


Aspetos Profissionais e Sociais da Engenharia Informática

Security issues and challenges

Rui L Aguiar, UA/IT

1




Covered aspects....

- AI
 - Market, technology, what is "IA"
- Open source models, trabalhos derivados
- Marcas, IPR
- Standards
- Dilemas de personalidade – tempo e constância.
- Applied AI issues: autonomous driving and decisions
- Cybersecurity – what is it and what is the impact
- Cybercrime
 - Employment and information leakage

2

2



Today....

- Reputation
- Legal intercept
- Cybermarket
- GPDR

3

3



CYBERSECURITY


4



AQUI

REPUTATION AT STAKE

5



Types of Data Breaches

The Hacking Attack

1

- ◆ Cybercriminals break into a company's computer system and steal data.

The Accidental Data Leak

2

- ◆ An employee accidentally sends sensitive data to the wrong person or posts it online where anyone can access it.

The Inside Job

3

- ◆ A company employee steals data for their gain.

6



Prevent a Data Breach

- Restrict access to sensitive information to only those who need it.
- Install a firewall
- Install antivirus software on your computer.
- Keep software up to date.
- Regularly back up data.
- Impose password policies
 - strong passwords
 - change them regularly.
 - Don't use the same password for different accounts.
- Educate employees
 - Beware of spear-phishing attacks, emails that appear to be from a trusted source but are designed to steal your information.
 - Do not open attachments or click on links in.
 - Install a security plugin on your browser.
 - Be careful about what information you share online.

7

7



Post-Data Breach Reputation Recovery Checklist



- 1 Be the first source to break the news
- 2 Engage in threat-sharing
- 3 Implement a robust notification plan
- 4 Hire a CISO and other security professionals
- 5 Be transparent enough with all parties involved
- 6 Regularly measure and report on your cybersecurity improvements

8

8

CyberReputation Recovery

- Be honest and upfront with customers and LE
 - Explain what happened,
 - Solutions being taken
 - Action for them to protect themselves.
- Improve your security.
 - Ensure your systems are up-to-date
 - “force” your employees to follow best practices.
- Establish a trust relation with your customers.
 - Tell them actions you're taking to protect their data,
 - remind them that you're a reputable company.

9

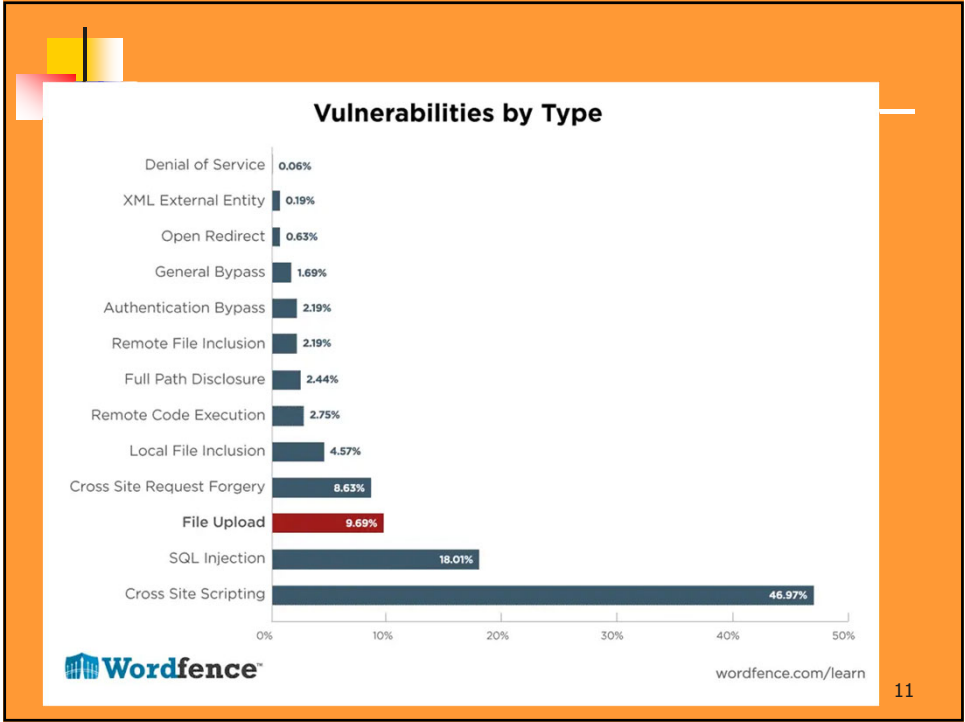
Snowflake attack and resolution

UNC5537 Campaign Timeline

APR 14	APR 17	APR 19	MAY 14	MAY 22	MAY 24	MAY 30	JUN 2
Earliest evidence of access to Snowflake customer instances	Earliest evidence of FROSTBITE usage	Mandiant begins investigating data stolen from an unknown database	Mandiant identifies multiple impacted Snowflake customer instances	Mandiant notifies Snowflake and Law Enforcement of ongoing campaign targeting multiple customer Snowflake instances	Earliest advertisement of Snowflake customer Data for sale on cybercrime forums	Snowflake publishes statement and guidance	Joint statement from Snowflake, Mandiant, and CrowdStrike regarding the ongoing investigation

```
graph TD; A[Infostealer Malware] --> B[Acquired Snowflake Credentials from Infostealer Logs]; B --> C[Login with Stolen Snowflake Credentials]; C --> D[Snowflake Customer Instance]; D --> E[Database & External Storage Breach]; E --> F[Exfiltration]; G[Customer Personal Devices] --> B;
```

