DATA BREACH E SICUREZZA INFORMATICA: La segnalazione delle violazioni tra GDPR e D.Lgs. 65/2018

Perugia, 9 ottobre 2018

ARRAY

Avv. Francesco Paolo **Micozzi**

Di cosa si occupa il GDPR?

La valutazione del rischio… quale rischio?

"I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale"

RISCHIO = PROBABILITÀ x DANNO MASSIMO IPOTIZZABILE

$$R=PxD$$

Potenziali danni derivanti da trattamento di dati personali:

- **danno fisico**
- **danno materiale**
- **danno immateriale**

Security

is a state of mind!

Secure

Secure?

World's Biggest Data Breaches

Selected losses greater than 30,000 records

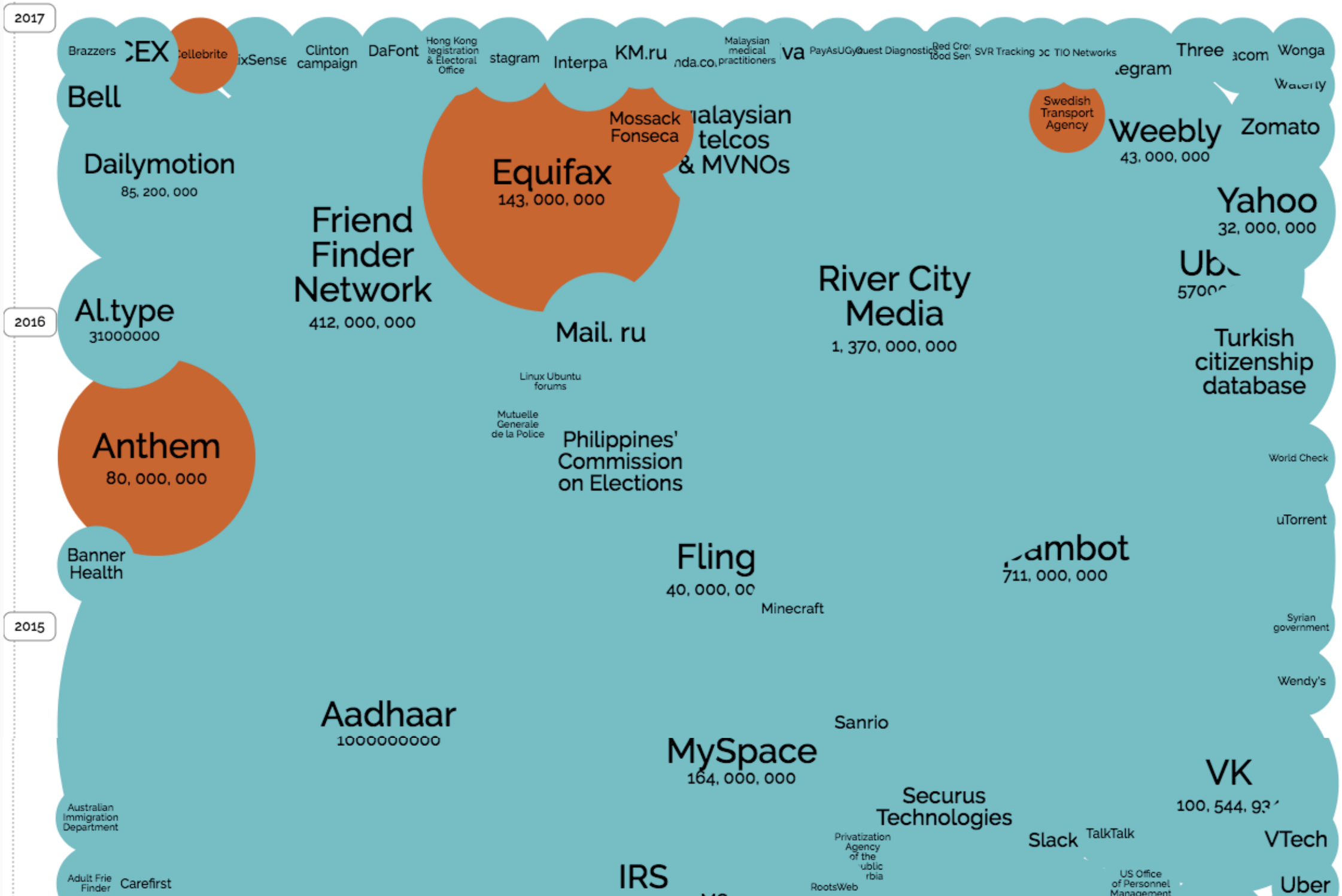
(updated 02nd Feb 2018)

interesting story

YEAR

BUBBLE COLOUR YEAR METHOD OF LEAK BUBBLE SIZE NO OF RECORDS STOLEN DATA SENSITIVITY

SHOW FILTER



2007

City and Hackney Teaching Primary Care Trust

Compass Bank

Driving Standards Agency

Fidelity National Information Services

Driving Standards Agency,

Gap Inc

Hannaford Brothers Supermarket Chain

Monster.com

Texas Lottery

UK Revenue & Customs

TK / TJ Maxx
94, 000, 000

2006

AOL

Countrywide Financial Corp

Hewlett Packard

KDDI

T-Mobile, Deutsche Telecom

US Dept of Vet Affairs

2005

Automatic Data Processing

Cardsystems Solutions Inc.

Ameritrade Inc.

