

# **Cibersegurança: o contributo da supervisão comportamental**

**Maria Lúcia Leitão**  
**Diretora do Departamento de Supervisão  
Comportamental**

**2.ª Conferência de Cibersegurança: “A Ciber-resiliência no setor financeiro”**

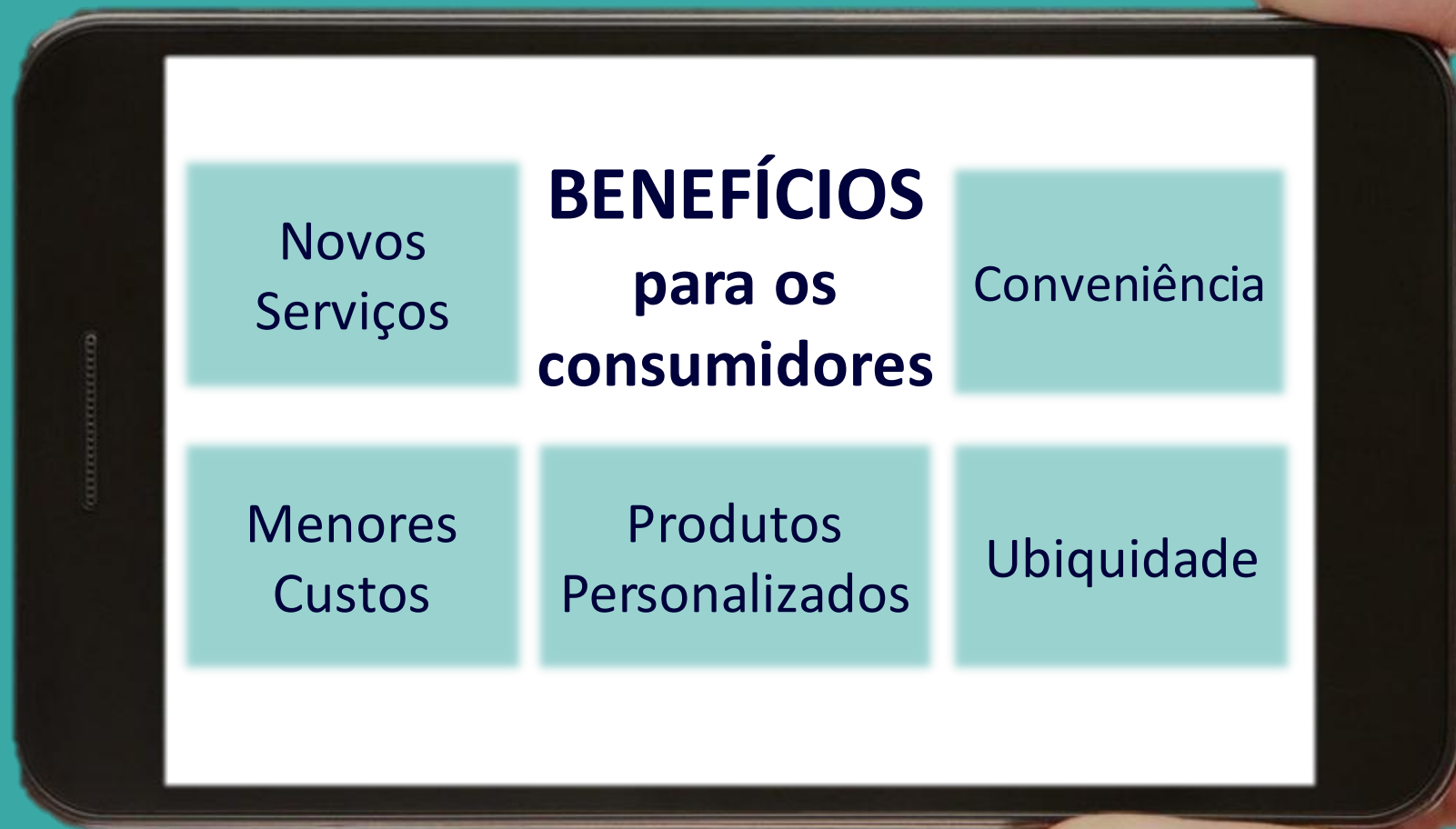


**BANCO DE  
PORTUGAL**  
EUROSISTEMA

«[FinTech] is already reshaping large financial services markets in ways that deliver BENEFITS for consumers, but that can also magnify existing RISKS and detriments, as well as introduce new ones»