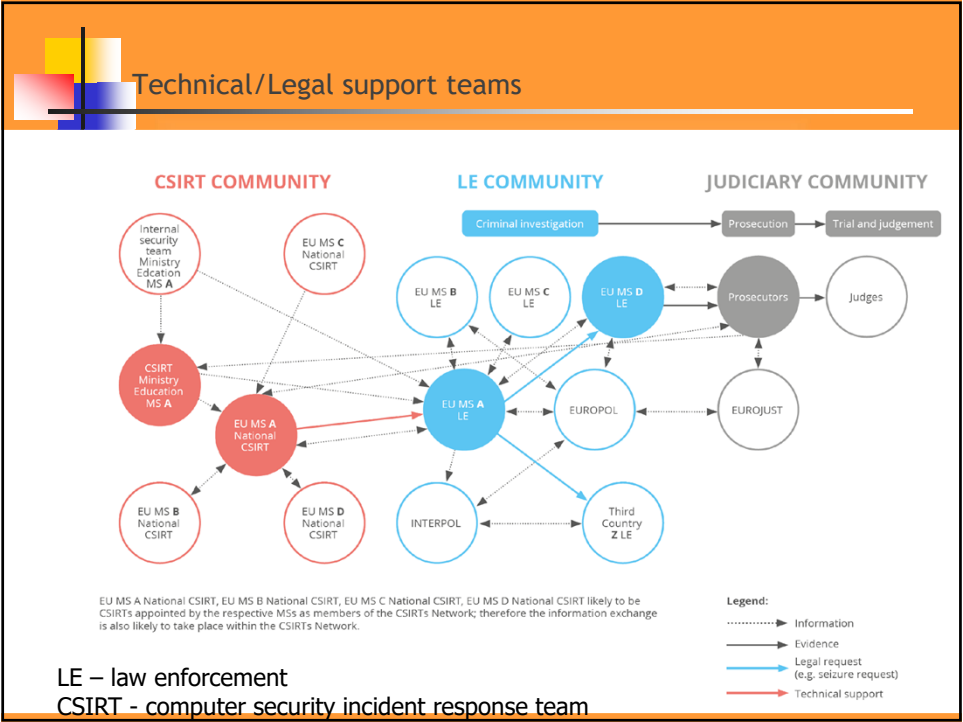
10

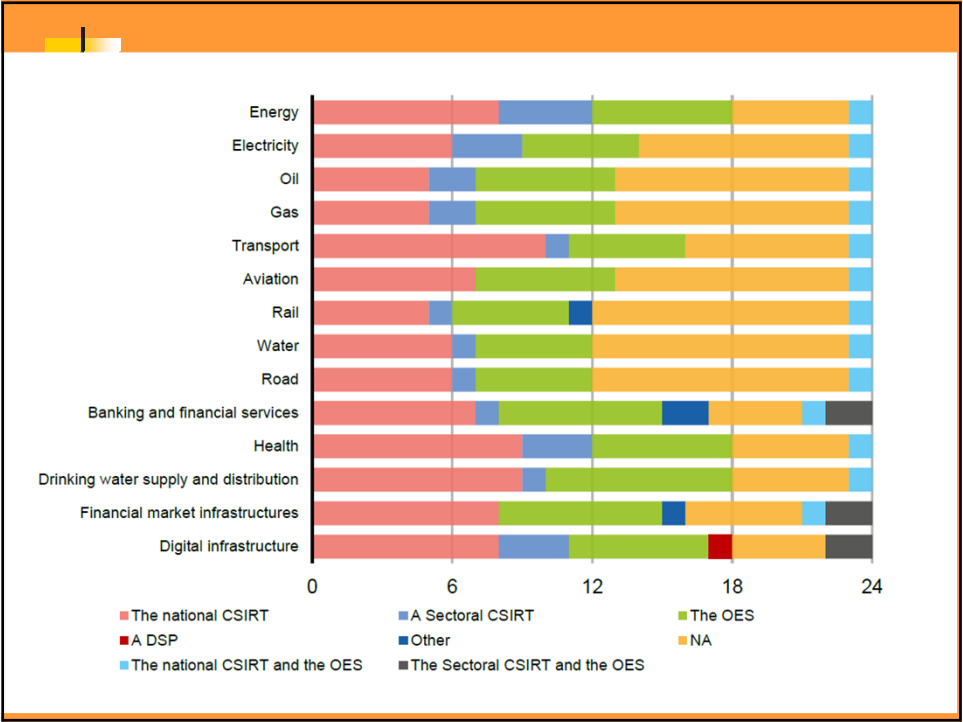


11



12





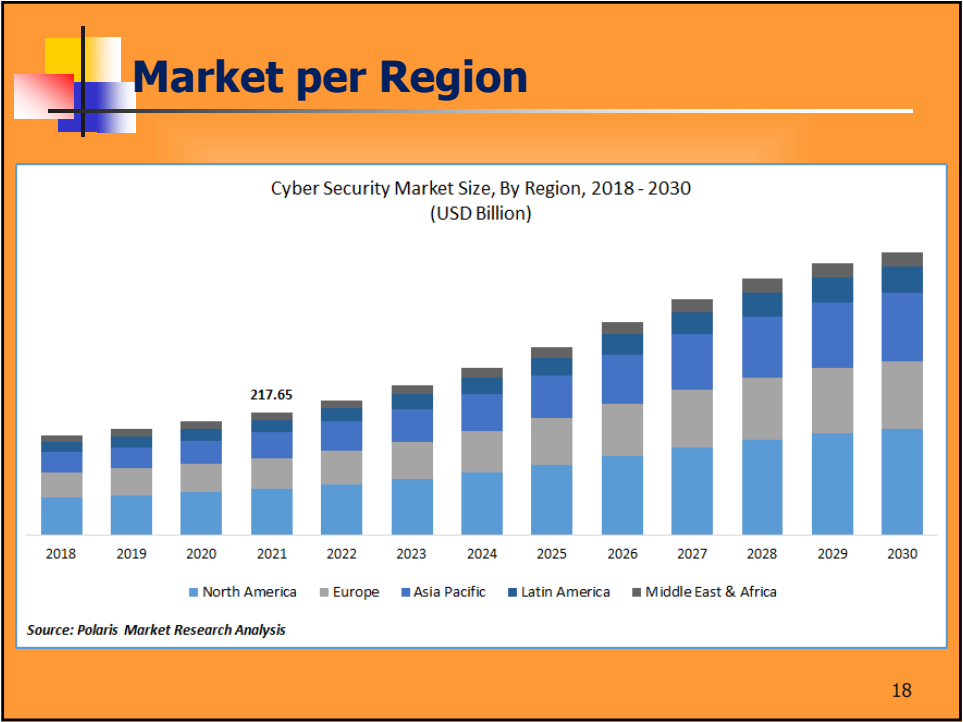
