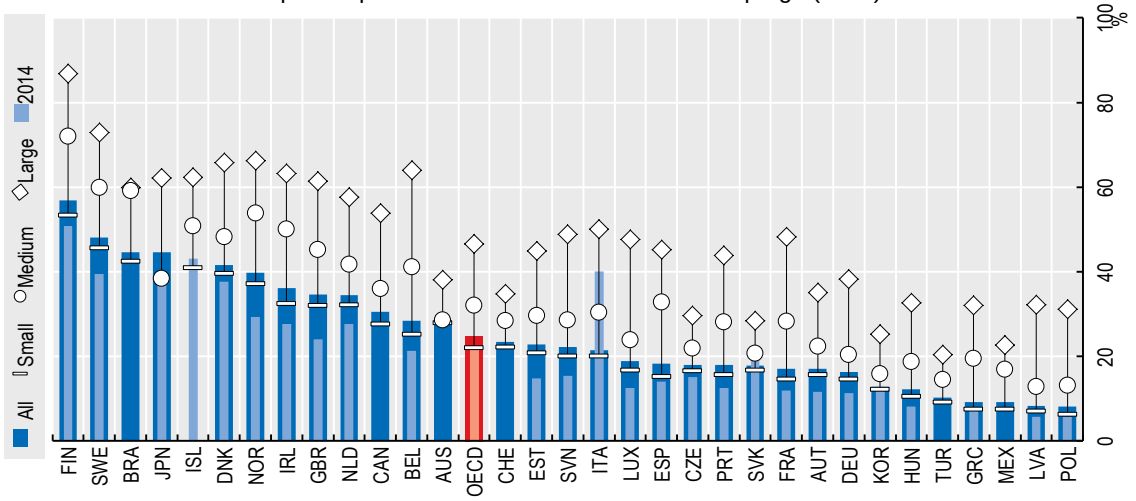
Em 2016, tal como referido, cerca de 18,0% das empresas portuguesas usavam estes serviços, abaixo da média da OCDE (24,8%).

A adesão é maior entre as grandes empresas (perto de 43,8%) em comparação com as pequenas ou médias empresas, que registram 15,6% e 28,1%, respectivamente.

O comércio electrónico e particularmente os serviços de *cloud computing* têm permitido impulsionar o negócio de muitas empresas, permitindo-lhes alcançar novos mercados. Em Portugal, 17,9% das empresas usaram esses serviços em 2016, em comparação com 12,6% em 2014. Apesar da subida significativa registada por Portugal (de 2014 para 2016, Portugal avançou 5,4p.p. enquanto a média da OCDE avançou 3,1 p.p.), o país encontra-se abaixo da média da OCDE (24,8%)

Novamente, a intensidade de uso de serviços de *cloud computing* varia de forma expressiva entre empresas de diferentes dimensões. Em média, apenas 15,6% das pequenas empresas portuguesas usam aqueles serviços, face a 28,1% nas empresas médias e 43,8% nas empresas grandes.

Gráfico 40 - Empresas que utilizam serviços de *cloud computing*, por dimensão, em percentagem das empresas por cada classe de dimensão de emprego (2016)



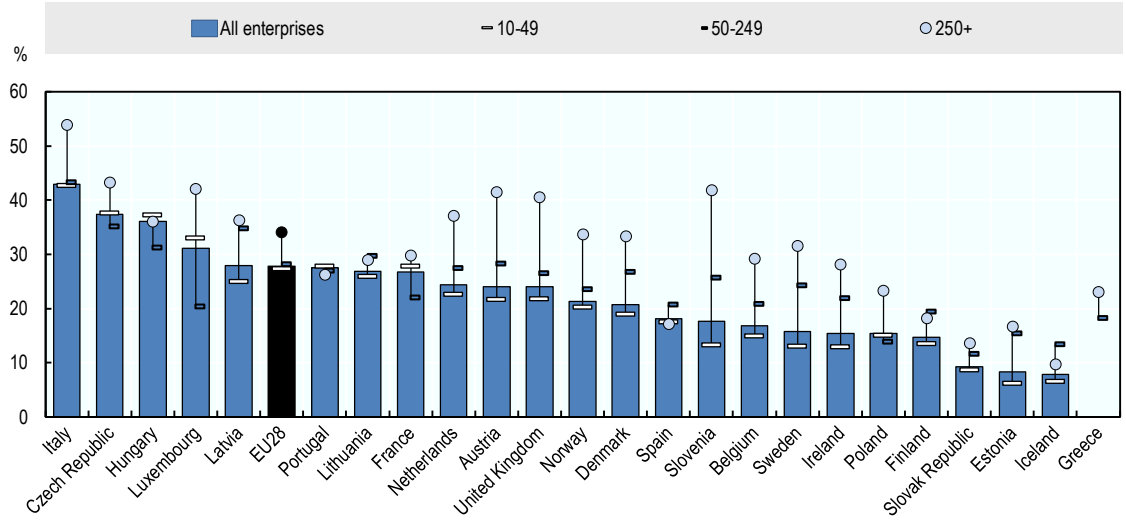
Fonte: OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation (OCDE, 2017a) - http://dx.doi.org/10.1787/888933619638

Em Portugal, em 2014, 27,5% das empresas não utilizavam *cloud computing* em todo o seu potencial por causa da percepção de dificuldades no cancelamento do serviço ou na mudança de provedor. O país encontra-se no 6.º lugar na lista de países em que existe mais essa percepção, embora ligeiramente abaixo da média da UE28 (27,8%).

A distribuição é relativamente semelhante em qualquer das dimensões de empresas consideradas (27,8% nas pequenas, 26,9% nas médias e 26,2% nas grandes).

Tal como referido pela OCDE, o problema na dificuldade na troca de provedor é que os usuários podem tornar-se vulneráveis ao aumento dos preços dos serviços pois os provedores de infra-estruturas poderão aumentar o preço para maximizar o lucro.

Gráfico 41 – Uso limitado de serviços de *cloud computing* devido a dificuldades das empresas na mudança de prestadores de serviços, 2014 (% de empresas que compram serviços de *cloud computing*)

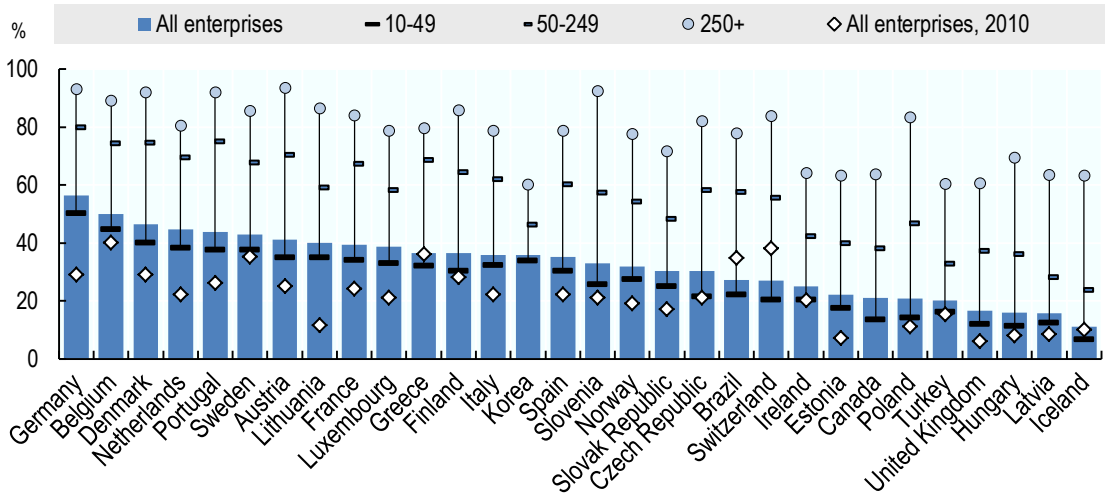


Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017b) - http://dx.doi.org/10.1787/888933586407

A utilização de ferramentas de gestão nas empresas Portuguesas aumentou entre 2010 e 2015, sendo utilizada em média por 43,8% das empresas em 2015, em comparação com os 26,0% registados em 2010. Esta evolução colocou Portugal na 5.ª posição em 2015 (6.ª posição em 2010) entre os países considerados no gráfico, apenas atrás da Alemanha (56,5), Bélgica (50,0), Dinamarca (46,5) e Holanda (44,8).

Registaram-se grandes diferenças nas empresas Portuguesas consoante a sua dimensão. No referido ano, os *softwares* de gestão foram utilizados por 91,8% das grandes empresas, mas por apenas 37,4% das pequenas empresas.

Gráfico 42 – Uso de *software* de planeamento de recursos empresariais, por dimensão da empresa, 2015 (% das empresas em cada classe de dimensão de emprego)



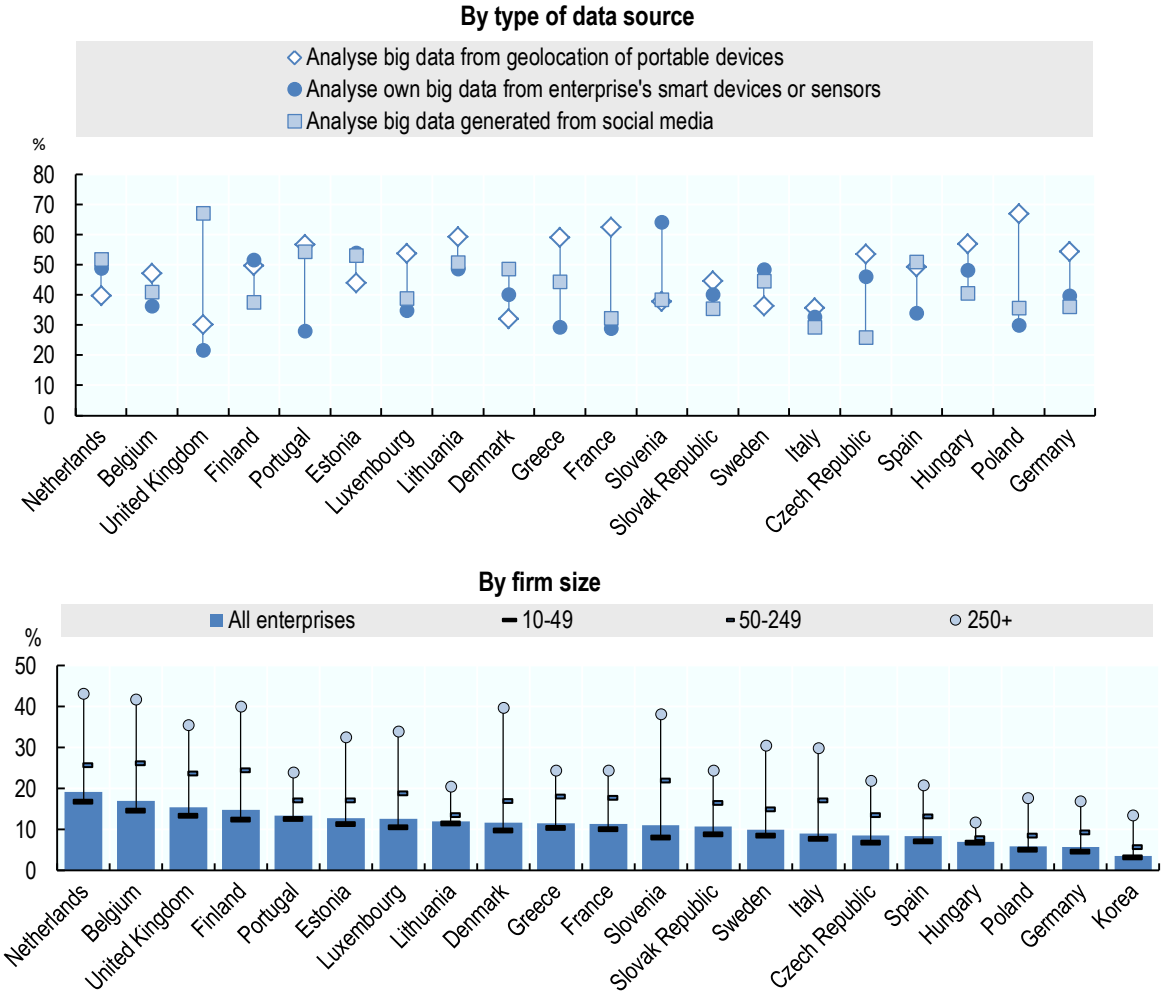
Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017b) - http://dx.doi.org/10.1787/888933585476

A percentagem de empresas em Portugal que realizaram *big data analysis* em 2016 foi de 13,4%, sendo o 5.º país com maior percentagem a seguir à Holanda (19,1%), Bélgica (17,0%), Reino Unido (15,4%) e Finlândia (14,8%).

