UNIVERSITÀ DI TRENTO

DIPARTIMENTO
FACOLTÀ DI GIURISPRUDENZA

lawtech
The Law and Technology Research Group

Diritto civile A-J

Lezione 16 – La sorveglianza di massa e il trasferimento dei dati fuori dell'Unione Europea

Università di Trento – Facoltà di Giurisprudenza
a.a. 2024-2025

Roberto Caso

Snowden (Oliver Stone, 2016)

Datagate

Exclusive

The whistleblower

I can't allow the US government to destroy privacy and basic liberties

the guardian

guardian.co.uk

Edward Snowden, 29, emerges from hiding in Hong Kong

IT contractor says his concerns were ignored and he had to go public

Glenn Greenwald Hong Kong
Julian Borger

The whistleblower behind the most significant US intelligence leak in modern times broke cover last night, saying he had decided to leave his position at a National Security Agency (NSA) contractor because he believed its unconstrained collection of electronic intelligence was destroying civil liberties and creating the conditions for tyranny.

Edward Snowden, a 29-year-old IT administrator for the defence contractor Booz Allen Hamilton, was speaking in Hong Kong after leaking a series of agency documents on the collection of telephone data on millions of Americans, the NSA's relationship with US internet providers and the Obama administration cyber-warfare policy.

"I can't allow the US government to destroy privacy, internet freedom and basic liberties," he said. "My sole motive is to inform the public as to that which is done in their name and that which is done against them."

Snowden said he felt compelled to speak out because in his job helping to run the NSA computer systems, he had witnessed a pattern of excessive and intrusive surveillance of Americans, and that his objections had been ignored by his superiors.

"When you're in positions of privileged access, like a systems administrator for these sort of intelligence community agencies, you're exposed to a lot more information on a broader scale than the average employee, and because of that you see things that may be disturbing but over the course of a normal person's career you'd only see one or two of these instances," Snowden said. "I, sitting at my desk, certainly had the authorities to wiretap anyone: you, your accountant, to a federal judge, even the president if I had a personal email."

He argued that NSA surveillance was not being effectively constrained by administration policy and would continue to grow as the technology improved. "And the months ahead, the years ahead, it's only going to get worse, until eventually there will be a time where policies will change - because the only thing that restricts the activities of the surveillance state are policy."

Snowden warned that if there was no greater awareness of what US intelligence was doing and not much greater oversight the "surveillance state" would outrun the ability of the American people to control it. "And there will be nothing the people can do at that point to oppose it. And it'll be turn-key tyranny," Snowden said.

He said he had given up a comfortable existence in Hawaii and now risked arrest and imprisonment. In a note accompanying the first set of documents he provided, he wrote: "I understand that I will be made to suffer for my actions."

But in an interview with the Guardian, Snowden declared: "I've no intention of hiding, I've done nothing wrong.

"The greatest fear that I have regarding the outcome of these disclosures for America is that nothing will change," he said. "People will see in the media all of these disclosures, they'll know the lengths the government is going to grant themselves powers unilaterally, to create greater control over American society and global society, but they won't be willing to take the risks necessary to stand up and fight to change things, to force their representatives to actually take a stand in their interests," Snowden said.

He also sounded a warning to other nations that the US intelligence establishment does not view international treaties as being binding constraints on its operations. "Even our agreements with other sovereign governments, we consider that to be a stipulation of policy rather than a stipulation of law," he said. "And because of that, a new leader will be elected, they'll flip the switch, say that because of the 'crisis', because of the dangers we face in the world, you know, some new and unpredicted threat, we need more authority, we need more power."

He defended his decision to go to Hong Kong to share his knowledge of NSA operations, pointing out that the enclave had autonomies and freedom not shared by the rest of China. He insisted his intention was not to harm America's security and pointed out that he had access to a huge amount of information that could have crippled US intelligence collection, but had not given it away.

Snowden said that he had raised his concerns at work, but they had been shrugged off, so he felt he had little choice but to go public.