15

CYBERSECURITY MARKET & ECOSYSTEM

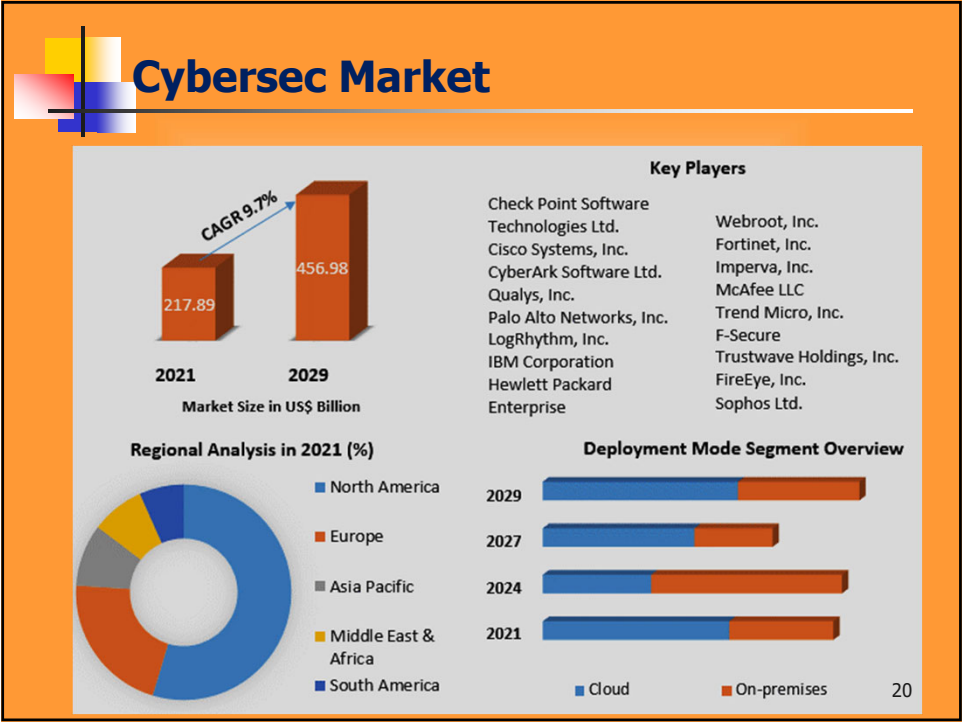
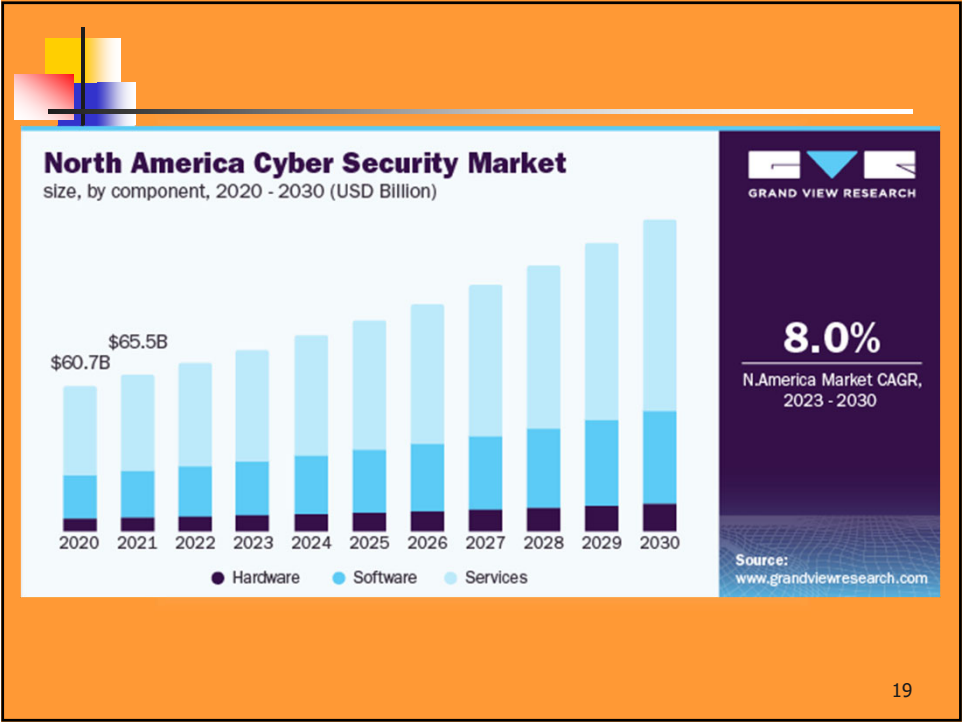
16