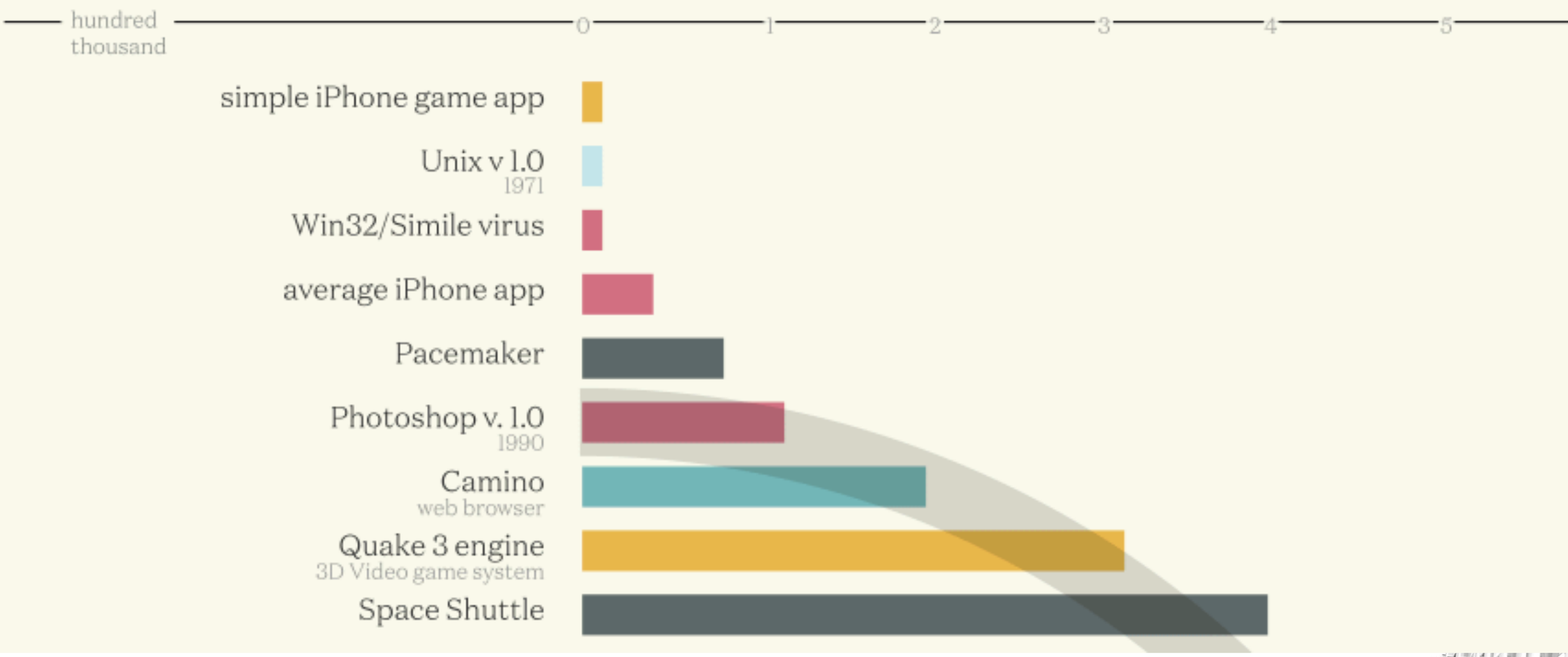
Citigroup

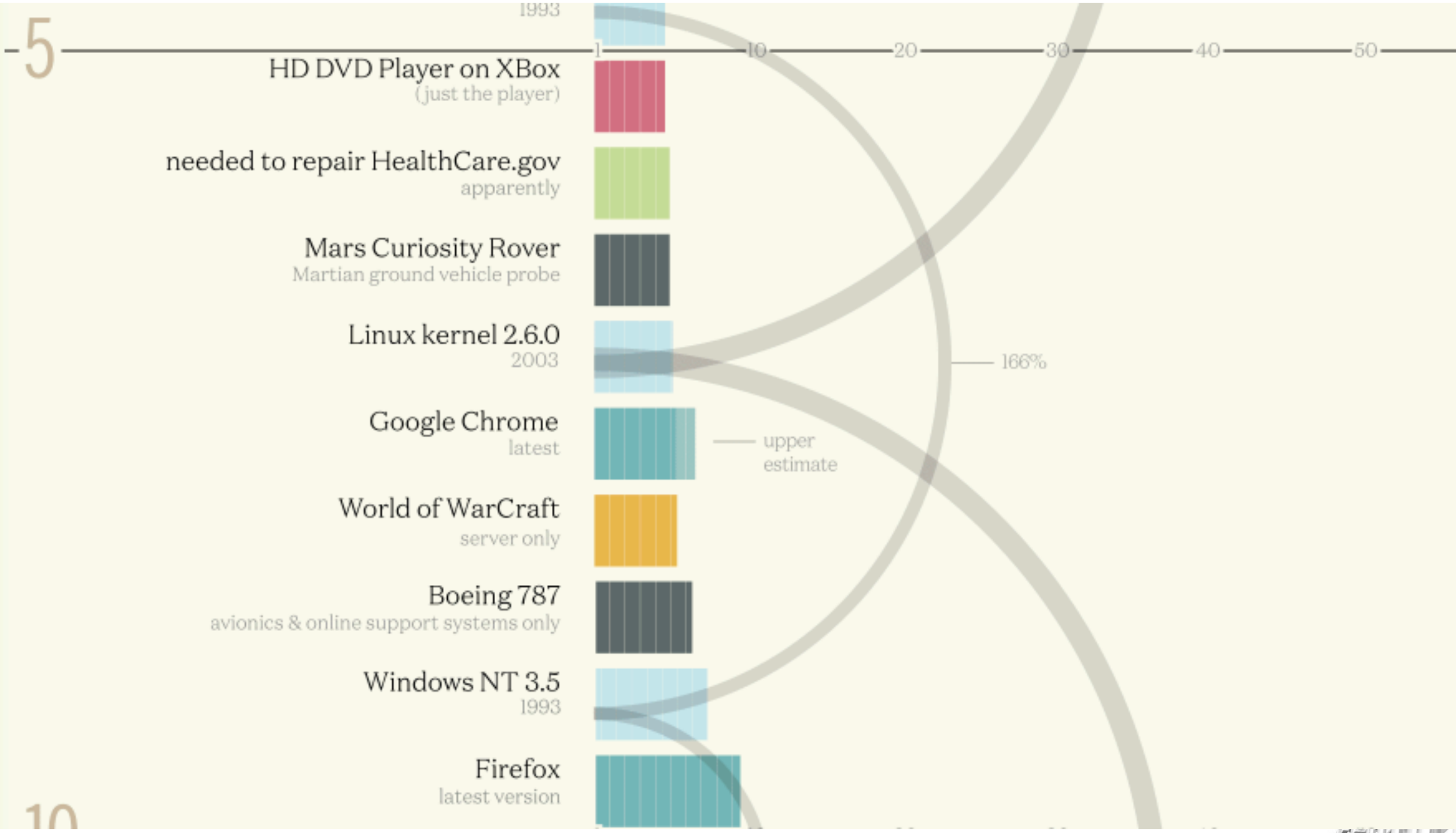
2004

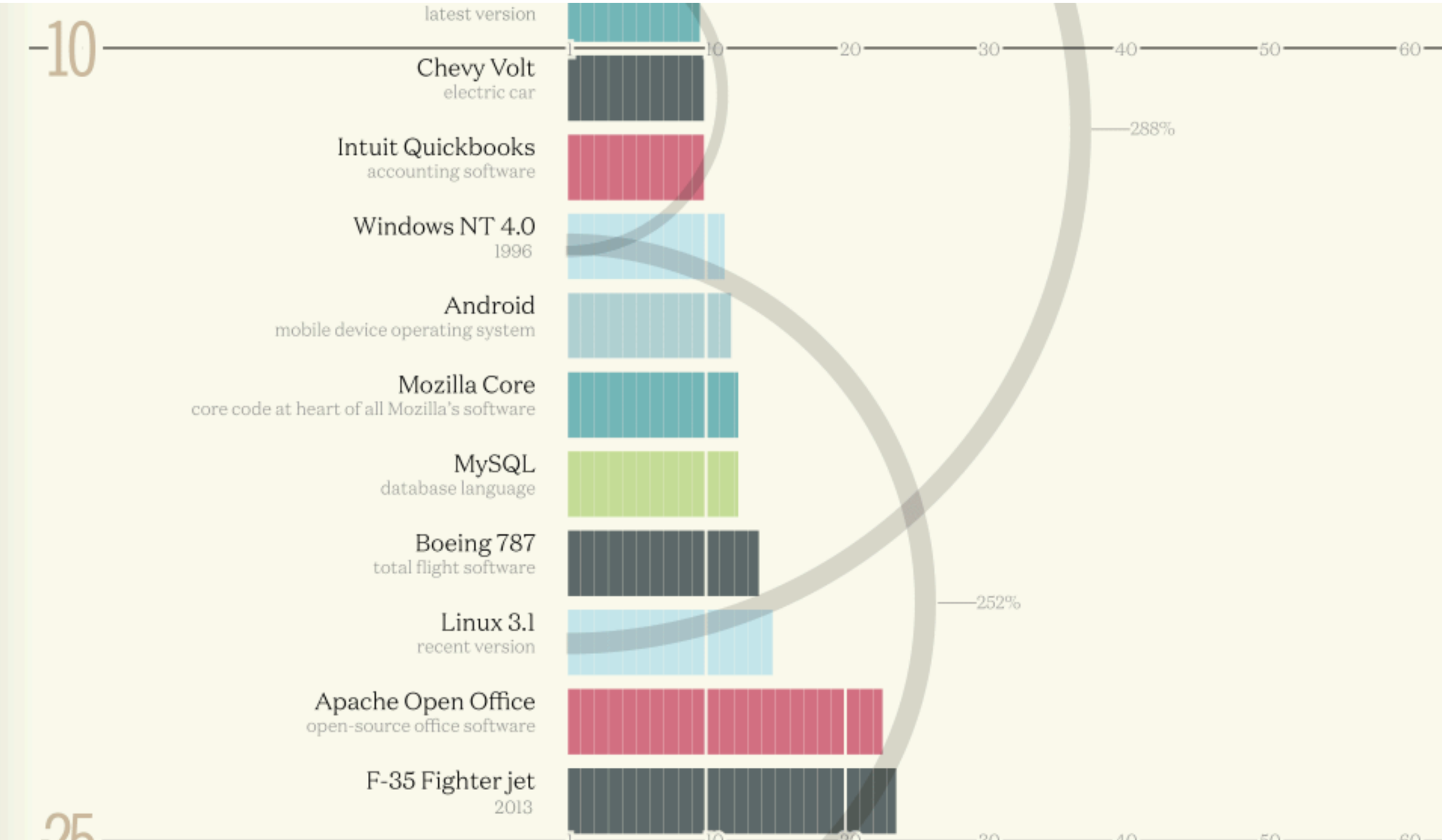
AOL
92, 000, 000

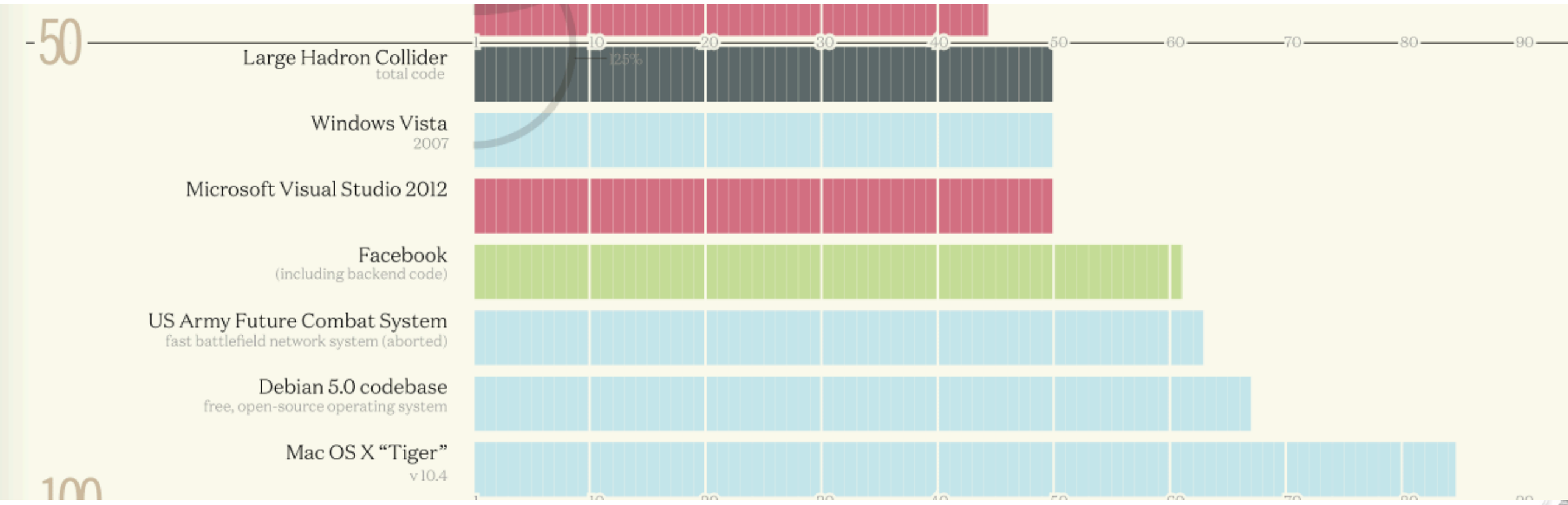
Codebases

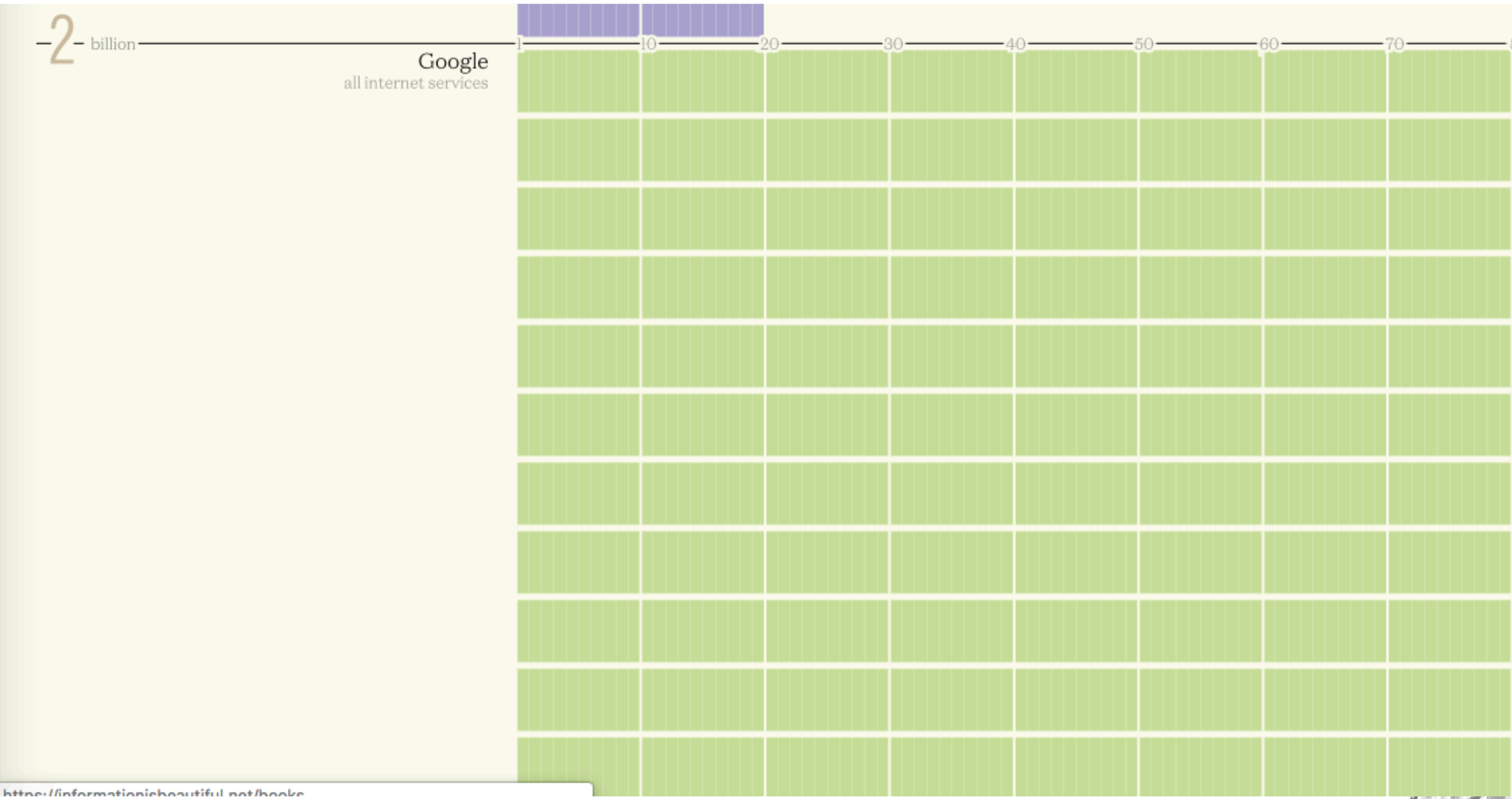
Millions of lines of code




1993
5
1
10
20
30
40
50
HD DVD Player on XBox
(just the player)
needed to repair HealthCare.gov
apparently
Mars Curiosity Rover
Martian ground vehicle probe
Linux kernel 2.6.0
2003
166%
Google Chrome
latest
upper
estimate
World of WarCraft
server only
Boeing 787
avionics & online support systems only
Windows NT 3.5