2-5

PRISM

Monday 10.06.13
Published in London and Manchester
£1.40 (IR €1.40)

Oxbridge bias
London and the south-east dominate entries
Page 7

Gillian Anderson
Star of The Fall who never sang Hollywood's tune
Page 10

Rafa's triumph
Nadal wins record eighth French Open title
Sport Page 1

MIF
MANCHESTER INTERNATIONAL FESTIVAL
4 – 21 July 2013
See page 2

The Washington Post

MONDAY, JUNE 10, 2013

Man who leaked NSA secrets steps forward

A REPORTER'S ACCOUNT

To leaker, personal risks were clear

BY BARTON GELLMAN

He called me ERASSEANNER, a code name in the double-barreled style of the National Security Agency, where he worked in the signals intelligence directorate.

Verax was the name he chose for himself, "truth teller" in Latin. I asked him early on, without reply, whether he intended to hint at the alternative fates that lay before him.

Two British dissenters had used the pseudonym. Clement Walker, a 17th-century detractor of Parliament, died in the brutal confines of the Tower of London. Two centuries later, social critic Henry Dunckley adopted "Verax" as his byline over weekly columns in the Manchester Examiner. He was showered with testimonials and an honorary degree.

Edward Joseph Snowden, 29, knew full well the risks he had undertaken and the awesome powers that would soon be arrayed to hunt for him. Pseudonyms were the least of his precautions as we corresponded from afar. Snowden was spilling some of the most sensitive secrets of a surveillance apparatus he had grown to detest. By late last month, he believed he was already "on the X" -- exposure imminent.

"I understand that I will be made to suffer for my actions, and that the return of this information to the public marks my end," he wrote in early May, before we had our first direct contact. He warned that even journalists who

SNOWDEN CONTINUED ON A4

Before the world knew his name, tech specialist Edward Snowden, 29, now in Hong Kong, drafted a note of explanation. STORY, A4

Risks of outsourcing
Government reliance on private spying contractors comes with costs as well as benefits. A2

A historic leak
Edward Snowden receives praise and criticism as his name joins that of Daniel Ellsberg. A4

EDWARD SNOWDEN: 'I'M NOT GOING TO HIDE'

Booz Allen consultant could face prosecution

BY BARTON GELLMAN, AARON BLAKE AND GREG MILLER

A 29-year-old man who says he is a former undercover CIA employee said Sunday that he was the principal source of recent disclosures about top-secret National Security Agency programs, exposing himself to possible prosecution in an acknowledgment that had little if any precedent in the long history of U.S. intelligence leaks.

Edward Snowden, a tech specialist who has contracted for the NSA and works for the consulting firm Booz Allen Hamilton, unmasked himself as a source after a string of stories in The Washington Post and the Guardian that detailed previously unknown U.S. surveillance programs. He said he disclosed secret documents in response to what he described as the systematic surveillance of innocent citizens.

In an interview Sunday, Snowden said he is willing to face the consequences of exposure.

"I'm not going to hide," Snowden told The Post from Hong Kong, where he has been staying. "Allowing the U.S. government to intimidate its people with threats of retaliation for revealing wrongdoing is contrary to the public interest."

Asked whether he believes that his disclosures will change anything, he said: "I think they already have. Everyone everywhere now understands how bad things