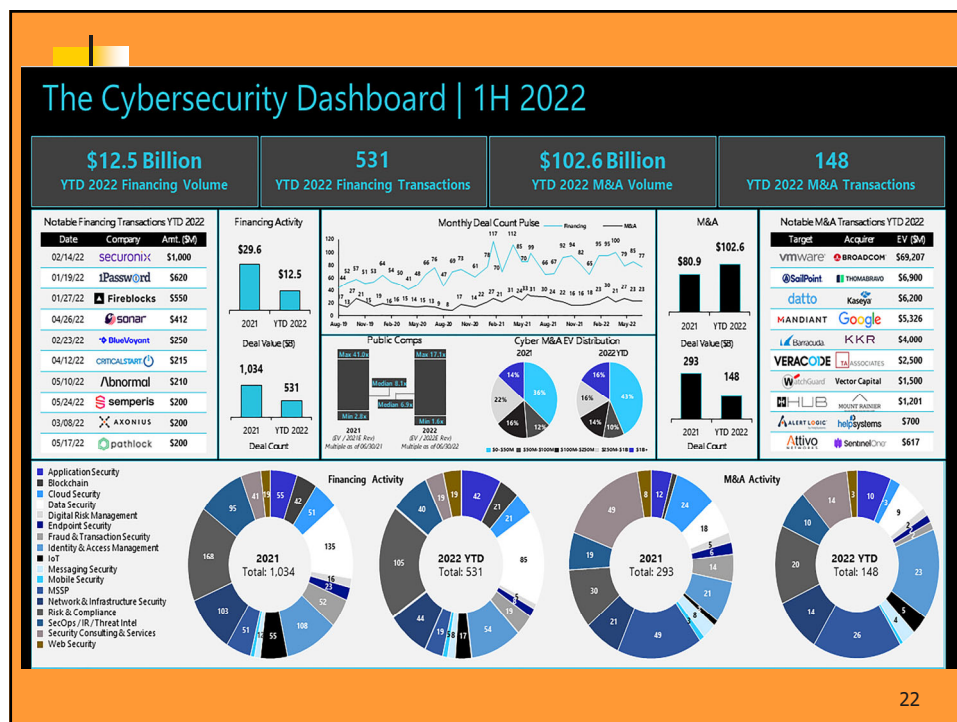
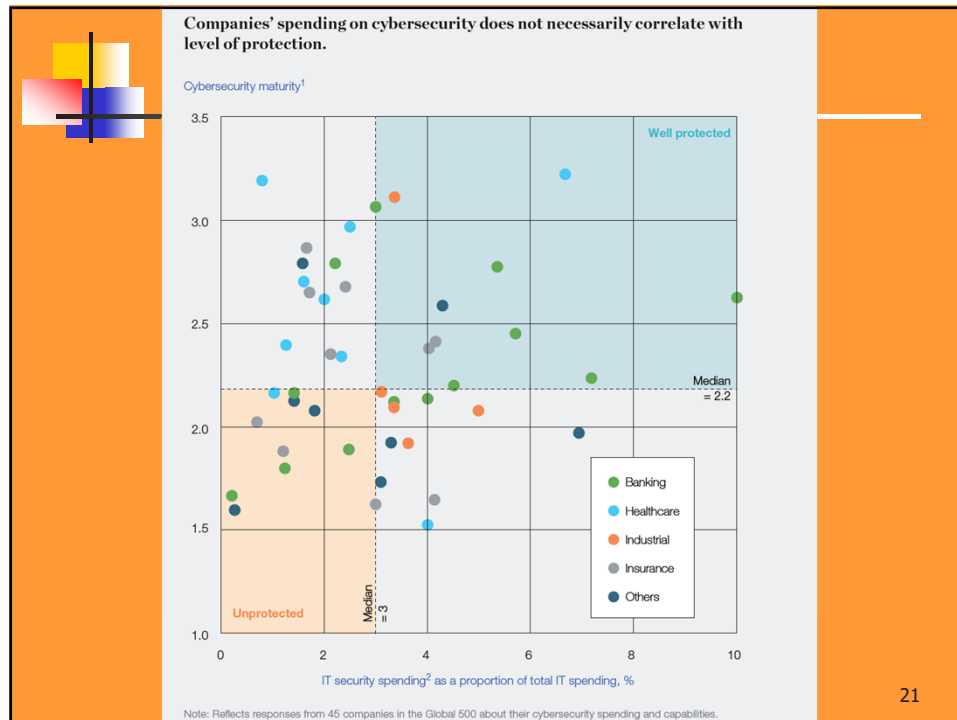


17



18





What does a Cyber Security Professional look like?

23

In reality...