*Banking on the Future: An exploration of fintech and the consumer interest, Consumers International, 2017*







# NOVOS RISCOS



**SEGURANÇA**



**PRIVACIDADE DOS DADOS**



***“Consumers’ financial and personal information should be protected through appropriate control and protection mechanism”***

***– Principle 8 Protection of Consumer Data and Privacy***

***G20 High-Level Principles on Financial Consumer Protection (2011)***

***“Financially excluded and underserved groups, in particular, face diverse consumer risks specific to digital financial services. They include: (...) inadequate security of systems”***

***G20 High-Level Principles for Digital Financial Inclusion (2016)***

***“The need for effective financial consumer protection is more important than ever”***

***G20/OECD Policy Guidance Financial Consumer Protection Approaches in the Digital Age (2018)***





# SEGURANÇA



In **2014**, *JP Morgan Chase*, the largest retail bank in the United States, was the **VICTIM OF A HACK** that compromised the data of more than half of all US households – **76 MILLION** – plus **7 million small businesses**

In 2014, the data of **20 MILLION INDIVIDUALS** – **40% of the Korean population** – were **stolen from three Korean credit card companies** (*KB Kookmin Bank, Lotte Card and Nonghyup Bank*). Personal data included identification numbers, addresses and credit card numbers

In **2016** *Tesco Bank*, British retail bank, **WAS VICTIM OF A CYBER-ATTACK** affecting **8.261 out of 131.000** Tesco Bank personal current accounts

In **2017**, **HACKERS STOLE THE PERSONAL DATA** of nearly **150 million people** from the databases of *Equifax*, a consumer-reporting agency



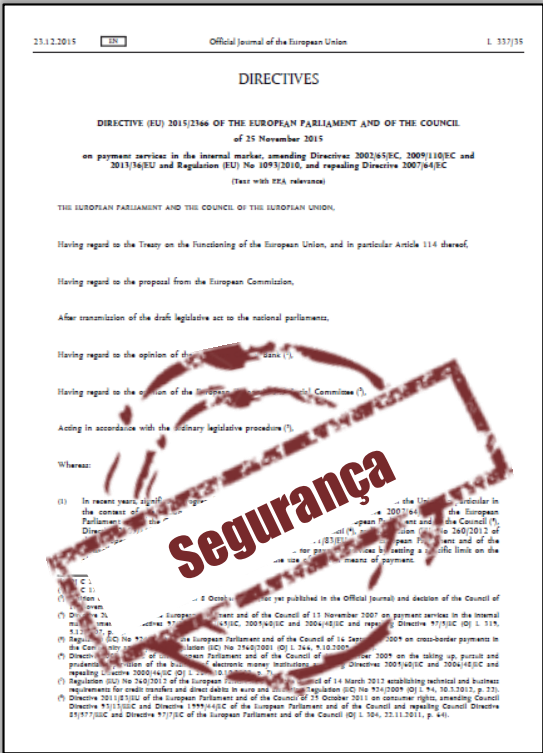
# A cibersegurança está na agenda internacional a nível mundial