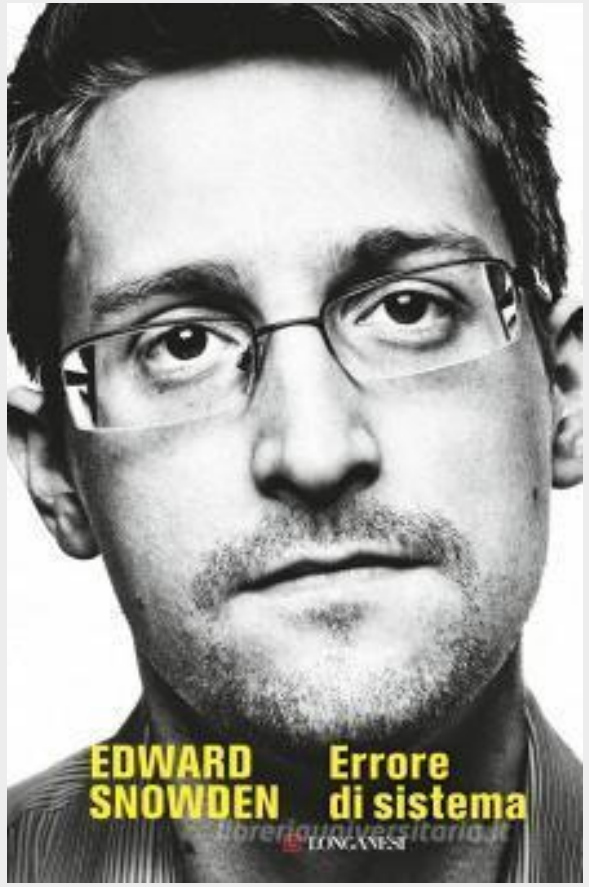
SURVEILLANCE CONTINUED ON A5

Datagate: una cronistoria

- https://www.internazionale.it/notizie/2015/06/25/datagate-snowden-spionaggio

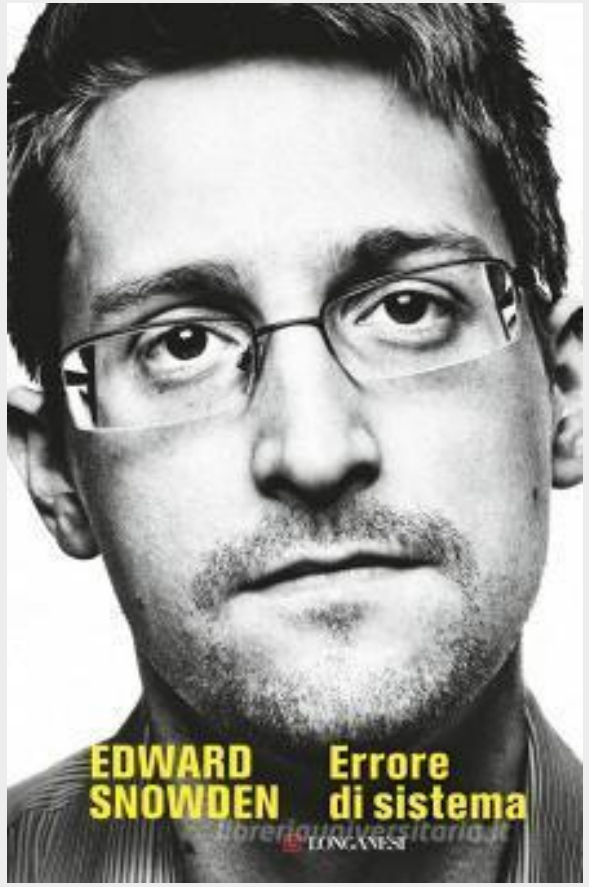
Snowden «Errore di sistema» 2019

- “Mi chiamo Edward Joseph Snowden. **Un tempo lavoravo per il governo, ora lavoro per le persone. Mi ci sono voluti quasi trent’anni per capire che c’era una differenza tra le due cose e, quando è successo, ho iniziato ad avere qualche problema sul lavoro**.”