A análise de grandes quantidades de informação é principalmente realizada entre as grandes empresas (23,9%, ocupando a 14.ª posição), seguidas pelas médias empresas (17,1%, ocupando a 9.ª posição) e pelas pequenas empresas (12,5%, ocupando a 4.ª posição). Para o resultado de Portugal contribui o facto de ter uma percentagem mais elevada de pequenas empresas que realizam *big data analysis* e um tecido empresarial constituído em grande parte por empresas pequenas.

Considerando a origem da informação, as empresas Portuguesas realizam *big data analysis* em particular de dados de geo-localização de dispositivos portáteis (56,6%, ocupando o 6.º lugar), seguido de informação gerada a partir das redes sociais (54,4%, ficando no 2.º lugar) e, em último, dados de dispositivos ou sensores inteligentes das próprias empresas (28,0%, ocupando a 19.ª posição).

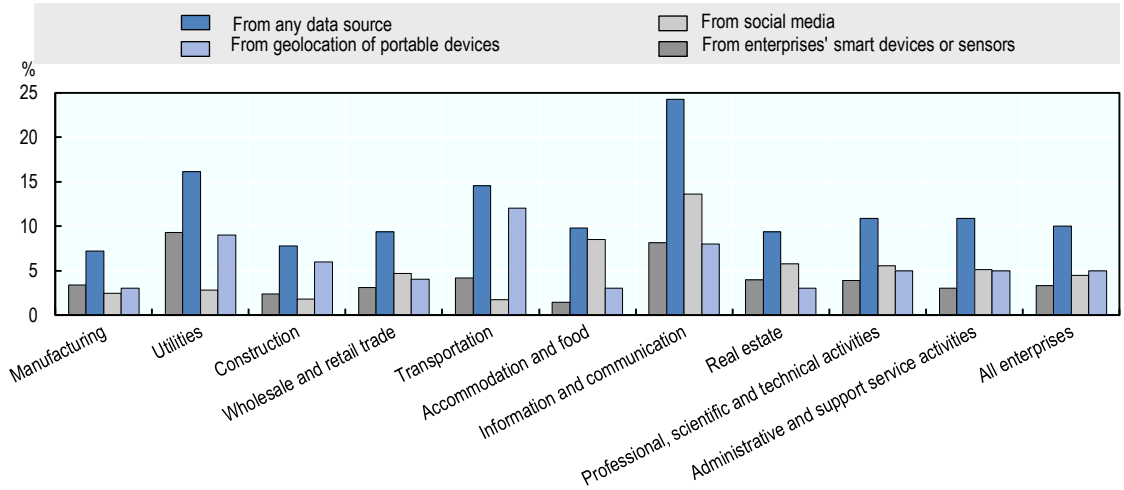
Gráfico 43 – Empresas que executam análise de grande volume de dados (*big data analysis*), 2016



Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017b) - http://dx.doi.org/10.1787/888933585514

É interessante notar que entre os diferentes sectores se verificam diferenças no tipo de dados pessoais recolhidos e nos meios usados para recolher esses dados (informação respeitante à UE28). Desde logo, o sector das TIC é naturalmente o maior utilizador de *big data*. O sector dos serviços (*utilities*) utiliza em particular dados dos dispositivos inteligentes. O sector dos transportes, por seu lado, destaca-se pela utilização de informação de dispositivos móveis. Finalmente, no alojamento e alimentação recorre-se em especial aos dados das redes sociais.

Gráfico 44 – Utilização comercial de *big data* por fonte de dados e sector, 2016
(% de todas as empresas)



Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017b) - http://dx.doi.org/10.1787/888933586521

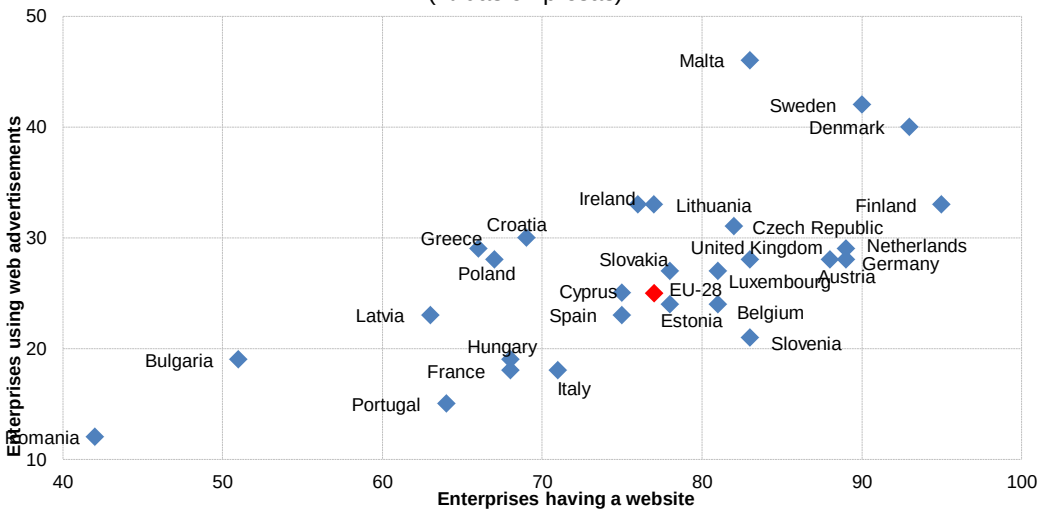
3.2.2. O Comércio Electrónico

Entraremos agora no subcapítulo em que faremos referência ao ponto de situação das principais questões ligadas ao comércio electrónico por parte das empresas.

À medida que a internet se tornou uma importante fonte de informação e uma componente essencial em todo, muitos clientes passaram a procurar cada vez mais adquirir bens e serviços através deste meio, pelo que muitas apostaram na presença na internet e na publicidade por este meio.

Como já foi referido, 64,2% das empresas portuguesas tinham um *website* em 2016 mas apenas cerca de 15,0% pagava por publicidade na *internet*. Como podemos observar no gráfico seguinte, existe tendência para que a percentagem de empresas com publicidade na internet seja maior nos países em que existe uma maior percentagem de empresas com *website*. Portugal que, como já tínhamos visto, apresenta uma percentagem baixa de empresas com *website*, é também dos países que apresentam percentagens mais reduzidas de empresas que pagaram por anúncios na Internet.

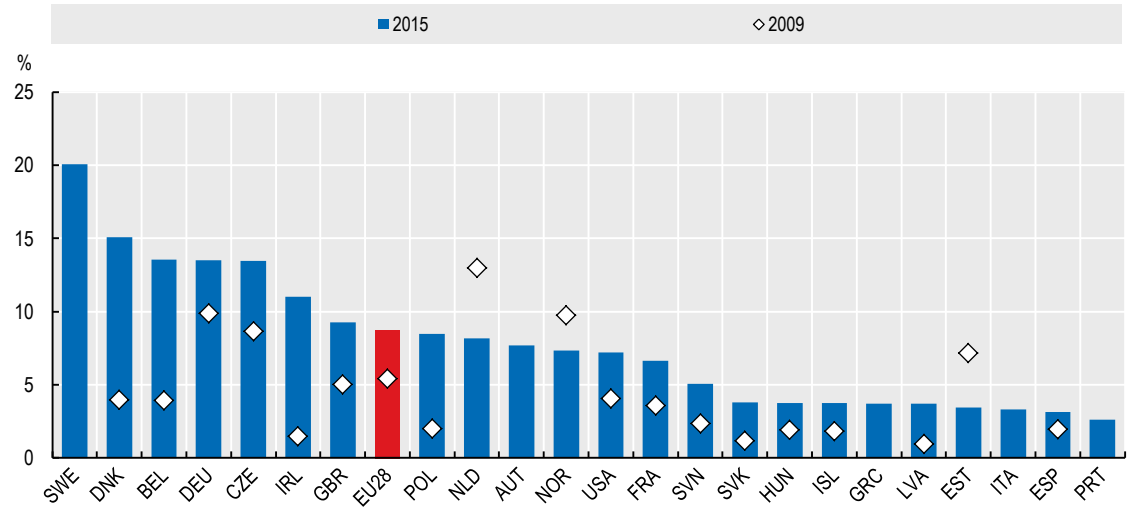
Gráfico 45 – Empresas que possuem um *website* e pagam por publicidade na *web*, 2016
(% das empresas)



Fonte: Eurostat (online data codes: isoc_cismt and isoc_ciweb)

O volume de negócios das empresas Portuguesas resultantes do e-commerce representou, em 2015, 2,6% do volume de negócios do retalho, muito abaixo da média da UE28 (8,7%) e colocando o país na última posição, sendo esta uma área que deverá merecer uma aposta no futuro.