1993
Firefox
latest version
10


latest version
10
1
10
20
30
40
50
60
Chevy Volt
electric car
Intuit Quickbooks
accounting software
288%
Windows NT 4.0
1996
Android
mobile device operating system
Mozilla Core
core code at heart of all Mozilla's software
MySQL
database language
Boeing 787
total flight software
252%
Linux 3.1
recent version
Apache Open Office
open-source office software
F-35 Fighter jet
2013
25


50
1
10
20
30
40
50
60
70
80
90
125%
Large Hadron Collider
total code
Windows Vista
2007
Microsoft Visual Studio 2012
Facebook
(including backend code)
US Army Future Combat System
fast battlefield network system (aborted)
Debian 5.0 codebase
free, open-source operating system
Mac OS X "Tiger"
v 10.4
100


2 billion
1
10
20
30
40
50
60
70
Google
all internet services

LA STAMPA ITALIA

Privacy, più di un milione i dati violati nei primi quattro mesi di Gdpr

Sono state 305 le notificazioni inviate al Garante italiano per la privacy dall'entrata in vigore della normativa europea. Ma c'è il rischio che molti non segnalino i data breach

RAFFAELE ANGIUS

Pubblicato il 28/09/2018

A quattro mesi dalla piena operatività del Regolamento Generale per la Protezione dei Dati (Gdpr), in Europa è già iniziata la corsa alle segnalazioni che