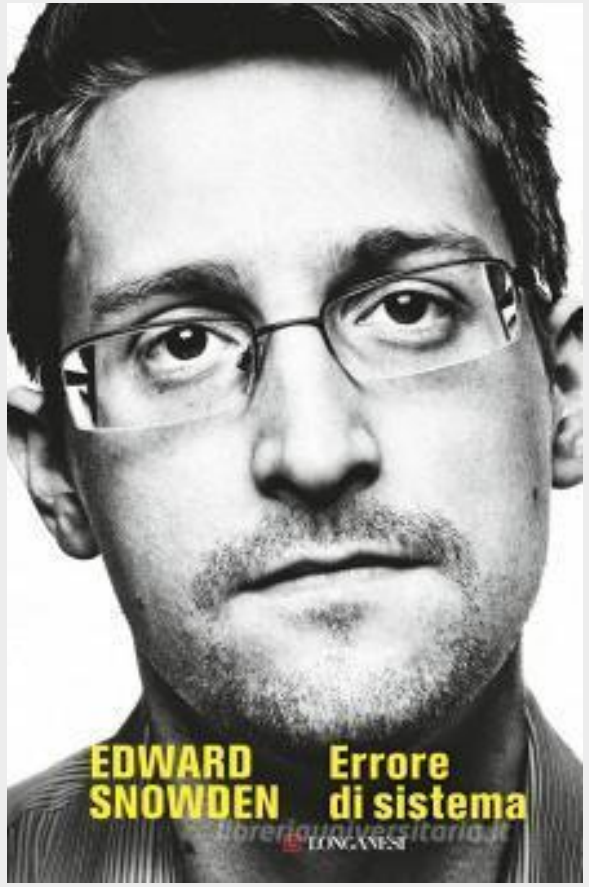
Snowden «Errore di sistema» 2019

- “So bene quale luogo **tossico** e **insano** sia diventato oggi il Web, ma dovete capire che per me, quando ci sono entrato in contatto per la prima volta, Internet era qualcosa di totalmente diverso. **Era come un amico, un genitore**. Una comunità […] i cui membri erano **liberi di scegliere il proprio nome**, la propria storia e le proprie abitudini. ”



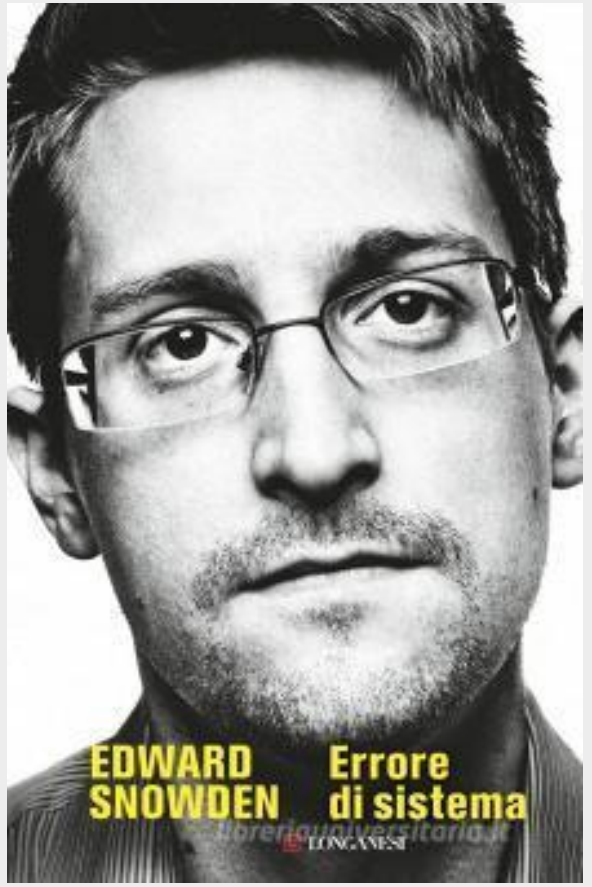
Snowden «Errore di sistema» 2019

- “Mi capirete, quindi, se dico che oggi Internet è diventata irriconoscibile. Questo cambiamento **è il risultato di una scelta consapevole** e di sforzi sistematici da parte di un’élite privilegiata. La repentina evoluzione del commercio in e-commerce ha portato alla creazione di **una bolla che sarebbe prontamente scoppiata** con l’avvento del nuovo millennio. ”