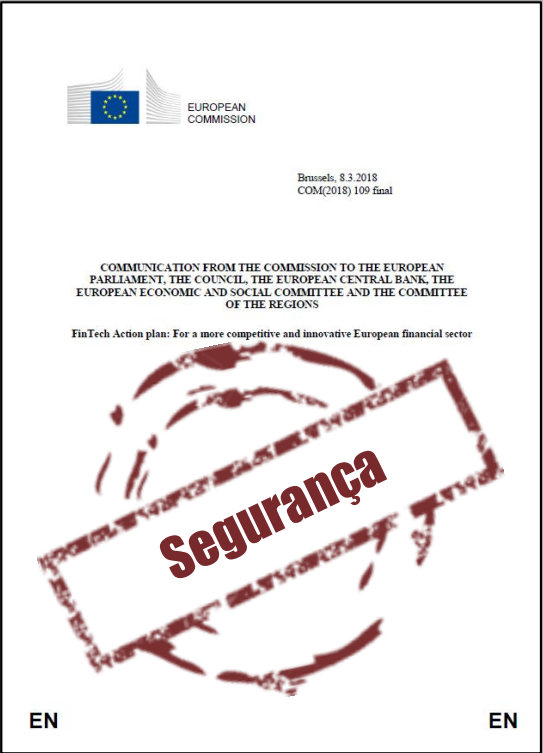


# A promoção da segurança tem sido uma preocupação do legislador europeu

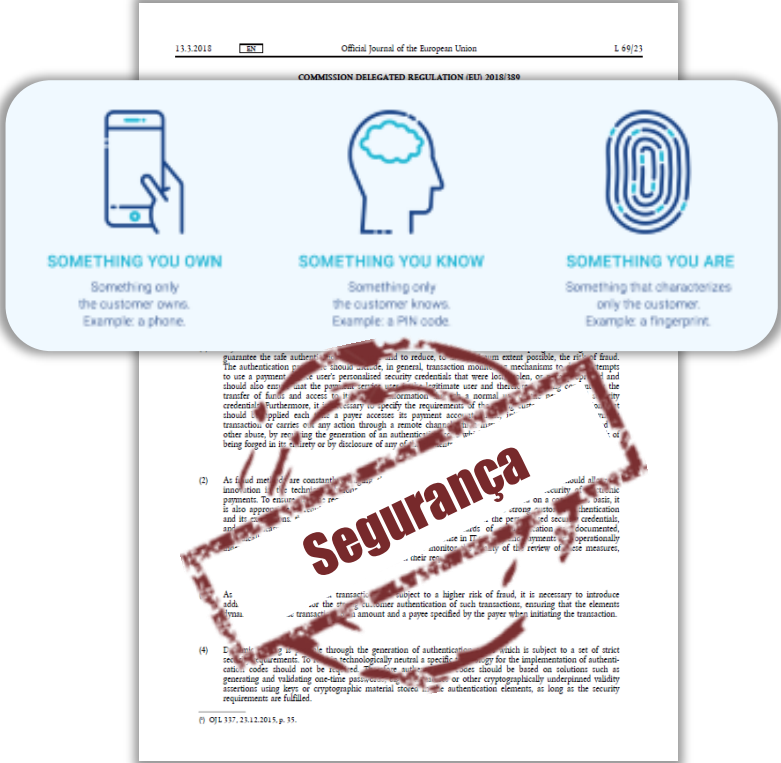
## PAYMENTS SERVICE DIRECTIVE 2 (PSD2)