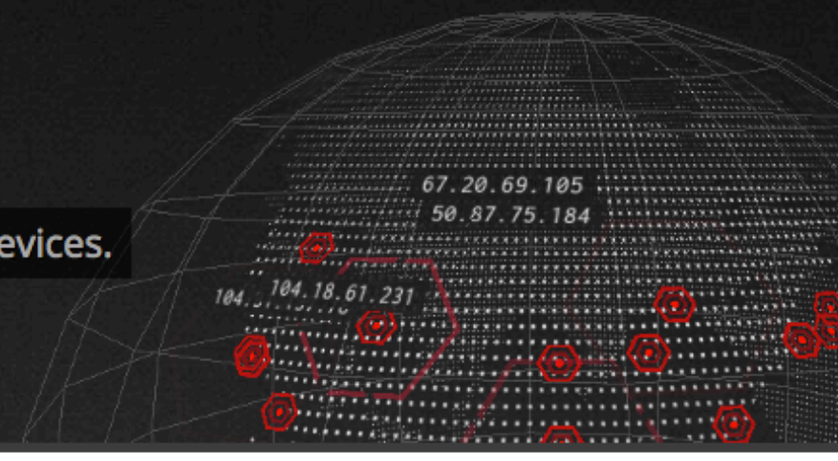
SHODAN

Explore | Developer Pricing | Enterprise Access | Contact Us

The search engine for Security

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account | Getting Started



Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are p
refrigerators and much more that can be found with Sho

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? empirical market intelligence.

56% of Fortune 100

1,000+ Universities

Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.