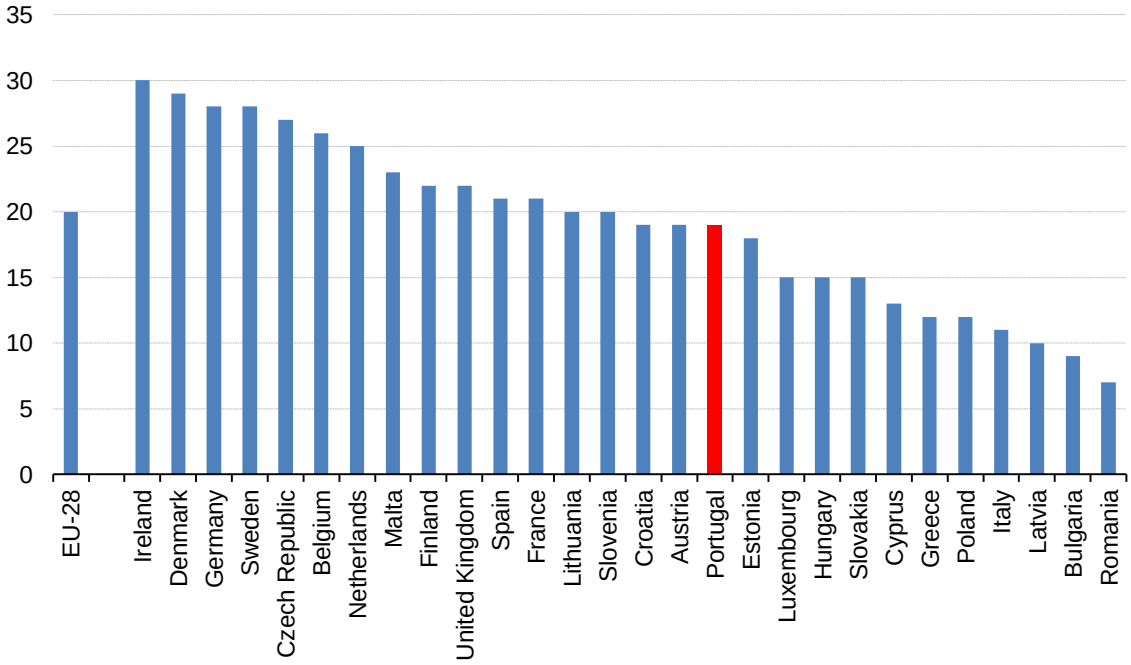
Gráfico 46 – Transacções entre empresas e consumidores (B2C), 2009 e 2015 (volume de negócios do comércio a retalho electrónico em percentagem do volume de negócios total no sector retalhista)



Fonte: OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation (OCDE, 2017a) - http://dx.doi.org/10.1787/888933620189

A quota de empresas em Portugal a realizar vendas electrónicas atingiu aproximadamente 19% (ver gráfico seguinte) em 2015 (aproximadamente o mesmo valor que o registado para a UE28 - 20%), registando-se o maior valor na Irlanda (30%).

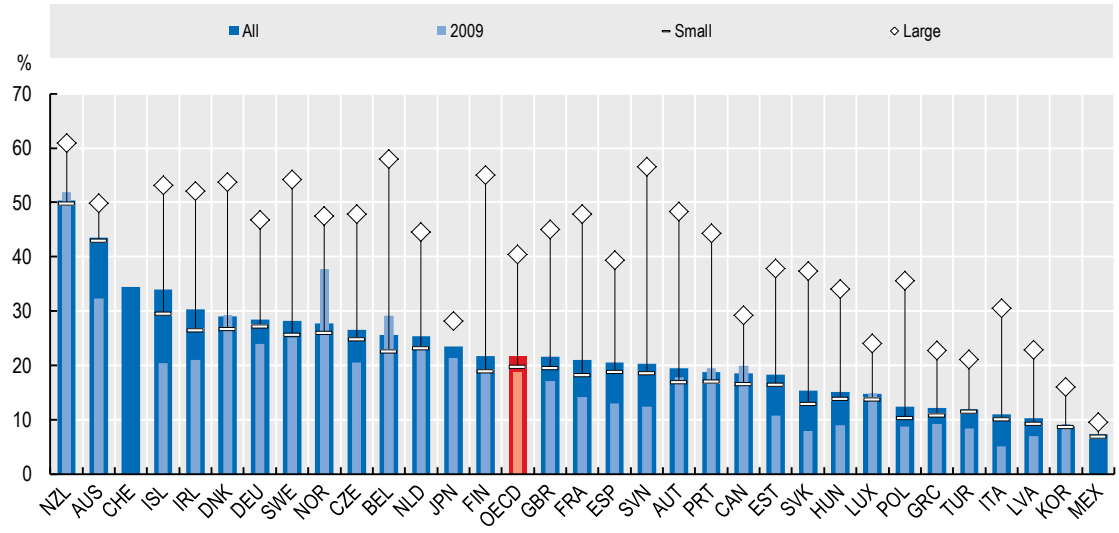
Gráfico 47 – Empresas que realizam vendas electrónicas, 2015 (% de empresas)



Fonte: Eurostat (online data code: isoc_ec_eseln2)

Em média, 22% das empresas da OCDE realizaram vendas via e-commerce em 2015, representando um aumento de 3 p.p. desde 2009. Portugal encontra-se abaixo da média da OCDE: 18,8% das empresas realizaram vendas via e-commerce em 2015, menos 0,6 p.p. do que em 2009. Os baixos valores atingidos por Portugal estarão associados à prevalência de pequenas e médias empresas pois estas empresas têm menos actividade nesta área (18,2%) do que as empresas maiores (44,2%).

Gráfico 48 - Empresas envolvidas em vendas por comércio electrónico, por dimensão, 2015
(em percentagem das empresas em cada classe de dimensão de emprego)

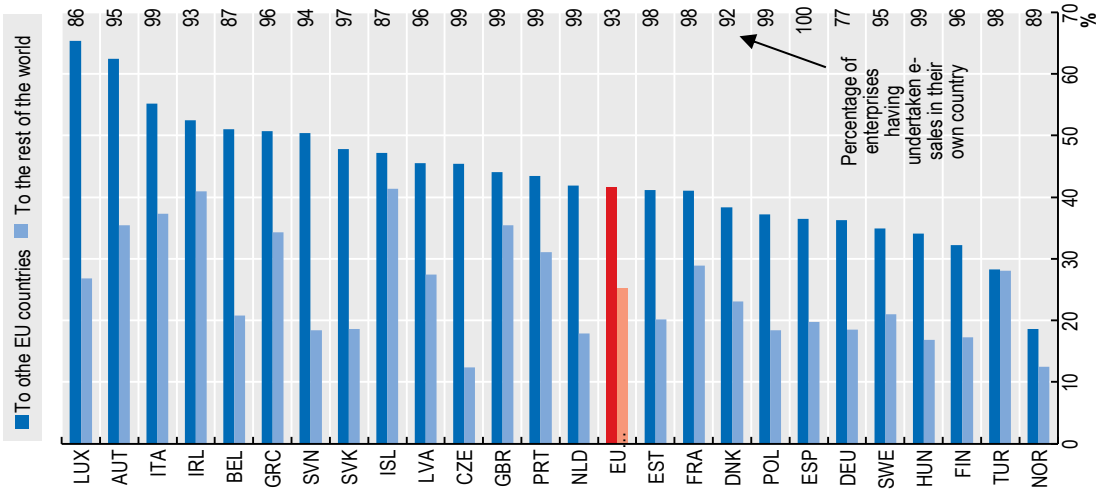


Fonte: OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation (OCDE, 2017a) - http://dx.doi.org/10.1787/888933619619

A Internet facilitou o acesso a novos mercados globais. Em 2014, 43,5% das empresas portuguesas que vendem *online* efectuaram vendas transfronteiriças para outros países europeus e 31,1% para países não europeus (41,7% e 25,3%, respectivamente, na média da UE28).

Embora a proporção de empresas que realizaram vendas para outros países da UE28 se tenha mantido constante entre 2010 e 2014, Portugal registou o segundo maior aumento nas vendas para o resto do mundo (+12,5 p.p.) naquele período (a seguir à Polónia que registou +18,4 p.p.).

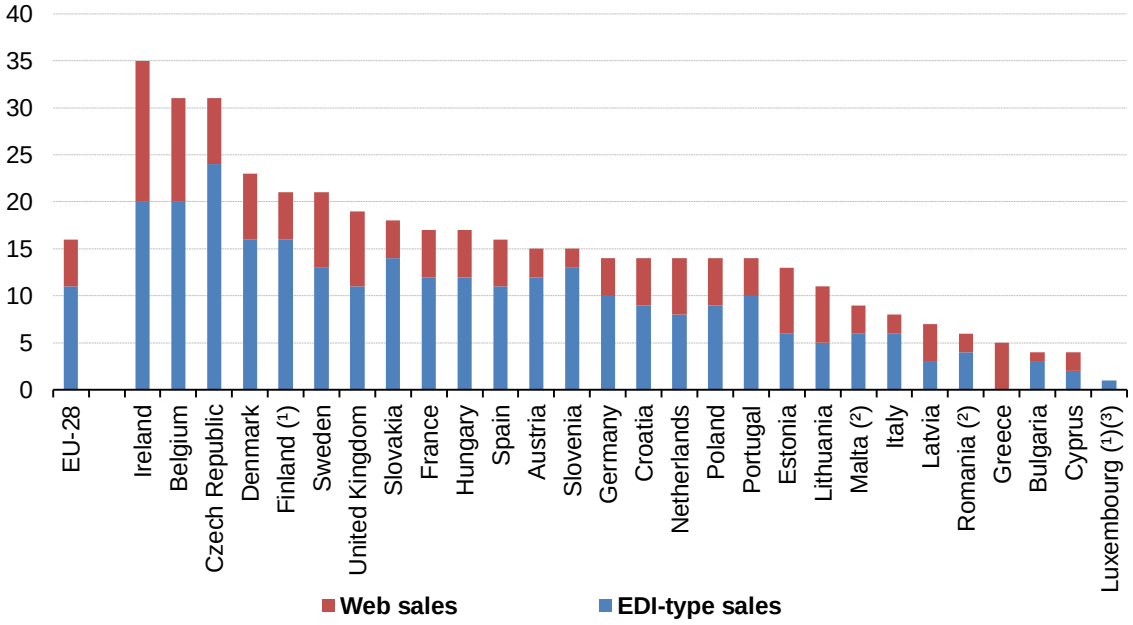
Gráfico 49 – Empresas que realizaram vendas transfronteiriças por comércio electrónico, 2014
(% de todas as empresas que efectuaram vendas por comércio electrónico)



Fonte: OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation (OCDE, 2017a) - http://dx.doi.org/10.1787/888933620151

Embora a percentagem de empresas que utiliza *websites* para efectuar vendas em linha em 2015 seja superior à que efectua vendas por meio de *electronic data interchange* (EDI), o peso das vendas na web no volume total de negócios gerado pelas empresas da UE28 foi relativamente baixa (5%) em comparação as vendas do tipo EDI (11%). Em Portugal, a tendência foi semelhante: 4% e 10%, respectivamente.

Gráfico 50 – Volume de negócios de vendas electrónicas, por tipo de encomenda, 2015
(% do volume de negócios total)



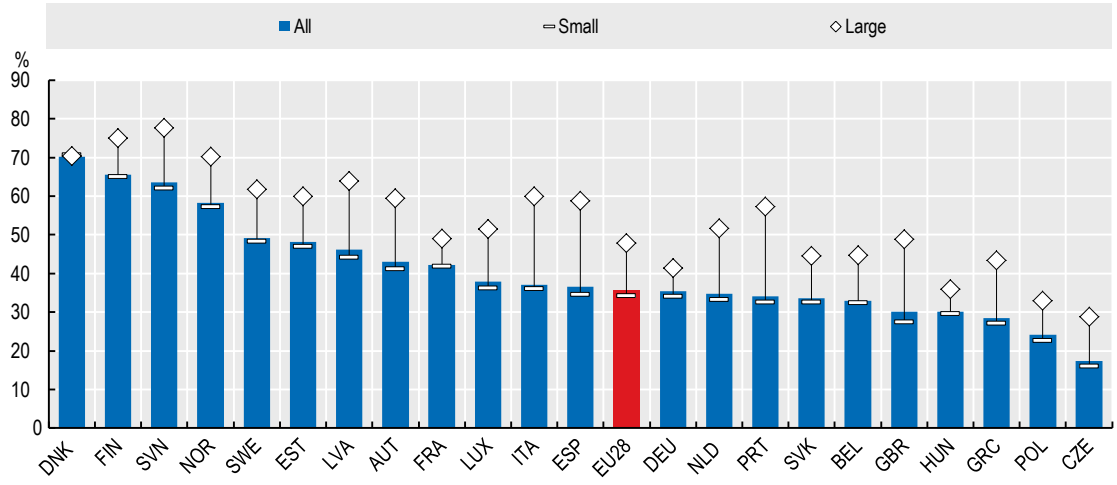
(1) 2014 | (2) 2013 | (3) Web sales: not available
Fonte: Eurostat (online data code: isoc_ec_evaln2)

3.2.3. A Cibersegurança

Depois de identificarmos as principais questões ao nível das TIC e do Comércio Electrónico, iremos neste subcapítulo abordar os principais indicadores disponíveis ao nível da Cibersegurança nas empresas, nomeadamente a forma como as empresas contactam as autoridades ou os receios que têm em relação à segurança da informação.