## FINTECH ACTION PLAN

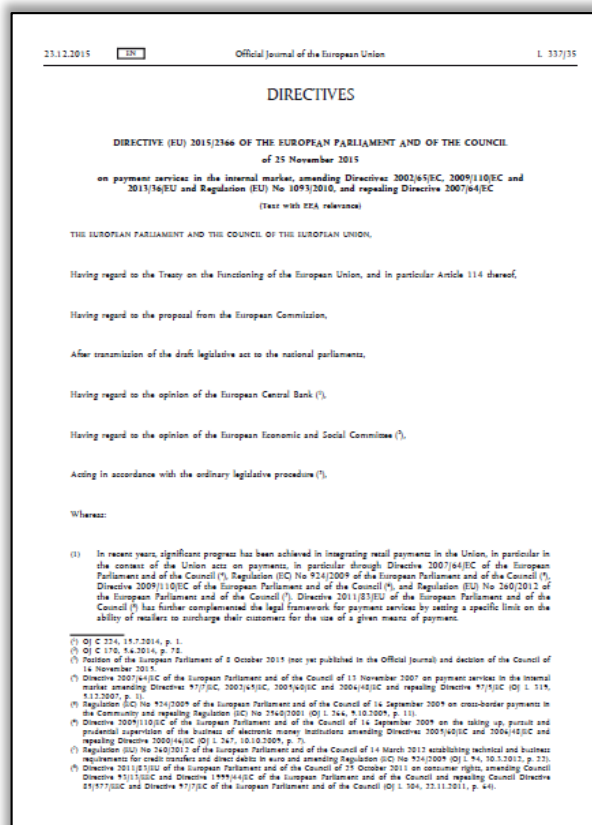


## REGULATORY TECHNICAL STANDARDS FOR STRONG CUSTOMER AUTHENTICATION



# A promoção da segurança é uma preocupação do legislador europeu

## DIRETIVA DOS SERVIÇOS DE PAGAMENTO 2



# A promoção da segurança é uma preocupação do legislador europeu



- Desde 2015, os prestadores de serviços de pagamento devem cumprir com os requisitos de **autenticação forte** definidos nas *EBA Guidelines on the security of internet payments*
- A DSP2 torna este cumprimento obrigatório
- ✓ *Serviços de pagamento seguros constituem “uma condição indispensável para o bom funcionamento do mercado de serviços de pagamento”*





# A promoção da segurança é uma preocupação do legislador europeu

---



Os prestadores de serviços de pagamento devem:

- Disponibilizar mecanismos de autenticação forte ao consumidor
- Reportar os incidentes de segurança
- Adotar medidas e mecanismos adequados à gestão do risco operacional e de segurança
- Dotar-se de mecanismos de deteção de pagamento não autorizados ou fraudulentos

*(Commission Delegated Regulation (EU)  
2018/389)*





### Publications

[FinCoNet Report on Digitalisation of Short-term, High-cost Consumer Credit: Guidance to Supervisors, 2019](#)

[FinCoNet Report on Digitalisation of Short-term, High-cost Consumer Credit, 2018](#)

[FinCoNet Report on Practices and Tools Required to Support Risk Based Supervision in a Digital Age, 2018](#)

[FinCoNet Report on Online and Mobile Payments: An Overview of Supervisory Practices to Mitigate Security Risks, 2018](#)

[FinCoNet Report on the Digitalisation of Short-Term, High-Cost Consumer Credit, 2017](#)

[Guidance to Supervisors on the setting of Standards in the field of Sales Incentives and Responsible Lending, 2016](#)

[FinCoNet Report on Online and Mobile Payments; Supervisory Challenges to Mitigate Security Risks, 2016](#)

[Impact of Sales Incentives on the Sale of Consumer Credit Products, 2016](#)

[FinCoNet Report on Sales Incentives and Responsible Lending, 2016](#)

[FinCoNet Report on Responsible Lending, 2014](#)

### Newsletters

[March 2019](#)

[December 2018](#)

[September 2018](#)

[May 2018](#)

[January 2018](#)

[November 2017](#)

[July 2017](#)

[March 2017](#)

[December 2016](#)

[July 2016](#)

[April 2016](#)

[December 2015](#)

[September 2015](#)

[May 2015](#)

[December 2014](#)

[October 2014](#)

[February 2014](#)

### Annual reports

[FinCoNet Annual Report 2017](#)

[FinCoNet Annual Report 2016](#)

[FinCoNet Annual Report 2015](#)

[FinCoNet Annual Report 2014](#)

<http://www.finconet.org/>





### Publications

FinCoNet Report on Digitalisation of Short-term, High-cost Consumer Credit: Guidance to Supervisors, 2019

FinCoNet Report on Digitalisation of Short-term, High-cost Consumer Credit, 2018

FinCoNet Report on Practices and Tools Required to Support Risk Based Supervision in a Digital Age, 2018

FinCoNet Report on Online and Mobile Payments: Overview of Supervisory Practices to Mitigate Security Risks, 2018

FinCoNet Report on the Digitalisation of High-Cost Consumer Credit, 2017

Guidance to Supervisors on the setting of Standards in the field of Sales Incentives and Responsible Lending, 2016