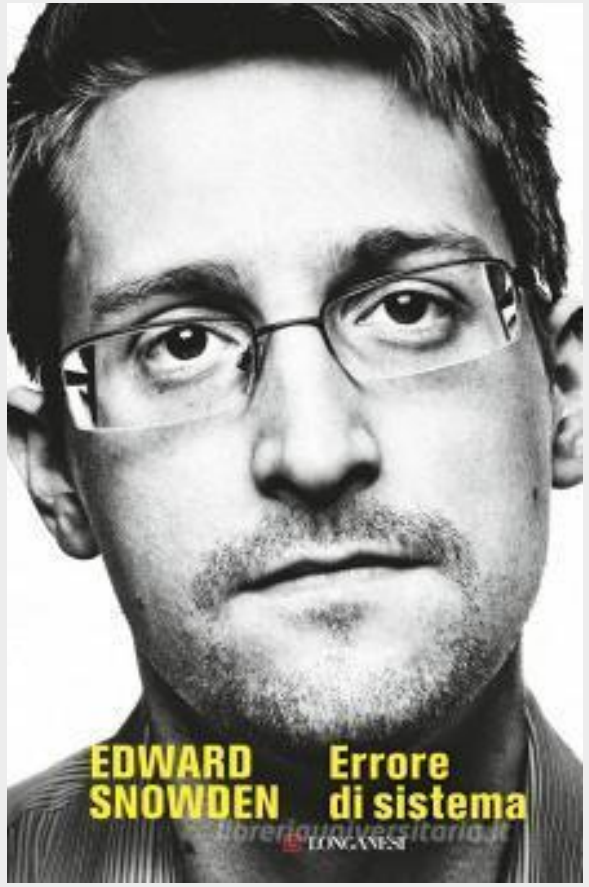
Snowden «Errore di sistema» 2019

- “[…] allora le aziende dovevano semplicemente **trovare il modo di inserirsi in questi scambi sociali e trarne profitto**.
- È così che è iniziato il **capitalismo di sorveglianza**, decretando la fine di Internet per come la conoscevo io.”



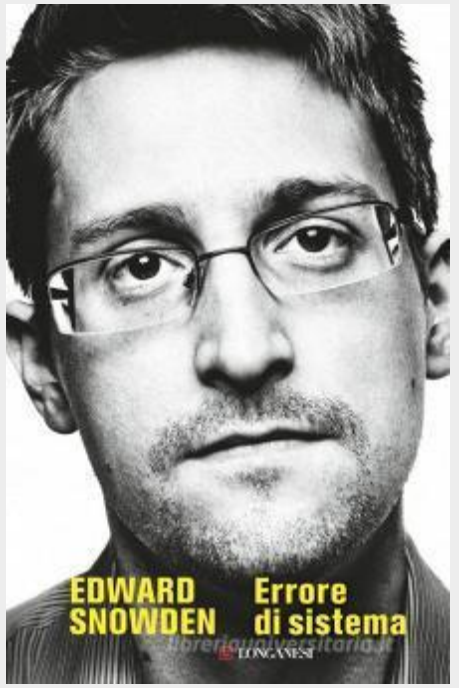
Snowden «Errore di sistema» 2019

- «La gente, attirata dalla **maggiore facilità d'uso**, ha preferito **abbandonare i propri siti personali** – che richiedevano un costante lavoro di manutenzione – **a favore di pagine Facebook o account Gmail**, dei quali, però, erano proprietari solo nominalmente»



Snowden «Errore di sistema» 2019

- **«Pochi di noi allora se ne resero conto**, ma ormai **non ci apparteneva più niente di quello che condividevamo**. Chi era succeduto alle società che avevano fallito nell'e-commerce, perché non erano riuscite a trovare nulla che ci interessasse comprare, **ora aveva un nuovo prodotto da venderci.**
- **Quel prodotto eravamo noi stessi.**»



L’ordine del ragionamento

1. Caso 1

2. La disciplina del trattamento dei dati personali: cenni

3. La sorveglianza di massa e il trasferimento dei dati fuori dell’Unione Europea – Come sta andando a finire? – Soluzione caso e problema 1

1. Caso 1

- Con reclamo del XX, come successivamente integrato in data XX, uno studente dell'Università Commerciale "Luigi Bocconi" di Milano (di seguito, l'"Università" o l'"Ateneo") ha lamentato possibili violazioni della disciplina sulla protezione dei dati personali in relazione all'impiego di un sistema di supervisione (proctoring) nell'ambito dello svolgimento delle prove scritte d'esame degli studenti, al fine di identificare questi ultimi e/o di verificarne il corretto comportamento durante lo svolgimento della prova d'esame. In particolare è stato rappresentato che l'Ateneo avrebbe richiesto il consenso degli studenti al trattamento "delle categorie particolari di dati personali (dati biometrici […]), [in mancanza del quale gli studenti] non sarebbero in grado di svolgere esami online" con ciò comportando un "pregiudizio estremo […]".