Em Portugal, em 2015, 34,1% das empresas enviaram uma factura *online* às autoridades públicas (ligeiramente abaixo da média da UE28 (35,6%), variando esta percentagem entre 17,4% na República Checa e 70,2% na Dinamarca. Tal como em todos os outros países considerados com excepção da Dinamarca, a utilização da internet para este fim é mais elevada nas grandes empresas (57,2%) do que nas pequenas empresas (32,6%).

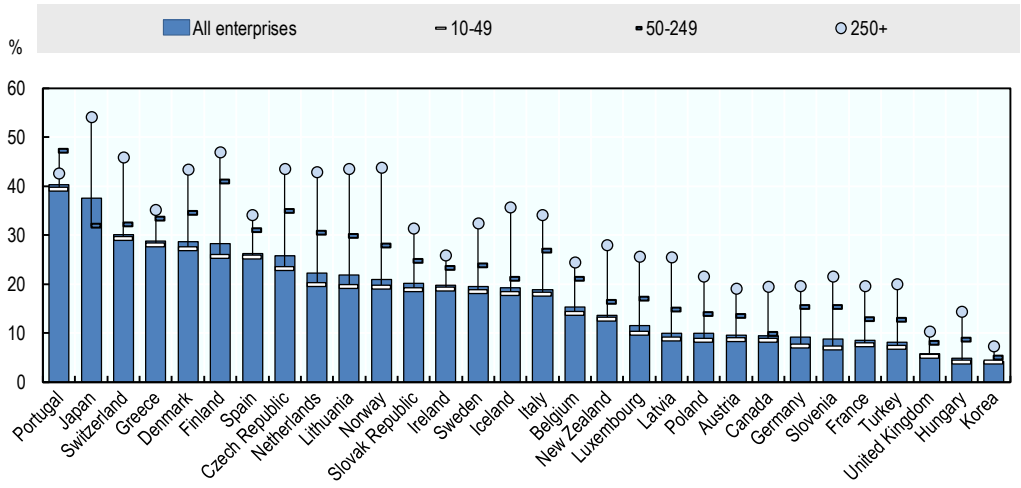
Gráfico 51 – Empresas que usam a Internet para enviar facturas às autoridades públicas, por dimensão, 2015 (% de empresas em cada classe de dimensão de emprego)



Fonte: OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation (OCDE, 2017a) - http://dx.doi.org/10.1787/888933620246

Também ao nível das empresas, Portugal é o país que regista um maior nível de incidentes em termos de Cibersegurança, embora se deva registar que em relação aos países da UE a informação disponível se reporta a 2010. Em termos de dimensão das empresas, as mais atingidas são as que têm entre 50 e 249 trabalhadores (47,1%), seguidas das que têm mais de 250 trabalhadores (42,6%), sendo as empresas com entre 10 e 49 trabalhadores as menos afectadas por estarem menos expostas (39,3%).

Gráfico 52 – Incidentes de segurança digital enfrentados pelas empresas, 2010 ou posterior (% de todas as empresas)

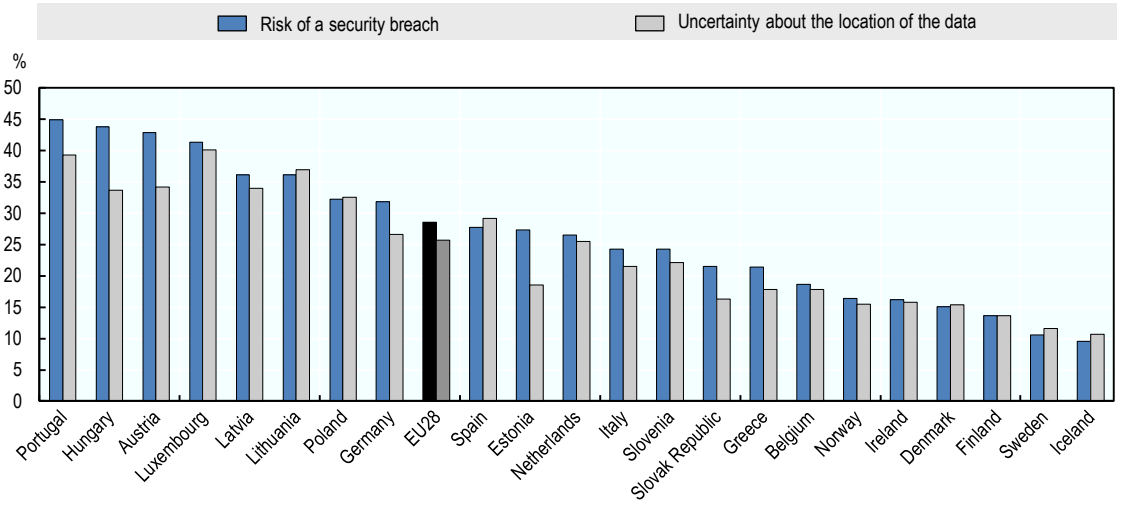


Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017b) - http://dx.doi.org/10.1787/888933586426

As empresas em Portugal, em 2014, referiam não utilizar *cloud computing* devido ao risco de quebra de segurança (44,9%) e por incerteza quanto à localização dos dados (39,3%). O risco de violação de segurança em Portugal é, assim, muito superior à média dos países da UE28 (28,5% e 25,6%, respectivamente).

Desta forma, entre os 20 países UE28 considerados no gráfico seguinte, Portugal encontra-se na primeira posição no que respeita a empresas que não usam *cloud computing* por receio de quebras de segurança e em 2.º lugar no que respeita a empresas que não usam *cloud computing* por incerteza na localização dos dados (apenas atrás do Luxemburgo em que esta percentagem atinge 40,1%).

Gráfico 53 – Razões pelas quais as empresas não utilizam *cloud computing*, 2014
(% de todas as empresas)

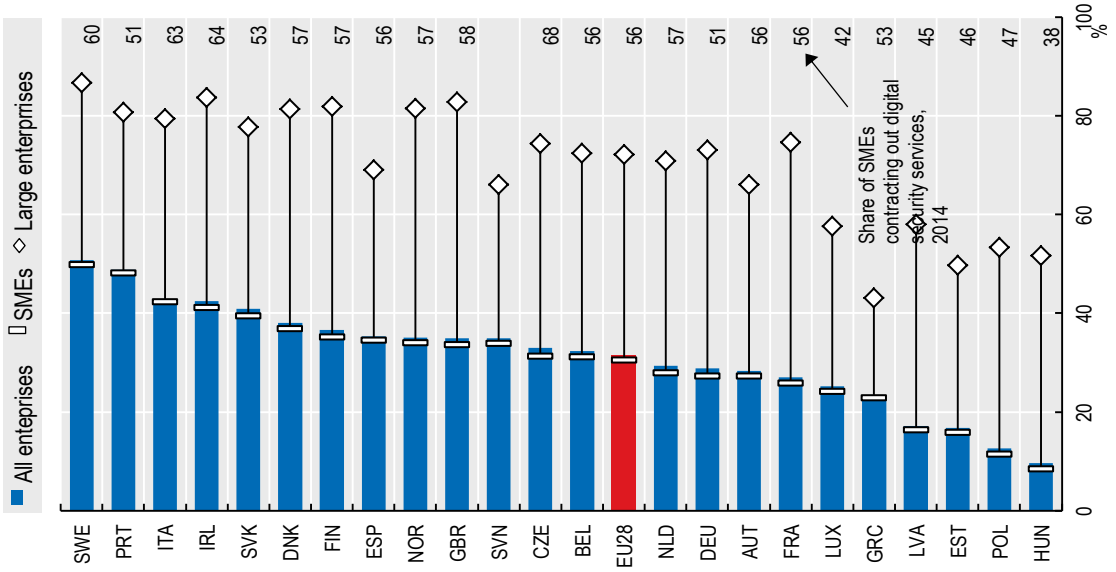


Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017b) - http://dx.doi.org/10.1787/888933586388

Quanto a percentagem de empresas que implementaram formalmente políticas de segurança nas TIC, Portugal é o segundo país da UE28 com o maior valor (48,8%), a seguir à Suécia (50,8%) e muito acima da média da UE28 (31,6%). Este valor é maior nas empresas grande (80,7%) do que nas PME (48,1%). Em termos de dimensão das empresas, Portugal, entre 22 países, ocupa a 7.ª posição nas grandes empresas mas esta posição é compensada pela 2.ª posição ocupada pelas PME, as quais representam a maioria do tecido empresarial português.

Ainda assim, Portugal é apenas o 18.º país entre os 23 da UE28 para os quais é fornecida informação, em termos de número de PME que contratam serviços de Cibersegurança.

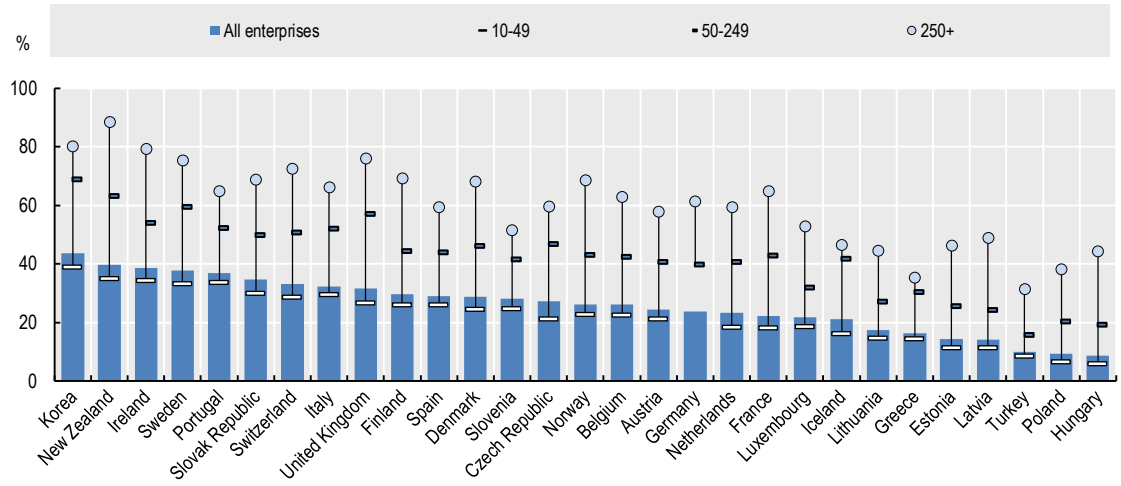
Gráfico 54 – Empresas com uma política de segurança formalmente definida, por dimensão, 2015
(% de empresas em cada classe de dimensão de emprego)



Note: Data for SMEs contracting out digital security services refer to the share of SMEs who have a formal ICT security policy where the security and data protection are mainly performed by external suppliers.
Fonte: OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation (OCDE, 2017a) -
http://dx.doi.org/10.1787/888933620265

No que respeita a empresas que implementaram uma política formal para gerir os riscos de privacidade digital, Portugal ocupa a 5.ª posição entre os 29 países considerados no gráfico (36,7% das empresas), precedido pela Coreia (43,7%), Nova Zelândia (39,7%), Irlanda (38,6%) e Suécia (37,6%). Considerando o número de funcionários, dentro de cada dimensão, verifica-se que este tipo de políticas é implementado com mais frequência nas empresas com mais trabalhadores: 33,5% nas empresas com entre 10 e 49 trabalhadores, 52,0% nas empresas com entre 50 e 249 trabalhadores e 64,8% nas empresas com mais de 250 trabalhadores.