FinCoNet Report on Online and Mobile Payments: Supervisory Challenges to Consumer Protection, 2016

Impact of Sales Incentives on the Sale of Consumer Credit Products, 2016

FinCoNet Report on Sales Incentives and Responsible Lending, 2016

FinCoNet Report on Responsible Lending, 2014

### Newsletters

March 2019

December 2018

September 2018

May 2018

January 2018

November 2017

July 2017

December 2016

July 2016

April 2016

December 2015

September 2015

May 2015

December 2014

October 2014

February 2014

### Annual reports

FinCoNet Annual Report 2017

FinCoNet Annual Report 2016

FinCoNet Annual Report 2015

FinCoNet Annual Report 2014

A FinCoNet identificou os **riscos de segurança como uma importante ameaça** à proteção do consumidor financeiro

<http://www.finconet.org/>





Analisa os **principais desafios de supervisão** decorrentes dos riscos de segurança na utilização dos canais digitais, *online* e *mobile*



**Online and mobile payments:  
Supervisory challenges to  
mitigate security risks**

September 2016



Identifica **práticas de supervisão de conduta** para a **mitigação dos riscos de segurança** no contexto dos pagamentos digitais



**FinCoNet**  
INTERNATIONAL FINANCIAL CONSUMER  
PROTECTION ORGANISATION

**Online and mobile payments**

**An overview of supervisory practices to mitigate security risks**

January 2018

# DESAFIOS PARA A SUPERVISÃO COMPORTAMENTAL NA MITIGAÇÃO DOS RISCOS DE SEGURANÇA





## 1 Adequate legal and regulatory framework



- ✓ *The legal and regulatory supervisory framework should encompass **payment services** with a specific emphasis on **security principles and rules** to ensure consumer protection*
- ✓ *Conduct of business supervisors should have a clear mandate to oversee the mitigation of security risks and develop a risk-based methodology*
- ✓ (...)

## 2 Ongoing and comprehensive monitoring of the main risks



- ✓ *The **monitoring of the payments market** and its evolution should also be considered a task **to be pursued by conduct of business supervisors***
- ✓ *To this end, supervisors need to put in place different kinds of initiatives, with emphasis on **mandatory reports and/or surveys to PSPs***
- ✓ (...)

## 3 *Close cooperation between supervisors and other relevant entities*



- ✓ *The digitalization of the payments market compels to a **collaborative supervisory approach***
- ✓ *At the national level, conduct of business supervisors, prudential supervisors and payment overseers should work together to guarantee a secure, reliable and well-functioning payment system, while taking into consideration consumer protection*
- ✓ *Supervisors should also cooperate with the public administration, telecommunication operators, and cybersecurity agencies*
- ✓ *The **sharing of information is fundamental to reduce the vulnerabilities and better shield the national infrastructures from threats.***
- ✓ *Cross-border provision of payment services and the global nature of security threats call for **international cooperation***



## 4 Close supervision of PSPs' disclosure of information



- ✓ *PSPs should disclose information on the features of each payment service, their specific risks and the security procedures to be adopted by payment users*
- ✓ *Conduct of business supervisors should oversee the completeness and adequacy of the information ensuring that users can make enlightened decisions*
- ✓ (...)

## 5 Ongoing assessment of security risks through supervisory tools



- ✓ *The **evolving digital ecosystem brings new risks**, in particular security risks that also conduct of business supervisors need to address to ensure consumer protection*
- ✓ *Security risks are perceived as one of the most significant hurdles to the usage of digital financial services, in particular digital payments. **Conduct of business supervisors should have a wide range of oversight tools** based not only on inspections, but also on complaints handling*
- ✓ *The **use of complaints data** allows the supervision of security mechanisms adopted by PSPs. The effectiveness of the different oversight tools, especially complaints handling, requires an adequate regulatory framework within which conduct of business supervisors have the proper competences*