Eugene Kaspersky, CEO Kaspersky Labs, £1.1bn

David Ulevitch, Founder OpenDNS

Katie Moussouris, Microsoft Bug Bounty creator

James Lyne, CTO, SANS

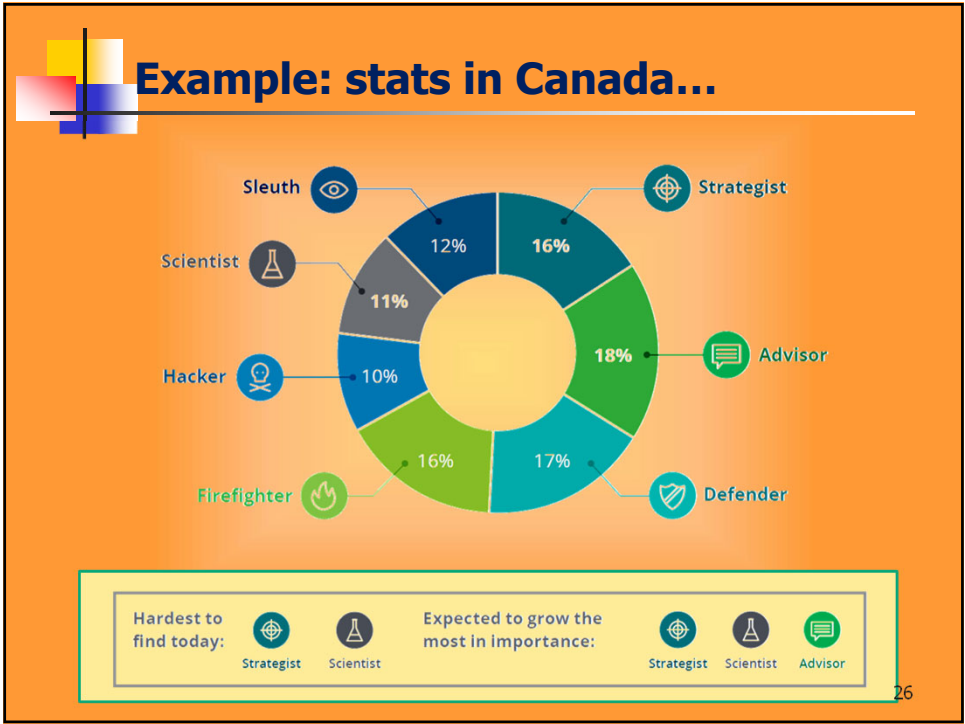
Erin Jacobs, CSO at UCB Financial Services

Dr Laura Toogood, MD Digitalis Reputation

24



25



26

ENISA

european union agency for cybersecurity

Figure 2: Overview of ENISA's work in the area of CSIRTs and LE cooperation

2012: ENISA-Europe Workshop for CSIRTs and LE, Good Practice Guide for Addressing Cybercrime - No Aspects of Cybercrime (2012)

2013: Annual ENISA-EC3 Workshop for CSIRTs and LE, The fight against Cybercrime - A first collection of practices (2013)

2014: Cooperation in the area of Cybercrime - Addressing its Cyber Crime Cases (2014) Handbook - Toolkit, Electronic evidence - A basic guide for first responders (2014)

2015: Annual ENISA-EC3 Workshop for CSIRTs and LE, Information sharing and common scenarios between CSIRTs and LE (2015)

2016: Annual ENISA-EC3 Workshop for CSIRTs and LE

2017: Annual ENISA-EC3 Workshop for CSIRTs and LE, Tools and Methodologies to Support Cooperation between CSIRTs and LE (2017)

2018: Annual ENISA-EC3 Workshop for CSIRTs and LE, Improving Cooperation between CSIRTs and LE (2018)

2019: Annual ENISA-EC3 Workshop for CSIRTs and LE, Cooperation between CSIRTs and LE: Interaction with the judiciary (2019), Roadmap on the enhancing technical cooperation between CSIRTs and LE (2019)

2020: Annual ENISA-EC3 Workshop for CSIRTs and LE, An overview on enhancing technical cooperation between CSIRTs and LE (2019)

2021: Annual ENISA-EC3 Workshop for CSIRTs and LE, 2020 Report on CSIRT-LE Cooperation

2022: Annual ENISA-EC3 Workshop for CSIRTs and LE, 2021 Report on CSIRT-LE Cooperation

CSIRT - computer security incident response team
LE – Law enforcement

- Implements NIS (Directive (EU) 2016/1148), NIS2 (Directive (EU) 2022/2555) and Cybersecurity toolbox.

Privacidade e Proteção de Dados

Regulamento Europeu de Proteção de Dados (UE) 2016/679
+ Lei Nacional 58/2019

Slides based in:

Fernando Ferreira Batista

universidade de aveiro

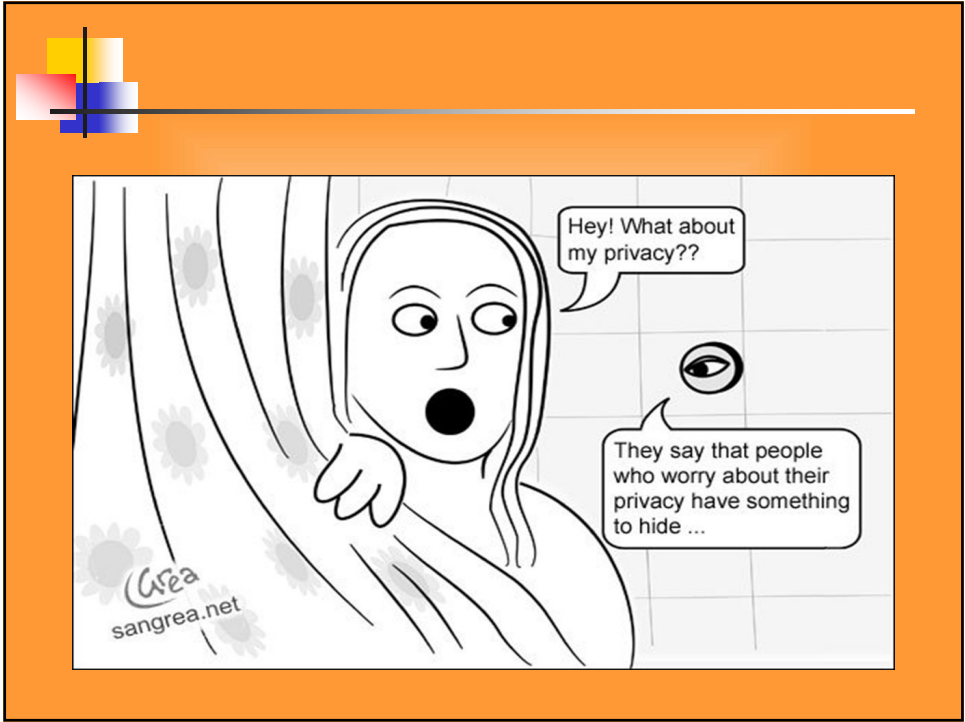
Maashik University

ECPC-B

Certified Data Protection Officer

32

15



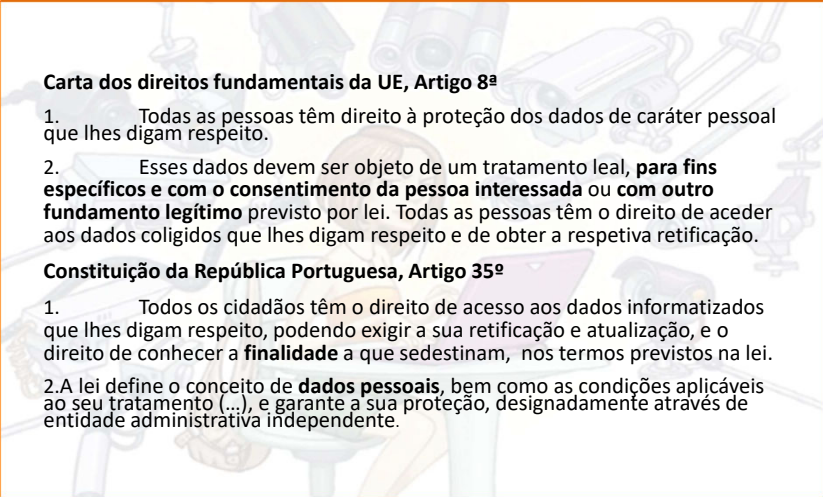
33

Privacidade: valor intrínseco ou instrumental?

- Permite estabelecer laços com outras pessoas, impossíveis de estabelecer de outra forma?
- Essencial para a *autonomia* (Johnson)
- *Valores nucleares*? Embora em expressões diferentes, partilhados e presentes de alguma forma em culturas diversas
- Como expressão do valor nuclear da **segurança**, representa um *bemintrínseco* numa sociedade informatizada e ligada em rede
- Cidadãos têm o direito de ser *protegidos*, o que inclui a **proteção da privacidade e dos seus dados de carácter pessoal**

34

Privacidade e proteção de dados como direitos



Carta dos direitos fundamentais da UE, Artigo 8º

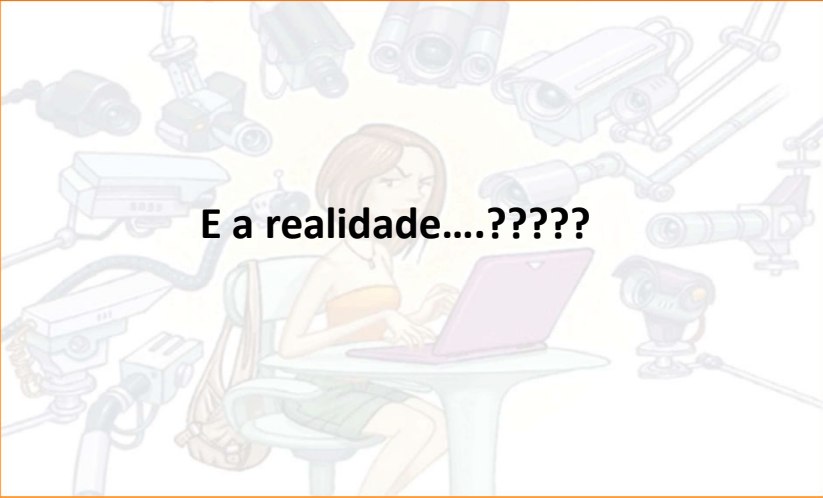
1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.
2. Esses dados devem ser objeto de um tratamento leal, **para fins específicos e com o consentimento da pessoa interessada** ou **com outro fundamento legítimo** previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.

Constituição da República Portuguesa, Artigo 35º

1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a **finalidade** a que se destinam, nos termos previstos na lei.
2. A lei define o conceito de **dados pessoais**, bem como as condições aplicáveis ao seu tratamento (...), e garante a sua proteção, designadamente através de entidade administrativa independente.

35

Privacidade e proteção de dados como direitos



E a realidade....?????