Gráfico 55 – Empresas que têm uma política formal para gerir os riscos de privacidade digital, 2015 (% de todas as empresas em cada classe de dimensão de emprego)



Fonte: (OCDE, 2017b) - http://dx.doi.org/10.1787/888933586730

4. O papel das instituições nacionais e supranacionais

A existência de falhas de mercado, tais como as referidas no Tema Económico n.º 54 sobre "A Economia da Cibersegurança", justifica a intervenção através de políticas públicas. No entanto, muitas das intervenções tradicionais não funcionam num contexto de Ciberespaço.

Algumas das políticas públicas destinadas a corrigir falhas de mercado passam por esquemas de certificação, divulgação de informações e responsabilização dos intermediários.

Neste capítulo, iremos analisar o papel das autoridades Portuguesas e das instituições supranacionais no que respeita a medidas de política pública implementadas em Portugal e a recomendações/resoluções ao nível das diferentes entidades supranacionais.

Entrando na questão do papel das instituições, interessa antes de mais conhecer os papéis associados aos principais *stakeholders*, Estado e Indústria, os quais desempenham diferentes papéis.

O relatório do EastWest Institute (2016) refere 5 âmbitos de acção dos referidos *stakeholders*:

- O Governo é, antes de mais, o responsável pelo desenho e implementação das políticas públicas e como regulador das TIC;
- A Indústria, por seu lado, desenvolve e fornece produtos e serviços de TIC;
- Finalmente, existem áreas em que os dois *stakeholders* têm um papel activo: o governo e a indústria são compradores de produtos e serviços de TIC e ambos deverão ser responsáveis pelo aumento da segurança.

Tabela 5 – Papéis e Responsabilidades dos *Stakeholders* Cibernéticos

Actor >	Government		Industry
Role >	Policymaker	ICT Buyer*	ICT Provider
The Five Principles			
Maintain an **open market** that fosters innovation and competition and creates a **level playing field** for ICT providers	●		
Create procurement practices that utilize **fact-driven, risk-informed, and transparent requirements** based on international standards and approaches		●	
Avoid requirements or behavior that **undermine trust** in ICT (e.g., by installing back doors)	●		●
Evaluate the practices of ICT providers in terms of creating product and service integrity		●	
Create and use tools and approaches to **address risk** and **assign high value** to cybersecurity investments	●	●	●

*Government and industry organizations both act as buyers of ICT products and services.

Fonte: EastWest Institute (2016)

Nesta secção forcar-nos-emos na função das instituições, considerando aqui não apenas o papel dos estados nacionais "tour court" mas também das organizações internacionais que desempenham um papel essencial nas políticas de Cibersegurança, em especial quanto às estratégias concretas e aos meios adequados de combate à Cibercriminalidade.

Convém notar que os países, ao prosseguirem estratégias de Cibersegurança, não estão apenas a proteger os interesses nacionais mas também os interesses dos membros das organizações internacionais de que fazem parte.

4.1. Conselho da Europa

Devido à evolução da tecnologia, o Conselho da Europa[7] avançou com a Convenção de Budapeste sobre o Cibercrime, de 23 de Novembro de 2001, tendo sido a principal iniciativa desta instituição ao nível da Cibersegurança por ter sido a primeira convenção a tentar harmonizar a legislação relativa ao cibercrime.

O Conselho da Europa proporciona aos países orientação na interpretação da Convenção, bem como programas de capacitação.

Com esta Convenção procurou-se harmonizar a lei penal na área do cibercrime, bem como melhorar a cooperação internacional. A Convenção prevê como crimes, entre outros, o acesso e a intercepção ilegítimos, a interferência em dados e em sistemas, o uso indevido de dispositivos, a falsidade e a burla informática e as infracções penais relacionadas com a pornografia infantil, o dano e sabotagem informática ou o uso de vírus.

[7] https://ccdcoe.org/coe.html

Por ser cada vez maior a ameaça de Ciberataques que pode pôr em causa a segurança e a soberania dois países, a Convenção foi ratificada[8] por 43 Estados-Membros do Conselho da Europa (incluindo todos os países da UE28 com excepção da Irlanda e da Suécia) e por 17 não membros.

4.2. Organização do Tratado do Atlântico Norte (OTAN)

Pela importância que os Ciberataques podem ter no âmbito das guerras convencionais (chamadas guerras híbridas), a Organização do Tratado do Atlântico Norte (OTAN) é outra das instituições supranacionais que inclui a Cibersegurança na sua agenda, tendo aprovado uma Política de Defesa e um Conceito Estratégico do Ciberespaço e fazendo abranger o Ciberespaço pelo Direito internacional.

Sendo prioridade da OTAN a protecção das redes e infra-estruturas de comunicação e informação dos seus aliados, a Agência de Comunicações e Informação da OTAN (NATO Communications and Information (NCI) Agency) inclui uma área dedicada à Cibersegurança.

Para garantir a Cibersegurança, fazendo face à crescente sofisticação das ameaças e ataques cibernéticos, a OTAN procura coordenar os esforços dos seus membros no âmbito do planeamento da defesa, nomeadamente através de uma maior cooperação com o sector privado intensificando a cooperação com a indústria[9] (NATO Industry Cyber Partnership). Ao nível do reforço da cooperação com a indústria, esta deverá centrar-se na partilha de informação e de boas práticas.

A OTAN desenvolveu diversos projectos de defesa na área do Ciberespaço, em especial no que diz respeito à partilha de informação sobre *malware*, ao desenvolvimento da cooperação e à formação na área da Ciberdefesa. Relativamente ao planeamento operacional, a OTAN define acções para preparar possíveis Ciberataques que consistem em criar uma maior consciência dos riscos e das acções necessárias através de actividades educativas e de formação.

Em 2016, os Ministros da Defesa da OTAN, na Cimeira de Varsóvia, acordaram incluir o Ciberespaço como mais um domínio de operações para efeito de segurança a juntar aos já tradicionais (Ar, Mar e Terra).

Recentemente, na Cimeira de Bruxelas (2018), os Ministros da Defesa acordaram a criação de um novo Centro de Operações do Ciberespaço (Cyberspace Operations Centre), procurando uma maior coordenação operacional (ao nível da cooperação e da troca de informação, bem como aproveitando melhor as capacidades nacionais para o desenvolvimento de missões e operações), fortalecer a Cibersegurança e integrar o Ciberespaço nas operações de defesa da OTAN.

A OTAN dispõe de um Centro de Excelência de Defesa do Ciberespaço (NATO Cooperative Cyber Defence Centre of Excellence[10]), do qual Portugal é membro[11], sedeado na Estónia (Tallinn) que se dedica à investigação e formação na área da Cibersegurança.

[8] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures
[9] http://www.nicp.nato.int/
[10] https://ccdcoe.org/
[11] https://ccdcoe.org/portugal-join-nato-cooperative-cyber-defence-centre-excellence-tallinn-0.html

Salienta-se a relevância do livro "Tallinn Manual 2.0 on the International Law applicable to Cyber Operations", redigido por um grupo de peritos internacionais em resposta ao convite do Centro de Excelência da OTAN, sendo o mais completo guia sobre a aplicação da legislação internacional às operações no Ciberespaço.

Adicionalmente, a OTAN dispõe de outros centros de formação em Itália (Escola de Comunicações e Sistemas de Informação) e Alemanha (Escola NATO), as quais proporcionam formação sobre funcionamento e manutenção dos sistemas associados às TIC e sobre Defesa do Ciberespaço. Em breve, a Escola de Comunicações e Sistemas de Informação passará a situar-se em Portugal (Oeiras). A OTAN dispõe ainda do Colégio de Defesa em Itália (Roma) com uma perspectiva mais estratégica e que abarca as questões da Devesa Cibernética.

Finalmente, a OTAN dispõe ainda de uma equipa de reacção rápida permanentemente pronta para prestar assistência aos aliados.

De forma a evitar duplicação de esforços, a OTAN trabalha articuladamente com outras instituições, como União Europeia. Serão feitas referências a exemplos dessa cooperação no respectivo subcapítulo.

4.3. Nações Unidas

As Nações Unidas[12], enquanto organização intergovernamental (constituída por quase 200 estados-membros[13], incluindo Portugal) que tem como objectivo a manutenção da paz e da segurança internacional, desenvolvem diversas actividades no âmbito da Cibersegurança.

Convém, antes de mais, referir que as resoluções das Nações Unidas são, em geral, não vinculativas (com excepção das recomendações do Conselho de Segurança, o qual não aprovou até ao momento qualquer resolução sobre Cibersegurança), tratando-se portanto de recomendações.

Até ao momento foram aprovadas várias resoluções por diferentes comités sobre questões ligadas à Cibersegurança.

Destaca-se o papel do Comité para o Desarmamento e a Segurança Internacional no qual se têm desenvolvido discussões de alto nível, desde 1988, sobre as ameaças à segurança da informação. Também ao nível deste Comité se realça a criação de grupos de peritos governamentais, em 2004, 2009, 2011 e 2014, com o objectivo de identificar as potenciais ameaças à segurança da informação e as possíveis medidas de cooperação que permitam combate-las. O primeiro grupo de peritos não conseguiu consenso mas posteriormente foi possível aprovar relatórios, em geral muito genéricos, destacando-se a aprovação de medidas de cooperação entre os países e da aplicação do direito internacional ao Ciberespaço (embora ainda não exista um consenso sobre a forma como a legislação se deve aplicar ao Ciberespaço).

Salienta-se ainda o papel do Comité para as Questões Sociais, Humanitárias e Culturais que adoptou resoluções direccionadas para o Cibercrime e para o direito à privacidade na Era Digital (2000, 2001 e 2013), bem como do Comité Económico e Financeiro que tem apresentado diversas resoluções (2002, 2003 e 2009) tendo como foco a criação de uma cultura de Cibersegurança e a protecção das infra-estruturas de informação.

[12] https://ccdcoe.org/un.html
[13] https://www.itu.int/online/mm/scripts/gensel8

Realça-se o papel da União Internacional das Telecomunicações (International Telecommunication Union - ITU[14]), agência dependente das Nações Unidas especializada na área das TIC, funcionando como um organismo facilitador na cooperação internacional na área da Cibersegurança.