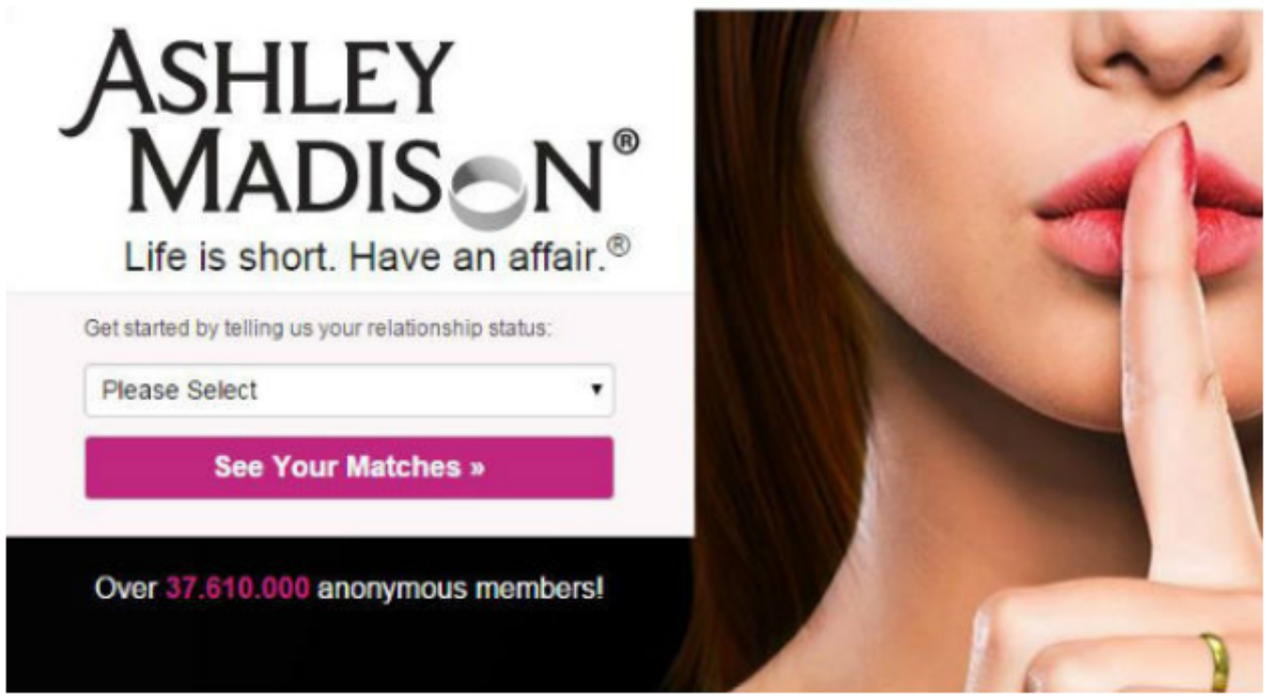
Analyze the Internet in Seconds

Shodan has servers located around the world that crawl the Internet 24/7 to provide the latest I
buys Smart TVs? Which countries are building the most wind farms? What companies are affec
Shodan provides the tools to answer questions at the Internet-scale.

di **Giuditta Mosca**
19 AGO, 2015

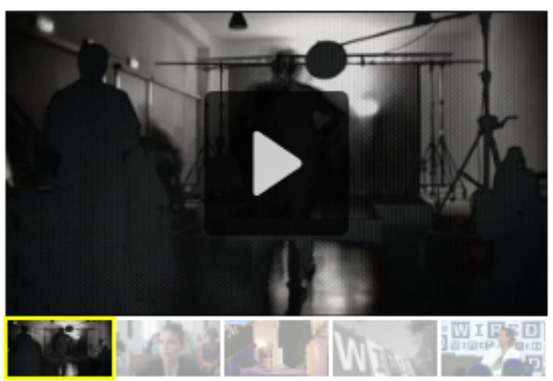
Ashley Madison, online tutti i dati dei traditori

Lo scorso luglio un gruppo di hacker ha violato il famoso sito per adulteri, prelevando milioni di dati sensibili. Ora sono disponibili online



I dati di **milioni di fedifraghi** prelevati dal sito **Ashley Madison** lo scorso luglio sono online, nel file da **9,7 GB** si possono trovare i **nomi** degli utenti, i loro **indirizzi email**, **preferenze sessuali** e le transazioni avvenute tramite

VIDEO



Data breach solo informatico?