## 6 Promotion of awareness campaigns on security risks



- ✓ **Awareness campaigns** focusing on risks and security precautions to be adopted by users contributes to mitigate security risks with a positive effect on consumers' confidence
- ✓ Conduct of business supervisors may encompass the promotion of awareness campaigns on risks raised by digital payments under the scope of their mission
- ✓ Awareness campaigns may be launched by supervisors alone or in cooperation with other bodies, using different channels
- ✓ **Digital channels** (e.g. dedicated websites) may be considered an effective vehicle to widespread information on security risks to consumers

## 7 Promotion of digital financial literacy



- ✓ *The empowerment of users is also crucial to mitigate security risks*
- ✓ *Supervisors play a key role in promoting precautionary measures by users by engaging themselves in **financial literacy initiatives** even when they do not have a specific mandate to do so*
- ✓ *Conduct of business supervisors can also play an important role to further promote the adoption of precautionary attitudes and safety procedures by users cooperating with national literacy bodies*



# PRIVACIDADE DOS DADOS



A silver laptop is placed on a weathered wooden stump. From the screen, numerous US dollar bills of various denominations (including \$100 and \$50 bills) are falling out, floating in the air against a bright, cloudy sky. The scene is set outdoors, with a body of water visible in the background.

# “Is data the new CURRENCY?”

World Economic Forum, 2019





“*Big data*” refere-se a largo volume de dados resultantes de atividades conduzidas eletronicamente e de comunicações entre máquinas (e.g. *IoT, social media, financial markets data, ...*)

**3V** Volume  
Variedade  
Velocidade



O setor financeiro está entre os maiores utilizadores de dados

*“(...) data intensity (...) is highest in financial services (including securities and investment services and banking (...))”*

*(Data-Driven Innovation: Big Data for Growth and Well-Being, OECD (2015))*





# “Should our bankers and insurers be our Facebook friends?”

The Economist, 2017

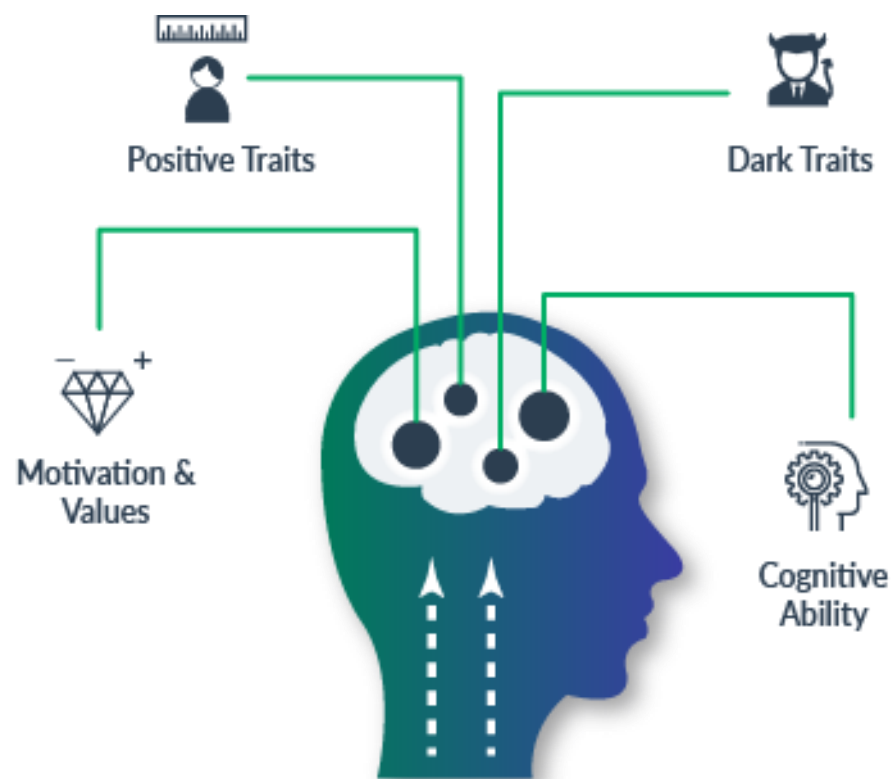
“FICO, America’s main credit-scorer, found that the **words** someone uses in his Facebook status could **help predict his creditworthiness** (tip: avoid “wasted”)



“The education levels of your **Facebook friends** or the **activity on your phone** can help reveal how likely you are **to repay a loan**. Money-managers are rummaging ever more curiously through customers’ digital lives.”