A Agência dispõe de um grupo de peritos de alto nível que inclui mais de 100 especialistas em Cibersegurança e em Políticas Públicas. Em termos de Cibersegurança, as principais linhas de acção são a implementação de mecanismos de aviso precoce e no desenvolvimento de uma plataforma de cooperação para resposta a incidentes e atenuação de ameaças.

4.4. Organização para a Cooperação e Desenvolvimento Económico (OCDE)

A OCDE[15] também tem abordado a questão da Cibersegurança, tendo como principais preocupações o futuro da economia digital, a digitalização das administrações públicas, a defesa das infra-estruturas e a protecção da privacidade da informação. Para tal, a OCDE procura articular os países-membros em torno de estratégias de Cibersegurança.

Esta preocupação tem ganho relevância na sequência dos grandes ataques ocorridos recentemente, quer pelo aumento da frequência quer pelo crescente nível de sofisticação utilizado. Neste sentido, as recomendações da OCDE vão no sentido de incentivar os países a ter em conta estas questões no processo de tomada de decisão das políticas públicas pois a Cibersegurança é essencial para permitir tirar o maior proveito possível da economia digital.

Ao nível da OCDE (2016a), destaca-se a recomendação de 2015 sobre "*Digital Security Risk Management for Economic and Social Prosperity (Security Risk Recommendation)*", a qual define um enquadramento das políticas de gestão do risco para assegurar a segurança digital, destacando as seguintes recomendações:

- "It is impossible to entirely eliminate digital security risk when carrying out activities that rely on the digital environment. However, the risk can be managed, that is, can be reduced to an acceptable level in light of the interests and benefits at stake, and the context.
- Leaders and decision makers should focus on the digital security risk to economic and social activities rather than only on the risk to the digital infrastructure.
- Organisations should integrate digital security risk management into their economic and social decision making processes and overall risk management framework rather than treating it solely as a technical problem".

A OCDE (2016a) realça as seguintes preocupações, salientando problemas associados às PME:

- Representando uma parte substancial do tecido empresarial dos países, as PME carecem de apoio na utilização de ferramentas digitais de forma a promover o funcionamento económico e o crescimento;
- Apresentam-se às PME desafios específicos da sua dimensão, nomeadamente falta de consciência dos Ciber-riscos e de capacidade de gerir a Cibersegurança;
- A limitação de recursos que normalmente se coloca às PME limita a sua capacidade de gerir o Ciber-risco e de implementar estratégias de Cibersegurança;

[14] https://ccdcoe.org/itu.html
[15] https://ccdcoe.org/oecd.html / http://www.oecd.org/sti/ieconomy/information-security-and-privacy.htm

- Refere ainda a importância de se analisar os factores que impedem o desenvolvimento da indústria de seguros contra Ciber-riscos.

4.5. União Europeia

Também a União Europeia[16] tem vindo a promover a segurança das redes e dos sistemas de informação e a combater o Cibercrime de forma a assegurar o funcionamento da economia digital, tendo publicado em 2013 o primeiro documento estratégico sobre Cibersegurança (Comissão Europeia, 2013a), o qual atribui aos governos o principal papel na prevenção e resposta aos Ciberataques em contraponto com uma supervisão centralizada por parte da União Europeia. Adicionalmente, a União Europeia aposta na cooperação internacional e na colaboração com o sector privado no combate ao Cibercrime.

Conforme refere a Comissão Europeia (2015), "cybercrime is by its nature borderless, flexible and innovative" e "Cybersecurity is the first line of defence against cybercrime". Esta é, alias, a razão que esteve por base na criação de estratégia europeia para a segurança da rede e da informação, procurando promover uma melhor cooperação entre as autoridades dos diversos Estados-membros, através da Agency for Network and Information Security. Através desta estratégia, a Comissão Europeia procurou criar legislação para criminalizar este tipo de crimes, incrementar a capacidade de Cibersegurança e promover a troca de informação entre os países (nomeadamente sobre incidentes registados).

A referida Estratégia (Comissão Europeia, 2013a) atribui um papel importante à União Europeia no apoio em caso de ocorrer um grande Ciberincidente ou Ciberataque, considerando ser motivo suficiente para que um Estado-membro invoque a Cláusula de Solidariedade prevista no artigo 222.º do Tratado sobre o Funcionamento da União Europeia.

Relativamente ao Cibercrime, a Directiva 2013/40/UE relativa a ataques contra os sistemas de informação (Comissão Europeia, 2013b) requer aos Estados-membros o reforço da legislação e das sanções aplicáveis ao Cibercrime.

Outra das vertentes essenciais da Directiva referida é o reforço da importância das redes, realçando em particular a rede do G8 e a rede de pontos de contacto do Conselho da Europa.

Outro marco essencial é a publicação da Directiva (UE) 2016/1148, a qual prevê medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União Europeia, obrigando os Estados-membros a aprovarem uma Estratégia Nacional, criando um Grupo de Cooperação para aumentar a cooperação e a troca de informação, criando uma rede de resposta rápida a incidentes e respectiva designação das entidades nacionais competentes e criando obrigações de notificação de incidentes a aplicar aos prestadores de serviços digitais e aos operadores de serviços essenciais (incluindo sector bancário e das infra-estruturas do mercado financeiro, energia, transportes, saúde, fornecimento e distribuição de água potável e infra-estruturas digitais).

Em 13 de Setembro de 2017, a Comissão anunciou o Pacote da Cibersegurança (Juncker, 2017) que veio rever a estratégia de 2013, com o objectivo de proteger os cidadãos e as empresas na era digital nomeadamente no que respeita à propriedade intelectual e aos dados pessoais, tendo por base não apenas instrumentos já existentes mas também novas iniciativas para melhorar a Ciberresiliência.

[16] https://ccdcoe.org/eu-0.html

O documento *State of the Union* 2017 (Juncker, 2017) refere o lançamento, entre outras, das seguintes iniciativas até ao final de 2018:

- Pacote de Cibersegurança que estabeleça medidas concretas para responder ao cenário de ameaças;
- Preparar uma resposta eficaz em caso de Ciberataques que afectem vários Estados-Membros;
- Proposta para reforçar a Agência Europeia para a Segurança das Redes e da Informação (ENISA - *European Network and Information Security Agency*), transformando-a na nova Agência Europeia de Cibersegurança, de forma a garantir que o organismo preste apoio aos Estados-Membros, instituições da UE e empresas em áreas-chave, incluindo a implementação da Directiva de Segurança das Redes e da Informação (SRI)[17];
- Criação de ferramentas de implementação para a Diretiva SRI, isto é, orientações sobre a forma como a Directiva deve funcionar na prática;
- Aposta na certificação europeia no sentido de tornar os dispositivos conectados mais seguros (*common cybersecurity certification framework*).

Adicionalmente, a Comissão havia anunciado que até final de Maio de 2018 proporia a primeira lei comum de Cibersegurança pelo que no dia 29 de Maio de 2018 apresentou a proposta de Regulamento do Parlamento Europeu e do Conselho relativo à:

- ENISA enquanto "Agência da UE em matéria de Cibersegurança" e
- Certificação em matéria de Cibersegurança da tecnologia da informação e comunicação.

Destacam-se, ainda, as seguintes iniciativas:

- Projeto para resposta rápida a emergências, no caso de um Ciberacidentes ou crise transfronteiriça em grande escala, estabelecendo os objectivos e os modos de cooperação entre os Estados-Membros e as instituições da UE na resposta a tais incidentes e crises;
- Reforço das relações externas, nomeadamente através de esforços para facilitar a cooperação com países terceiros para reforçar a rapidez na actuação e a responsabilidade do Estado no Ciberespaço.

Conforme foi referido no subcapítulo relativo à OTAN, a Cibersegurança é uma área de cooperação entre a União Europeia e organização através da troca de informação sobre ameaças e crises, da colaboração entre as equipas de resposta a emergências, da participação mútua em exercícios, do reforço da investigação e formação e da partilha de boas práticas.

4.6. Portugal

Em Portugal, a convenção de Budapeste sobre o Cibercrime, de 23 de Novembro de 2001, foi transposta para a legislação Portuguesa e entrou em vigor pela Lei n.º 109/2009, de 15 de Setembro, que aprova a Lei do Cibercrime, procurando dar segurança aos cidadãos e instrumentos às entidades que enfrentam a Cibercriminalidade.

[17] Foi publicada, no dia 19 de julho de 2016, a Diretiva (UE) n.º 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação (Directiva SRI).

Em 2012, o Governo de Portugal, através da Resolução do Conselho de Ministros n.º 12/2012, 7 de Fevereiro, considerou essencial a consolidação da Estratégia Nacional de Segurança da Informação, determinando a criação, instalação e operacionalização de um Centro Nacional de Cibersegurança.

A missão de criar uma comissão instaladora do Centro Nacional de Cibersegurança foi atribuída ao Gabinete Nacional de Segurança pela Resolução do Conselho de Ministros n.º 42/2012, de 13 de Abril.

Em 2013, o Governo de Portugal lança uma revisão do Conceito Estratégico de Defesa Nacional, através da Resolução do Conselho de Ministros n.º 19/2013, de 5 de Abril, tendo em conta a necessidade de proteger o funcionamento da economia e da sociedade da informação do Ciberterrorismo e da Cibercriminalidade[18], definindo as seguintes prioridades:

- "Garantir a proteção das infraestruturas de informação críticas, através da criação de um Sistema de Proteção da Infraestrutura de Informação Nacional (SPIIN);
- Definir uma Estratégia Nacional de Cibersegurança;
- Montar a estrutura responsável pela Cibersegurança, através da criação dos órgãos técnicos necessários;
- Sensibilizar os operadores públicos e privados para a natureza crítica da segurança informática e levantar a capacidade de Ciberdefesa nacional".

O Despacho n.º 13692/2013, de 28 de Outubro, veio introduzir as linhas orientadoras dos esforços a desenvolver ao nível da Defesa Nacional para o levantamento da capacidade nacional de Ciberdefesa, determinando que o Centro de Ciberdefesa fique na dependência do Chefe do Estado-Maior-General das Forças Armadas.

Mais tarde, o Decreto-Lei n.º 69/2014, de 9 de Maio, vem definir os os termos do funcionamento do Centro Nacional de Cibersegurança, o qual funciona no âmbito do Gabinete Nacional de Segurança.

Tendo em vista as prioridades anteriormente definidas, o Governo definiu a Estratégia Nacional de Segurança no Ciberespaço pela Resolução do Conselho de Ministros n.º 36/2015, de 12 de Junho, sendo o Centro Nacional de Cibersegurança definido como autoridade nacional nas questões relacionadas com o Ciberespaço.

A estratégia de 2015 salienta a necessidade de introduzir alterações na legislação no sentido de criminalizar novos tipos de crime (quer os crimes que têm como base o Ciberespaço quer os que consistem no ataque ao próprio Ciberespaço) e de introduzir uma maior cooperação entre as entidades judiciárias a nível nacional e internacional.