R.it | BARI

Puglia BARI BAT BRINDISI FOGGIA LECCE TARANTO Basilicata MATERA POTENZA

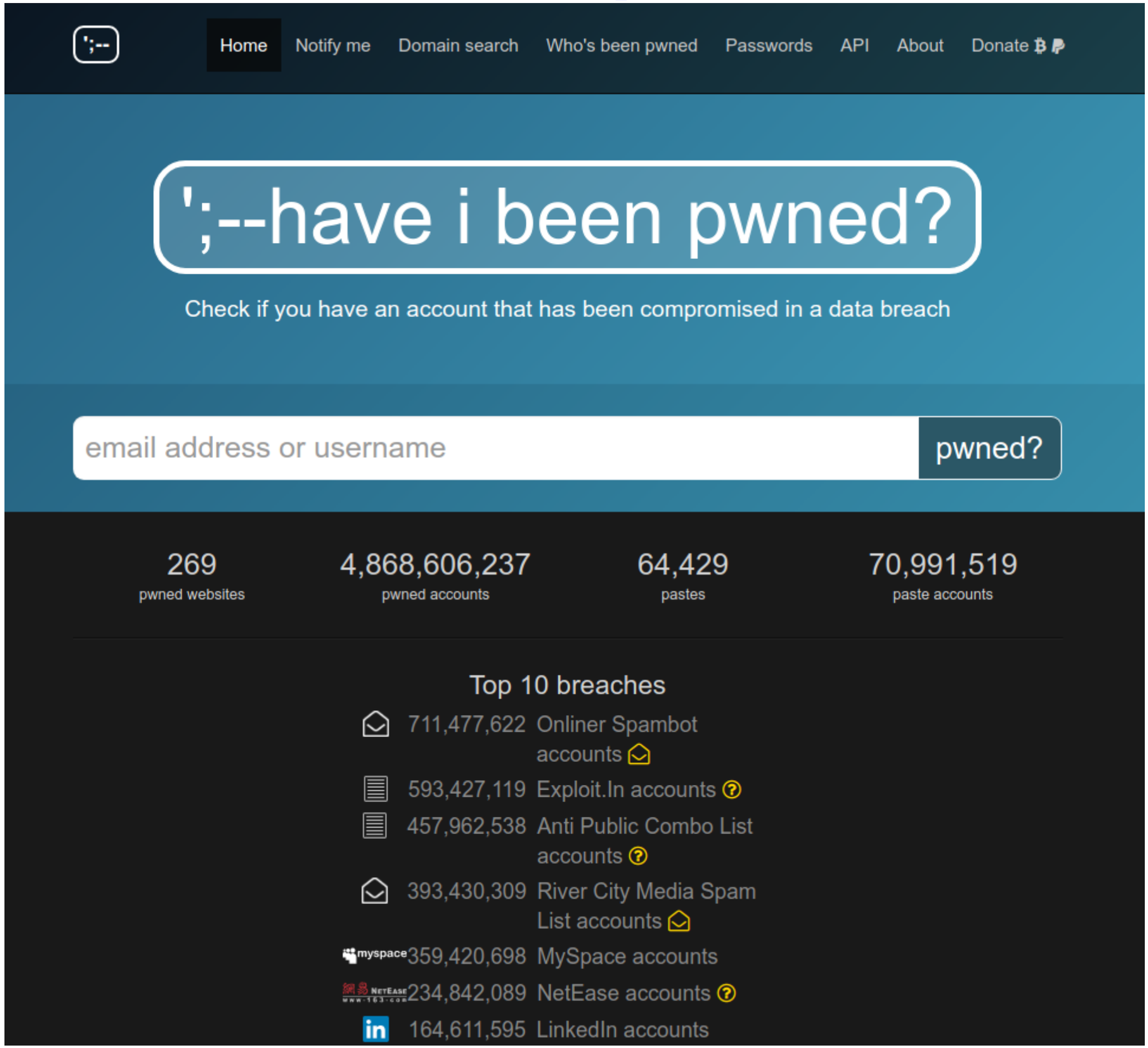
Cerca nel sito

METEO

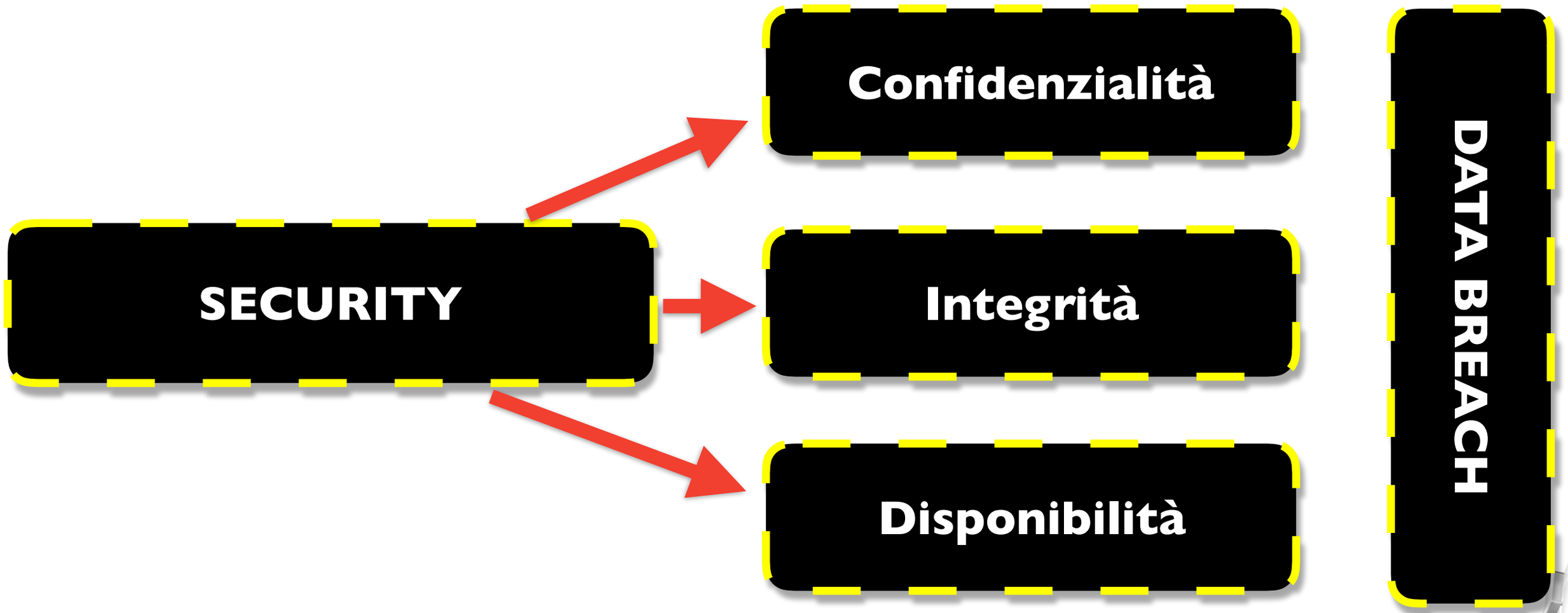
Home | Cronaca | Sport | Foto | Ristoranti | Annunci Locali | Cambia Edizione | Video

Lecce, centinaia di cartelle cliniche dell'ospedale Vito Fazzi abbandonate in campagna: è giallo

www.haveibeenpwned.com



quali data breach?