# Psychometric tests



“Lenddo EFL, a merger of two fintech startups, provides **“PSYCHOMETRIC TESTING”** – online quizzes that have a surprisingly good record in predicting a prospective **borrower’s propensity to pay**”

The Economist, 2018



39%

dos consumidores aceitaria disponibilizar o seus dados pessoais online em troca de benefícios

*The Kaspersky Lab Global Privacy Report 2018, Kaspersky*

*When using the Internet for online banking or shopping, the two most common concerns are about someone misusing personal data (mentioned by 43% of Internet users in the EU) and security of online payments (42%) EC (2015), Special Eurobarometer 423 Cyber Security - Report*





- Os consumidores disponibilizam dados pessoais permanentemente e muitas vezes de forma inconsciente
- O volume desses dados é cada vez mais significativo e o desenvolvimento tecnológico permite hoje agregar e analisar esses dados (e.g. Inteligência Artificial)
- Os prestadores de serviços financeiros utilizam-nos:
  - ✓ Na **segmentação** dos consumidores (*profiling*)
  - ✓ Na avaliação do seu **risco** (e.g. de **crédito**)
  - ✓ Na **agregação de contas**
  - ✓ ....





JC/2018/04  
15 March 2018

## Joint Committee Final Report on Big Data

### ***Report on Big Data (ESAs)***

Analisa os **potenciais benefícios e riscos** da utilização de *Big Data*

### **Report on innovative uses of consumer data by financial institutions**

28 June 2017

### ***Report on innovative uses of consumer data by financial institutions (EBA)***

Analisa **riscos e benefícios** de  
utilizações inovadoras de dados



# Riscos no uso da *Big Data*

- Incompreensão ou falta de informação quanto à finalidade dos dados
- Utilização dos dados distinto do divulgado
- Personalização dos serviços: difícil comparação de preços; preço em função de comportamentos
- Exclusão financeira
- Modelos de IA (“caixas pretas”; “as máquinas também erram”)
- ...



## “(….)Financial exclusion associated with artificial intelligence and data-driven algorithms:

- ✓ *“(….) By using Big Data, financial institutions can collect extensive information about customers and their risk profiles and therefore proceed with a risk micro-segmentation/refined credit scoring or a refined assessment of the suitability of an investment (...)*

*EBA Discussion Paper on FinTech (2017)*



# “Why it matters to consumers”:



- *Financial firms increasingly use **big data**, (...) while this evolution comes with some potential benefits for consumers (...) it also triggers **huge questions on privacy, fairness, and exclusion***
- *“(...) **supervisory authorities should be monitoring the potential detriment of the use of big data closely***
- *Potential policies approaches include **prohibiting the use of certain parameters in big analytics** which are highly prone to consumer detriment (...)”*





I

(Legislative act)

## REGULATIONS

## Regime Geral de Proteção de Dados (RGPD)

Assegura aos cidadãos **maior controlo sobre os seus dados pessoais**, nomeadamente quanto ao seu **acesso, processamento e utilização**

(1) OJ C 329, 31.7.2012, p. 90.

(2) OJ C 391, 18.12.2012, p. 137.

(3) Position of the European Parliament of 13 March 2014 (not yet published in the Official Journal) and position of the Council at first

reading of 8 April 2016 (not yet published in the Official Journal), Position of the European Parliament of 14 April 2016.

(4) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to

the processing of personal data and on the free movement of such data (Data Protection Directive).