Esta estratégia pretende "(i) promover a consciencialização, uso livre, seguro e eficiente do ciberespaço, (ii) proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos; (iii) fortalecer e garantir a segurança do ciberespaço, de infra-estruturas críticas e de serviços nacionais vitais e (iv) afirmar o ciberespaço como um lugar para o crescimento económico e a inovação" (Cyberwiser, 2017) e tem essencialmente 6 objectivos estratégicos:

- Estruturar a segurança do ciberespaço,

[18] "A cibercriminalidade, porquanto os Ciberataques são uma ameaça crescente a infraestruturas críticas, em que potenciais agressores (terroristas, criminalidade organizada, Estados ou indivíduos isolados) podem fazer colapsar a estrutura tecnológica de uma organização social moderna";
"No domínio da cibercriminalidade, impõe-se uma avaliação das vulnerabilidades dos sistemas de informação e das múltiplas infraestruturas e serviços vitais neles apoiados".
(Conceito Estratégico de Defesa Nacional, Resolução do Conselho de Ministros n.º 19/2013, de 5 de Abril)

- Combater o Cibercrime,
- Proteger o ciberespaço e as infraestruturas nacionais,
- Promover a educação, a consciencialização e a prevenção;
- Incentivar a investigação e desenvolvimento e
- Fomentar a cooperação.

A estratégia de 2015 pretende que o Centro Nacional de Cibersegurança possa apoiar pedidos para o desenvolvimento da capacidade de reação a incidentes através da criação de novas equipas. A Rede Nacional de Equipas de Resposta de Informações sobre Segurança de Computadores (CSIRT - National Network of Computer Security Information Response Teams) é composta por um conjunto de 23 entidades nacionais[19].

Finalmente, a estratégia de 2015 prevê os mecanismos de reporte de incidentes ao Centro Nacional de Cibersegurança por parte de órgãos públicos e de operadores de infra-estruturas críticas.

Recentemente, o Parlamento Português aprovou o regime de segurança do Ciberespaço (Lei n.º 46/2018[20], de 13 de Agosto), transpondo a Directiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de Julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União Europeia.

A exposição de motivos da Proposta de Lei realça algumas das questões que já foram referidas ao longo deste documento, em especial que "a abrangência, frequência e impacto dos incidentes de segurança estão a aumentar, constituindo uma importante ameaça para o funcionamento das redes e dos sistemas de informação" e que "as redes e os sistemas de informação[21] desempenham um papel vital na sociedade, sendo a sua resiliência e segurança essenciais para a prossecução de actividades económicas e societais".

Na Lei aprovada pela Assembleia da República prevê-se:

- A definição de uma "Estratégia Nacional de Segurança do Ciberespaço";
- A estrutura nacional de segurança do Ciberespaço, incluindo a criação do "Conselho Superior de Segurança do Ciberespaço";
- A identificação do ponto de contacto único nacional para efeitos de cooperação internacional (Centro Nacional de Cibersegurança);
- A definição dos requisitos de segurança nas redes e sistemas de informação
- A aprovação das obrigações de notificação de incidentes ao Centro Nacional de Cibersegurança;
- A definição do regime de contra-ordenações aplicável à violação da Lei.

[19] Entidades nacionais que compõem a Rede Nacional de Equipas de Resposta de Informações sobre Segurança de Computadores (entre parêntesis encontra-se o ano de início): RCTS CERT - education and research network (2008), NOS (2008), Cabovisão (2008), CC-CRISI (EMGFA) (?), Portugal Telecom – telecommunications (2009), Claranet Portugal - Claranet members (2009), CSIRT.UPORTO (2009), ONI communications (2010), IP Telecom (2010), Millennium bcp (2010), Caixa Económica da Misericórdia de Angra do Heroísmo (2011), IGFEJ- Instituto de Gestão Financeira e Equipamentos da Justiça, IP (2011), EDP - Energias de Portugal (2011), INESC (2012), UTIS (2012), Dognaedis (2012), Caixa Geral de Depósitos (2012), PTServidor (2012), Vodafone Portugal - Vodafone corporate network (2013), ayer8 (2014), Novo Banco (2015), Seedrs (2017) e Banco de Portugal (2017).

[20] https://dre.pt/application/conteudo/116029384

[21] A Lei n.º 46/2018, de 13 de Agosto, define redes e sistemas de informação como "qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede de comunicações electrónicas que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção".

Tal como anteriormente definido, o Centro Nacional de Cibersegurança continua a ser a Autoridade Nacional de Cibersegurança e continuando a depender desta entidade a equipa de resposta a incidentes de segurança informática nacional acima referida (CSIRT).

Tal como previsto na Directiva, a Lei estabelece regras para a Administração Pública (nomeadamente enquanto operador de serviços essenciais), para os operadores de infra-estruturas críticas, para os operadores de serviços essenciais, para os prestadores de serviços digitais e para qualquer entidade que utilize redes e sistemas de informação.

Não obstante, a Lei remete para legislação própria (artigo 31.º) a definição de requisitos de segurança (artigos 14.º, 16.º e 18.º) e de requisitos de notificação de incidentes (artigos 15.º, 17.º e 19.º).

Face ao nível de exigência e relevância do Regulamento Geral sobre a Protecção de Dados (Regulamento (UE) n.º 2016/679, do Parlamento Europeu e do Conselho, de 27 de Abril de 2016), a referida Lei refere especificamente que "não prejudica o cumprimento da legislação aplicável em matéria de protecção de dados pessoais"

Finalmente, é de salientar a definição de um regime sancionatório (Capítulo IV) com coimas aplicadas a infracções[22]:

- Graves, abrangendo o "incumprimento de instruções de Cibersegurança emitidas pelo Centro Nacional de Cibersegurança", o "incumprimento da obrigação de notificar o Centro Nacional de Cibersegurança do exercício de actividade no sector das infra-estruturas digitais" e o "incumprimento da obrigação de notificar o Centro Nacional de Cibersegurança da identificação como prestador de serviços digitais";
- Muito graves, nas quais se inclui o "incumprimento da obrigação de implementar requisitos de segurança" e o "incumprimento de instruções de Cibersegurança emitidas pelo Centro Nacional de Cibersegurança".

No âmbito das audições aquando da discussão da Proposta de Lei, a APDSI (Associação para a promoção e desenvolvimento da Sociedade da Informação) considerou que "se está a confundir demasiado a Cibersegurança com a Ciberdefesa". Segundo esta entidade, o facto de o Centro Nacional de Cibersegurança funcionar no âmbito do Gabinete Nacional de Segurança ("estrutura essencialmente militar") implica uma militarização da Cibersegurança.

Tal como já foi referido, é importante destacar a instalação em Portugal (Oeiras), concluída em breve, da Escola de Comunicações e Sistemas de Informação, dando ao país um papel de grande relevância ao nível da investigação e estudos na área da Cibersegurança.

Segundo a Wiser[23], embora Portugal tenha adoptado uma estratégia de Cibersegurança, o país não desenvolveu um quadro jurídico e de políticas públicas abrangente para a Cibersegurança e a sua estratégia. Ainda assim, convém referir que grande parte das obrigações constantes da Directiva (UE) 2016/1148 já tinham sido cumpridas por Portugal.

[22] No caso das infracções por negligência, os limites mínimos e máximos das sanções aplicáveis são reduzidos para metade.

[23] WISER is a European initiative that puts cyber-risk management at the very heart of good business practice, benefitting multiple industries in particular critical infrastructure and process owners, and ICT-intensive SMEs. [https://cyberwiser.eu/cartography]

Por último, salienta-se a criação pela COTEC Portugal (Associação Empresarial para a Inovação Cibersegurança) de um Laboratório de Ciber-resiliência, uma área de actividade para reflexão e partilha de boas práticas sobre Cibersegurança, procurando uma maior colaboração entre o sector público e o sector privado.

5. Notas finais

Segundo o World Economic Forum, estima-se que em 2017 tenham ocorrido perdas financeiras a pessoas e empresas de mais de 500 mil milhões de euros em todo o mundo em resultado de ataques informáticos. Este valor será provavelmente superior pois muitas empresas não comunicam esta informação para evitar dar a conhecer a sua vulnerabilidade e para impedir que tenha um impacto negativo na sua credibilidade e confiabilidade.

Ataques informáticos como o *Wannacry* ou o *Petya* (ambos em 2017) trouxeram para a agenda mediática a questão da Cibersegurança. Embora não tenham sido os mais graves, foram os mais mediáticos e deixaram como certa a possibilidade de ocorrerem novos ataques no futuro.

O *Wannacry*, por exemplo, teve um impacto imediato muito elevado em grande parte dos países, tendo também afectado Portugal.

Figura 3 – Países inicialmente afectados pelo *Wannacry*

Fonte: Cybersecurity – Nordea On Your Mind (2018)

Pela relevância do tema, o presente Tema Económico procurou dar uma visão da situação de Portugal em termos de Ciberespaço e de Cibersegurança, quer ao nível dos cidadãos quer ao nível das empresas.

No que respeita aos cidadãos, regista-se ainda uma fraca adesão às TIC, não obstante a tendência positiva registada nos últimos anos, destacando-se nesta evolução positiva a população jovem e as pessoas com maior nível de escolaridade. Verifica-se ainda uma adesão reduzida à banda larga, em particular a móvel, e ao *cloud computing*. Apresentam, também, um baixo nível de recurso ao comércio electrónico, não obstante aquele valor ser superior no caso dos jovens.

Os portugueses recorrem pouco à entrega de formulários pela *internet* e facultam pouca informação *online* por receio em relação à privacidade e segurança da informação, apresentando grande preocupação com a gestão do acesso às informações pessoais (em particular, preocupam-se com a utilização dos dados pessoais e receiam o uso indevido e perdas financeiras).

Devido ao reduzido número de utilizadores, o valor das perdas financeiras é reduzido mas ainda assim significativo e verifica-se um aumento dos ataques de *pharming* e *phishing*. Também se regista um aumento da violação de privacidade.

Face ao que foi acima elencado, verifica-se que os Portugueses continuam a ter receios de quebras de segurança na utilização da *internet* o que pode estar a atrasar a distribuição dos benefícios da digitalização. Face ao grande receio dos cidadãos em utilizar a internet por receio de ataques e à necessidade de reduzir vulnerabilidades a ataques, regista-se a relevância de criar campanhas de sensibilização para as questões da Cibersegurança e da Privacidade, nomeadamente que proporcionem informação sobre as consequências das acções realizadas *online*. Regista-se que as populações com mais idade e menor nível de escolaridade são potenciais focos para a promoção da inclusão social.

Relativamente às empresas, uma grande parte já utiliza banda larga, em particular as de maior dimensão mas com tendência para a redução do gap entre as empresas maiores e as mais pequenas. Ainda assim, muitas empresas continuam a não dispor de um *website* ou página, bem como de perfil nas redes sociais, e poucas pagam por publicidade na *web*.

As empresas portuguesas apresentam um fraco investimento nas TIC, utilizando pouco as ferramentas e actividades que aquelas proporcionam (e.g., *cloud computing* ou *big data*). Em termos de recursos humanos especializados na área das TIC, as empresas ainda apresentam alguma dificuldade em encontrar estes recursos, podendo esta ser uma área de aposta no futuro.

Em termos de comércio electrónico, o Volume de Negócios do *B2C* das empresas portuguesas é muito reduzido quando comparado com a média da UE28, embora a percentagem de empresas que realizam vendas electrónicas esteja perto daquela média e as empresas Portuguesas apresentem uma percentagem de vendas transfronteiriças acima da referida média.