36

Amazing mind reader reveals his 'gift'

<https://youtu.be/V7UoX5EuedU>

de acordo com a realização:

- é um “clip” de uma encenação “vidente” para um suposto “novo programa de televisão”, realizada no centro de Bruxelas com pessoas aleatoriamente escolhidas para que lhes fosse “lida a mente”, mas tendo em vista, afinal, alertar utilizadores de serviços bancários online, numa campanha com o título Sejam Vigilantes!

37

A Proteção de dados na UE e em Portugal: RGPD

Regulamento (EU) 2016/79 do Parlamento Europeu e do Conselho – **Regulamento Geral de Proteção de Dados**

- Defender os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção de dados, 1.º/2; e
- Promover a livre circulação dos dados pessoais, 1.º/3.

38

A Proteção de dados na UE e em Portugal: RGPD

Regulamento (EU) 2016/79 do Parlamento Europeu e do Conselho – **Regulamento Geral de Proteção de Dados**


- Em vigor desde Maio de 2018
- Regulamento do Direito Europeu: não necessita transposição, aplica-se diretamente a todos os estados membros
- Deixa algumas cláusulas abertas, reguladas por legislação nacional – Lei 58/2019, de Execução do RGPD

39



O RGPD na sua essência ...

40



1. Introdução ao Regulamento (EU) 2016/679
2. Direitos do titular dos dados
3. Obrigações dos responsáveis pelo tratamento
4. Legislação Nacional vs Regulamento

Informação dos slides para ser lida em casa, como material de estudo

Regulamento Europeu Proteção de Dados

Proteção de dados como direito fundamental

A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental.

- artigo 8.º, n.º 1, da **Carta dos Direitos Fundamentais da União Europeia** («Carta»)
- artigo 16.º, n.º 1, do **Tratado sobre o Funcionamento da União Europeia** (TFUE)

"Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito"

Regulamento Europeu Proteção de Dados

Introdução ao Regulamento (EU) 2016/679

Desde o dia 04 de Maio de 2016 que a União Europeia tem um novo quadro normativo para a Proteção de dados, estabelecendo as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. O Regulamento* entrou em vigor no dia 25 de Maio de 2018.

O regulamento aplica-se:

- em todo o território da União Europeia.
- a todas as empresas e entidades públicas que tratem dados pessoais.
- ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados.
- ao tratamento de dados, de residentes no território da União, efetuado por um responsável não estabelecido na União.

▪ -> [\(edpb_guidelines_3_2018_territorial_scope_pt.pdf\)](#)

- entidades subcontratadas.


* (deriva da anterior Diretiva Europeia 95/46 CE de 1995)

43


Regulamento Europeu Proteção de Dados

Introdução ao Regulamento (EU) 2016/679


REGULAMENTO GERAL PROTEÇÃO DE DADOS (UE) 2016/679




Harmonização



Proteção



Transparência



Menor burocracia

44

Regulamento Europeu Proteção de Dados

Definições

Para efeitos do presente regulamento, entende-se por:

Responsável pelo tratamento

Pessoa singular ou coletiva que, individualmente ou em conjunto com outras, ~~fidelidade~~ **define** os meios de tratamento de dados pessoais.

Subcontratante

Uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo **que trate os dados pessoais por conta do responsável pelo tratamento destes**

Violação de dados pessoais

Uma violação que provoque, de modo accidental ou ilícito a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

Autoridade de Controlo

Uma autoridade pública independente criada por um Estado-Membro.
CNPD em Portugal; CNIL na França
ICO na Inglaterra – fora da UE, mas existe uma decisão de adequação;
Etc

Art. 4º Regulamento (UE) 2016/679

45

Regulamento Europeu Proteção de Dados

O que são dados pessoais?

Todos e quaisquer dados relativos a pessoas singulares identificadas ou identificáveis, direta ou indiretamente, como por exemplo o nome, morada, e-mail, idade, estado civil, dados de localização, genéticos, fisiológicos, económicos, culturais, sociais ou identificadores por via eletrónica.

Nome

Morada

Localização

Identificador em linha

Informação de saúde

Rendimento

Perfil cultural


entre outros

46


22

Regulamento Europeu Proteção de Dados


Categorias Especiais de Dados Pessoais(sensíveis)




Origem étnica




Origem racial




Opiniões políticas




Convicções religiosas




Convicções filosóficas




Filiação sindical




Dados genéticos




Dados biométricos



Saúde



Vida sexual



Orientação sexual


Reserva de Intimidade da Vida Privada e Familiar


Situação económica

Videovigilância

Dados de Geolocalização

Condenações Penais


 Art. 9º Regulamento (UE) 2016/679

 Constituição Republica Portuguesa


47

Regulamento Europeu Proteção de Dados


Categorias Especiais de Dados Pessoais




Origem étnica




Origem racial




Opiniões políticas




Convicções religiosas




Convicções filosóficas




Filiação sindical




Dados genéticos




Dados biométricos



Saúde



Vida sexual



Orientação sexual


Reserva de Intimidade da Vida Privada e Familiar


Situação económica

Videovigilância

Dados de Geolocalização

Condenações Penais

 Art. 9º Regulamento (UE) 2016/679

 Constituição Republica Portuguesa

proibição de tratamento dados especiais

48

23

Regulamento Europeu Proteção de Dados

Princípios do Regulamento -> Categorias de dados especiais

A proibição não se aplica quando se verificar um dos seguintes casos:

Se o titular dos dados tiver dado o seu consentimento explícito (exceto a lei proibir)	Cumprimento de obrigações/exercício de direitos específicos de RdTou dotitular
Proteger os interesses vitais do titular dos dados	Por um organismo sem fins lucrativos e com fins políticos, filosóficos, religiosos ou sindicais (aos seus elementos)
A dados pessoais que tenham sido manifestamente tornados públicos	Necessário à declaração, ao exercício ou à defesa de um direito
Necessário por motivos de interesse público	Necessário para efeitos de medicina preventiva ou do trabalho
Interesse público no domínio da saúde pública	Necessário para fins de arquivo de interesse público, estatístico, científico ou histórico

49

Regulamento Europeu Proteção de Dados

O que são dados pessoais?