## *Ethics Guidelines for Trustworthy AI*

Visam **promover a confiança** na inteligência artificial, que deve ser ***lawful, ethical e robust***

## ETHICS GUIDELINES FOR TRUSTWORTHY AI



✓ *“The implications of the use of personal data for financial services consumers”*

- OECD Working Paper discutido na 11ª reunião do OECD /INFE Technical Committee e na 5ª reunião do OECD /INFE Working Group on Digital Financial Literacy

(Cape Twon, 21-22 de maio 2019)





# QUAL O CONTRIBUTO DO SUPERVISOR DE CONDUTA?





*“(...) as instituições recorrem aos canais digitais para a prestação de serviços e aos dados dos clientes para a identificação dos seus perfis de consumo e de risco.*

*Assim, num contexto em que a oferta de produtos e serviços bancários de retalho tende a assentar, cada vez mais, em canais digitais, em que surgem novos produtos e serviços, oferecidos, frequentemente, por novos prestadores e com diferentes modelos de negócio, a regulação e a **supervisão comportamental** têm de encontrar as respostas adequadas a que o processo de inovação tecnológica e o ambiente digital floresçam com segurança e garantia dos direitos dos consumidores, pois só assim ficarão criadas condições para maximizar os ganhos que podem gerar.(...)”*

Nota de abertura do  
Relatório de Supervisão Comportamental de 2017,  
Vice-Governador, Dr. Luís Máximo dos Santos





# O Banco de Portugal está atento aos procedimentos de segurança adotados



- Desde 2018, as instituições reportam **informação sobre os créditos** comercializados nos canais digitais, incluindo sobre **mecanismos de segurança adotados** (Carta-Circular n.º 4/2018)
- As **ações de inspeção** avaliam o cumprimento do quadro normativo, com enfoque nos **procedimentos de segurança**
- As instituições são chamadas a adotar **mecanismos de segurança robustos** para a celebração dos contratos de crédito



## O Banco de Portugal está atento aos procedimentos de segurança adotados

**Quadro II.2.5 • Ações de monitorização da comercialização de contratos de crédito aos consumidores nos canais digitais por matéria e tipo de crédito | 2018**

Matérias	Crédito pessoal	Facilidade de descoberto	Total	Instituições abrangidas
Informação pré-contratual e contratual	12	2	14	13
Venda facultativa de produtos	12	2	14	13
Dever de assistência ao consumidor	12	2	14	13
Avaliação da solvabilidade	12	2	14	13
Direito de livre revogação e direito ao reembolso antecipado	12	2	14	13
<b>Procedimentos de segurança</b>	<b>12</b>	<b>2</b>	<b>14</b>	<b>13</b>
<b>Total</b>	<b>72</b>	<b>12</b>	<b>84</b>	<b>-</b>

Fonte: Banco de Portugal. | Nota: O número de ações de inspeção é determinado pelos produtos e serviços bancários inspecionados e respetivas matérias por instituição. Foram inspecionadas 13 instituições.



## ...monitoriza a comercialização dos produtos e serviços bancários nos canais digitais



- ✓ As preocupações com a **segurança**, o **desconhecimento das novas tecnologias** e a **falta de literacia financeira** dos clientes são apontados pelas instituições como os principais obstáculos à expansão dos canais digitais

As instituições reconhecem a importância da **educação financeira digital**



... e promove a informação e formação financeira digital

# 5 DICAS PARA FICARES MAIS SEGURO ONLINE

## #ficaadica

A campanha **#ficaadica** visa sensibilizar os jovens para as precauções a tomar quando utilizam os canais digitais

Esta campanha, lançada nas redes sociais (Instagram) e no Portal do Cliente Bancário foi também publicada numa brochura distribuída pelas escolas secundárias de todo o país







O Banco de Portugal desenvolve  
campanhas com alertas para os  
consumidores e vai passar a divulgar  
informação referente à segurança digital  
num **novo espaço** do Portal do Cliente  
Bancário



# Segurança digital

Faça operações bancárias e compras na internet e nas apps em segurança

SABER MAIS



Consulta de  
preçários



Comparador de  
comissões



Simular crédito à  
habitação



Intermediários  
de crédito



Segurança digital



# Muito obrigada

**Maria Lúcia Leitão**  
**Diretora do Departamento de Supervisão**  
**Comportamental**

**[mleitao@bportugal.pt](mailto:mleitao@bportugal.pt)**



**BANCO DE  
PORTUGAL**  
EUROSISTEMA