Tal como no caso dos cidadãos, as empresas também utilizam pouco o envio de formulários, possibilidade que é utilizada com mais frequência nas grandes empresas.

Embora uma parte significativa das empresas Portuguesas tenham implementado formalmente políticas de segurança nas TIC e de gestão dos riscos de privacidade digital, apresentam um nível elevado de incidentes de segurança digital e receiam utilizar *cloud computing* devido ao risco de quebra de segurança. Ainda a este respeito, realça-se o facto de poucas PME (dos valores mais reduzidos quando comparado com os países da UE28) contratarem serviços de Cibersegurança.

Da parte das empresas ainda não se verifica uma aposta forte na Cibersegurança, provavelmente por não considerarem esta uma área prioritária (internalizando esta função), o que poderá ser explicada pelo facto de o tecido empresarial ser constituído na sua grande maioria por PMEs, com menos capacidade financeira para fazer face às necessidades de uma política de Cibersegurança eficaz.

É importante que os gestores de empresas passem a considerar a Cibersegurança e a gestão do risco como prioridades de gestão – a digitalização não traz apenas oportunidades mas também ameaças que deverão ser consideradas. Em particular, as empresas deverão adoptar estratégias de segurança claras, que dêem segurança aos clientes, e devem ter planos de resolução de uma crise de Cibersegurança e de comunicação externa.

Sendo certo que países em que as empresas apostam menos na Cibersegurança são menos atractivos ao comércio electrónico, é importante sensibilizar as empresas para a necessidade de direccionarem recursos para a Cibersegurança, pelo que as políticas públicas devem dar os estímulos adequados para que as empresas invistam nesta área.

A capacitação dos trabalhadores das empresas (e, também, a população de uma forma mais geral) nas questões digitais também poderá impedir que ocorram ataques informáticos pelo que é importante ter recursos humanos cada vez mais preparados. Neste sentido, é importante salientar a iniciativa Portugal INCoDe.2030 enquanto factor essencial para aumentar as competências digitais em Portugal, nomeadamente em termos de Cibersegurança. A aposta na formação digital dos recursos humanos poderá permitir antecipar e prevenir questões de Cibersegurança mas a mudança de mentalidades na gestão das empresas passa também por uma maior formação dos gestores das empresas.

É essencial, ainda, o cálculo e registo dos impactos de Ciberincidentes e da publicitação da informação por imposição legal. De certa forma é o que acontece actualmente com o RGPD[24], com as entidades a ser obrigadas a comunicar situações de violação de dados pessoais à entidade supervisora num prazo de 72 horas após a organização ter tido conhecimento da mesma. No mesmo sentido regista-se o novo Regime Jurídico da Segurança do Ciberespaço, o qual inclui a obrigação de notificar a ocorrência de incidentes nalgumas situações. Esta obrigação é essencial e deveria ser alargada pois, embora seja difícil impedir que ocorram ataques informáticos, é possível que do estudo dos incidentes ocorridos se retire aprendizagem que permita melhorar a Cibersegurança e a prevenção de novos Ciberataques.

O aumento de importância da Digitalização nos últimos anos e o consequente aumento da exposição dos cidadãos e das organizações a Ciberataques adiciona um potencial custo económico acrescido às falhas na Cibersegurança [25]. A este respeito, a estratégia Indústria 4.0 é essencial não apenas para apoiar a Digitalização da Economia mas também para contribuir para uma maior aposta na Cibersegurança.

[24] O RGPD define um conjunto de regras ao nível do tratamento e armazenamento de dados pessoais com as quais se espera aumentar a confiança dos consumidores e das empresas. A importância desta legislação prende-se directamente com a falta de confiança anteriormente sentida que prejudicava a economia digital pois uma grande parte das pessoas e empresas, como vimos, tinham receio de colocar informações pessoais na internet.
Por outro lado, o RGPD coloca novos desafios e dificuldades de aplicação às empresas (nomeadamente em termos de custos) pelo que resta saber se a aplicação demasiado rigorosa do RGPD tem efectivamente benefícios em termos de protecção da informação pessoal e/ou se poderá resultar num prejuízo para as empresas na área do comércio electrónico, em particular num país que é constituído maioritariamente por PMEs.

[25] "As Europe moves online, information security is becoming increasingly important: first, because the direct and indirect losses are now economically significant; and second, because growing public concerns about information security hinder the development of both markets and public services. While information security touches on many subjects from mathematics through law to psychology, some of the most useful tools for both the policy analyst and the systems engineer come from economics." Anderson et al. (2008a)

Em termos de infra-estruturas tecnológicas, não obstante a melhoria que tem vindo a ser registada por Portugal, esta é uma área com potencial para inovação num futuro próximo. Considerando que o impacto de iniciativas nesta matéria é tanto maior quanto menor a maturidade digital do país, a estratégia Indústria 4.0 é particularmente relevante para a Digitalização da Economia, contribuindo para o crescimento económico do país. Salienta-se, ainda, a importância da realização de grandes eventos tecnológicos como o Websummit, de grande investimento na área tecnológica como os recentemente anunciados pela Microsoft e pela Google, ou a instalação da Escola de Comunicações e Sistemas de Informação da OTAN em Portugal (Oeiras).

Conclui-se que, de uma forma geral, Portugal ainda tem muitas áreas em que se deverá desenvolver mas tem vindo a evoluir positivamente em termos de digitalização. Não obstante, quanto mais baixa a base de partida maior a possibilidade de crescer. Portugal tem potencial em termos de Economia Digital e para aumentar o crescimento da digitalização no futuro. Regista-se, ainda, a importância de haver uma maior cooperação internacional que permita identificar e neutralizar potenciais Ciberataques.

Tendo em conta a situação actual de Portugal e considerando a importância da Economia Digital para o crescimento da Economia, o país deverá continuar a apostar em iniciativas para o seu desenvolvimento, nomeadamente através do reforço das competências digitais nas empresas, em particular através da criação de programas universitários direccionados para esta área e de políticas que promovam o investimento nas novas tecnologias.

O RGPD é, certamente, muito importante para garantir a privacidade e segurança da informação. Também o novo Regime Jurídico da Segurança do Ciberespaço é essencial para criar condições para uma maior eficácia da Cibersegurança, embora fique por conhecer, para já, os requisitos de segurança e os requisitos de notificação de incidentes previstos na Lei.

Ainda no que respeita ao quadro legislativo, salienta-se a preocupação com a militarização da Cibersegurança que poderá acentuar a confusão entre Cibersegurança e Ciberdefesa. Neste sentido, a Cibersegurança não deveria ser uma área enquadrada numa estrutura essencialmente militar, como tem acontecido desde 2014, devendo focar-se mais na formação e sensibilização da sociedade civil e das empresas, tal como já foi referido.

Como linhas de investigação futura, realçam-se as seguintes hipótese que procuram compreender o papel das Políticas Públicas em termos de Cibersegurança, ou seja, se a Cibersegurança funciona graças às ou apesar das Políticas Públicas implementadas:

- Os impactos resultam de medidas do Governo ou são resultantes de políticas europeias, isto é, estamos perante uma Governação pela Europeização[26] ou uma Difusão de Políticas Públicas?
- As empresas reagem a políticas públicas, antecipam possíveis riscos independentemente das políticas públicas ou apenas actuam na sequência de Ciberataques?
- As políticas públicas têm tido impacto na actuação dos profissionais da área da Cibersegurança?

[26] A Europeização associada à adaptação institucional refere-se à forma como os actores são afectados e se adaptam às obrigações, orientações e pressões que advêm da integração na União Europeia.

Em qualquer dos casos, resta saber se o Estado e as empresas estão preparados para novos Ciberataques. É importante que as políticas públicas evoluam rapidamente de forma a fazer face às novas ameaças no Ciberespaço e que garantam a Cibersegurança, ainda que seja certo que não existem sistemas totalmente seguros. Em todo o caso, estas medidas são essenciais para dar confiança aos cidadãos e às empresas para que utilizem de forma plena os benefícios da Economia Digital.

Referências

AMROP (2017). "*Digitization on Boards Report | 2nd Edition - Are Boards Ready for Digital Disruption?*". Leadership Study.

Barros, Gabriel Osório de (2018). "Economia da Cibersegurança". Tema Económico n.º 53 – Gabinete de Estratégia e Estudos do Ministério da Economia.

Comissão Europeia (2015). "*Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security*".

Comissão Europeia (2013a). "*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*".

Comissão Europeia (2013b). "*Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA*".

Cyberwiser (2017). "*Wide-Impact Cyber Security Risk framework - Portugal*". Consultado em 30 de junho de 2018 em https://cyberwiser.eu/portugal-pt.

EastWest Institute (2016). "*Purchasing Secure ICT Products and Services: A Buyers Guide*". *Global Cooperation in Cyberspace Initiative*.

Governo de Portugal (2015). "*National Cyberspace Security Strategy - Portugal*". Resolução do Conselho de Ministros n.º 36/2015.

Governo de Portugal (2013). "Conceito Estratégico de Defesa Nacional". Resolução do Conselho de Ministros n. º 19/2013.

Governo de Portugal (2012). "Aprova o plano global estratégico de racionalização e redução de custos com as TIC na Administração Pública, apresentado pelo Grupo de Projeto para as Tecnologias de Informação e Comunicação (GPTIC)". Resolução do Conselho de Ministros n. º 12/2012.

Governo de Portugal (2009). "Lei do Cibercrime". Lei n. º 109/2009, de 15 de Setembro.

Instituto da Defesa Nacional e Centro Superior de Estudios de la Defensa Nacional (2013). "Estratégia da Informação e Segurança no Ciberespaço". Cadernos do Instituto da Defesa Nacional, 12.

International Telecommunication Union (ITU) (2017). "*Global Cybersecurity Index* (GCI) 2017". Telecommunication Development Bureau.

Juncker, Jean-Claude (2017). "*State of the Union 2017*".

Microsoft (2017). "*Microsoft Security Intelligence Report – Portugal*". *Volume 22, January through March, 2017* (https://www.microsoft.com/en-us/security/intelligence-report).

Nordea (2018). "*Cybersecurity - Nordea On Your Mind*". Nordea Bank AB (publ).

OCDE (2013a). "*Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*". OECD Digital Economy Papers No. 220, OECD Publishing, Paris.

OCDE (2015a). "*Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*". OECD Publishing, Paris (http://dx.doi.org/10.1787/9789264245471-en).

OCDE (2016a). "*Managing Digital Security and Privacy Risk*". *2016 Ministerial Meeting on the Digital Economy Background Report*.

OCDE (2016b). "*OECD Science, Technology and Innovation Outlook 2016*". OECD Publishing, Paris (http://dx.doi.org/10.1787/sti_in_outlook-2016-en).

OCDE (2017a). "*OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation*". OECD Publishing, Paris (http://dx.doi.org/10.1787/9789264268821-en).

OCDE (2017b). "*OECD Digital Economy Outlook 2017*". OECD Publishing, Paris (http://dx.doi.org/10.1787/9789264276284-en).

Website Builder Expert (2017). "*Which EU Country Is Most Vulnerable To Cybercrime?*".

World Economic Forum e The Boston Consulting Group (2018). "*Cyber Resilience Playbook for Public-Private Collaboration*". *Future of Digital Economy and Society System Initiative*.

World Economic Forum (2018). "*The Global Risks Report 2018*". Insight Report.