- O retrato físico de uma pessoa (fotografia ou outro) e registos de voz ou vídeo **são dados pessoais**
- Assunção a partir de um retrato físico de características possivelmente categorizáveis como dados especiais (e.g. a etnia a partir da cor), implica de tais assunções estar-se perante tratamento de dados sensíveis?
 - **Não**, salvo se houver tratamento de informação

E.g. Tratamento de fotografias por meios tecnológicos e que permitam a identificação inequívoca ou a autenticação de pessoa, corresponde a tratamento de dados biométricos, e bem assim dados sensíveis.

50

Regulamento Europeu Proteção de Dados

Anonimização

▪ Aplicação de técnicas de conversão de dados pessoais em dados anónimos, e.g. a supressão de atributos, a codificação, a generalização ou introdução de ruído.

▪ Se a finalidade de tratamento é possível com dados anonimizados, os dados têm que ser anonimizados.

Se adequadamente anonimizados, ficam fora do âmbito do RGPD!

▪ Se investigador recolher dados pessoais e só posteriormente os anonimizar, os dados brutos iniciais ainda são pessoais e devem ser tratados como tal.

e.g. dados de transcrição de entrevistas gravadas, ainda que subtraída de informações de identificação pessoal, não se traduz em anonimização, até que os dados brutos sejam destruídos.

51

Regulamento Europeu Proteção de Dados

Anonimização e re-identificação

▪ O RGPD aplica-se a dados pessoais; se os dados estão (adequadamente) anonimizados o quadro legal não se aplica.

▪ Mas... com a emergência do *big data* estudos mostram que pessoas podem ser re-identificadas a partir de dados anónimos e.g. usando apenas o código postal, data de nascimento e sexo, com 87% de precisão (Gumbus e Grodzinsky 2016)

52

Regulamento Europeu Proteção de Dados

Anonimização e re-identificação

<https://www.kdnuggets.com/2016/03/netflix-prize-analyzed-movie-ratings-recommender-systems.html>

- caso Netflix Prize Dataset

<https://www.kdnuggets.com/2016/03/netflix-prize-analyzed-movie-ratings-recommender-systems.html>

- ~500.000 registos anónimos de classificações de filmes
- Objetivo era fomentar investigação científica...
- ... e fomentar propostas de algoritmos capazes de prever filmes
- Dois investigadores - Arvind Narayanan e Vitaly Shmatikov – cruzaram os dados com perfis públicos no IMBD (The Internet Movie Database)
- Apenas algumas preferências ($2 \leq \text{filmes} < 8$) mostraram ser suficientes para realizar re-identificação
- Outras informações pessoais sensíveis foram inferidas, tais como orientação política...

PREDICTING MOVIE RATINGS AND RECOMMENDER SYSTEMS

Arvind Narayanan

★★★★★

53

Regulamento Europeu Proteção de Dados

Pseudonimização

Tratamento de dados de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a **informações suplementares**, e desde que essas **informações suplementares** sejam mantidas separadamente e sujeitas a medidas para assegurar que os dados não possam ser atribuídos a uma pessoa singular:

- Projetos onde a anonimização compromete finalidades, sendo necessário manter um vínculo entre os sujeitos da investigação e os dados pessoais.
- Não remove o carácter pessoal dos dados.**

54

Regulamento EuropeuProteção de Dados

Actividades de Tratamento

Operação ou um conjunto de operações efetuadas sobre dados pessoais, por meios automatizados ou não automatizados:

Recolha	Adaptação ou Alteração
Registo	Recuperação
Organização	Consulta
Estruturação	Utilização
Conservação	Divulgação por transmissão
Comparação ou Interconexão	Apagamento ou Destruição

55

Regulamento EuropeuProteção de Dados

“Direito” ao consentimento

«Consentimento» do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento;

Condições aplicáveis ao consentimento

- Quando o tratamento for realizado com base no consentimento, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais.
- Há que verificar se a execução está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato
- O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado.
- Caso a criança tenha menos de 16 anos (em Portugal e por via da Lei 58/2019 a idade mínima foi estabelecida nos 13 anos), o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança.

56


Regulamento Europeu Proteção de Dados

“Direito” ao consentimento AQUI

Normalmente obtido sob a forma de declaração escrita, com referência à Informação ao Titular, e pode ser recolhido por meios eletrónicos, por exemplo:

(1)Consinto em que os meus dados pessoais sejam utilizados no âmbito do projeto de investigação *[identificar qual o projeto de investigação]* de acordo com a finalidade e demais informações que me foram disponibilizadas na Informação supra:

Sim ☐ Não ☐



Somente após a disponibilização da Informação ao Titular e obtida a sua manifestação positiva de consentimento podem os dados ser tratados (incluindo a recolha).