Definizione di Data Breach (art. 4)

«violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito

la **distruzione**, [A]

la **perdita**, [A]

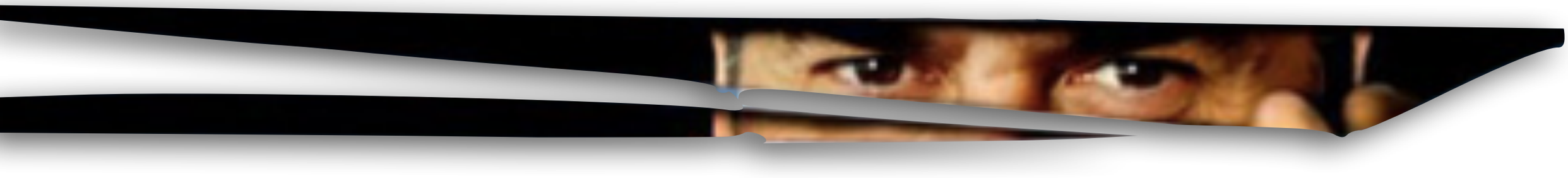
la **modifica**, [I]

la **divulgazione non autorizzata** [C] o

l'**accesso [non autorizzato]** ai dati personali trasmessi, conservati o comunque trattati [C]

le cause frequenti dei data breach

- ***Errore umano***
  - ***Errori di configurazione***
  - ***Errori nella gestione***
  - ***Formattazione e dismissione***
  - ***Compromissione dei backup***
  - ***Danni da liquidi***
  - ***Imprudenze e negligenze***
- ***Attacchi***
  - ***Accessi abusivi esterni/insiders***
  - ***Leak dei dati***
  - ***Virus & Malware***
  - ***Social engineering***
  - ***Furti e danneggiamenti***
- ***Danni e hardware***
- ***Fornitura di energia***
- ***Eventi naturali***
  - ***roditori, funghi…***
  - ***incendi, allagamenti etc***
- ***Obsolescenza hardware e software***



Paranoia is a virtue!

quanti data breach?

DATA BREACH

- **Reg. UE GDPR**
- **Reg. UE eIDAS**
  da
- **Direttiva NIS**
  D.Lgs. 65/2018
- **Circ. 2/17 AgID**

Direttiva NIS + DLgs 65/2018 (art. 1)

1. Il presente decreto stabilisce misure volte a conseguire un livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea.

2. Ai fini del comma 1, il presente decreto prevede:

c) il rispetto di **obblighi da parte degli operatori di servizi essenziali e dei fornitori di servizi digitali** relativamente all'adozione di misure di sicurezza e di **notifica degli incidenti con impatto rilevante**;

7. **Qualora gli obblighi previsti** per gli operatori di servizi essenziali o i fornitori di servizi digitali di assicurare la sicurezza delle loro reti e dei loro sistemi informativi o di notificare gli incidenti **siano oggetto di uno specifico atto giuridico dell'Unione europea, si applicano le disposizioni di detto atto giuridico** nella misura in cui gli effetti di tali obblighi siano **almeno equivalenti** a quelli degli obblighi di cui al presente decreto.

Art. 12, D.Lgs. 65/18

5. Gli operatori di servizi essenziali notificano al CSIRT italiano e, per conoscenza, all'autorità competente NIS, senza ingiustificato ritardo, gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti.

Art. 33 GDPR

Notifica di una violazione dei dati personali all'autorità di controllo

1. In caso di violazione dei dati personali, il **titolare** del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**, a meno che sia improbabile che la violazione dei dati personali presenti un **rischio per i diritti e le libertà delle persone fisiche**. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è **corredata dei motivi del ritardo**.

Data breach GDPR

Contenuto della notifica al Garante

3. La notifica di cui al paragrafo 1 deve almeno:
a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni **[records]** dei dati personali in questione;
b) comunicare **il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto** presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Art. 34 - Comunicazione all'interessato

Modalità della comunicazione

- Messaggio specifico (no a inserimento in newsletter etc.)
- Comunicazione sul sito
- Eventuale pubblicazione su quotidiani e simili
- Attenzione al formato e alla lingua
- Attenzione ai phishing che simulano i data breach

Tempestività

è opportuno che tali modalità e procedure tengano conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge **[law-enforcement authorities]**, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali. (C.88)

Art. 34 - Comunicazione all'interessato

3. **Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se** è soddisfatta una delle seguenti condizioni:
a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la **cifratura**;
b) il titolare del trattamento ha **successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà** degli interessati di cui al paragrafo 1;
c) **detta comunicazione richiederebbe sforzi sproporzionati**. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

Grazie

per la tensione