2. Rodotà (2000)

- Nella società dell'informazione tendono a prevalere **definizioni funzionali della privacy** che, in diversi modi, fanno riferimento alla possibilità di un soggetto di conoscere, controllare, indirizzare, interrompere il flusso delle informazioni che lo riguardano. La privacy, quindi, può essere più precisamente definita, in una prima approssimazione, come il **diritto di mantenere il controllo sulle proprie informazioni**.

2. Pascuzzi (2020)

- L’introduzione delle tecnologie informatiche ha comportato un cambiamento importante del campo della tutela dei diritti della personalità. L’avvento dei calcolatori ha richiesto l’adozione di specifici meccanismi di tutela perché il problema non era più (solo) quello di salvaguardare la vita privata di persone famose dall’aggressione portata dai mass media, bensì **quello di scongiurare i pericoli più o meno palesi e avvertibili (discriminazioni in testa) derivanti a ciascun cittadino dalla facilità con la quale possono essere trattate e incrociate le informazioni che lo riguardano**. La rivoluzione digitale comporta addirittura il cambiamento della nozione e del contenuto del diritto alla riservatezza: **non più diritto a essere lasciati soli, ma diritto al controllo sui propri dati**.

2. CDFUE art. 7 - Rispetto della vita privata e della vita familiare

- Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni.

2. CDFUE art. 8 - Protezione dei dati di carattere personale

- 1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.
- 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.
- 3. Il rispetto di tali regole è soggetto al controllo di un’autorità indipendente

2. Art. 16 TFUE

- Articolo 16 (ex articolo 286 del TCE)
- 1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
- 2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti.
- Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea.

2. Alcune tappe normative fondamentali

- Convenzione europea sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale (l. 21 febbraio 1989, n. 98)
- Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati
- L. 31 dicembre 1996, n. 675, Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali
- D.lgs. 30 giugno 2003, n. 196, codice in materia di protezione dei dati personali (codice privacy)
- Regolamento europeo in materia di tutela dei dati personali (n. 2016/679) - GDPR
- Decreto legislativo 10 agosto 2018, n. 101, modifica del codice privacy per adeguamento al GDPR

2. CDFUE art. 8 - principi

1. Principio di lealtà;
2. Principio della limitazione della finalità del trattamento;
3. Principio della legittimità (il trattamento deve avere una base di legittimità nel consenso della persona interessata o in altro fondamento legittimo previsto dalla legge);
4. Diritto di accesso e di rettifica;
5. Autorità indipendente di controllo.

2. GDPR - principi

a) Liceità, correttezza e trasparenza
b) Limitazione della finalità
c) Minimizzazione dei dati
d) Esattezza
e) Limitazione della conservazione
f) Integrità e riservatezza
g) Responsabilizzazione (accountability)
h) Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (privacy by design/by dafault)

2. GDPR - Liceità del trattamento

- Si basa sul consenso dell’interessato o su altre condizioni elencate all’art. 6 RGDP

2. GDPR - Liceità del trattamento – Art. 6, par. 1

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un **contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per **la salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per **l'esecuzione di un compito di interesse pubblico** o **connesso all'esercizio di pubblici poteri** di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il **perseguimento del legittimo interesse del titolare del trattamento o di terzi**, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

2. GDPR - diritti dell’interessato al capo III (art. 15-22)

a) Diritto di accesso;
b) diritto di cancellazione (diritto all’oblio);
c) diritto di limitazione del trattamento;
d) diritto alla portabilità dei dati;
e) diritto di opposizione;
f) diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato.

2. GDPR – dato personale e interessato

- qualsiasi **informazione** riguardante **una persona fisica identificata o identificabile («interessato»)**; si considera identificabile la persona fisica che **può essere identificata, direttamente o indirettamente**, con particolare riferimento a un **identificativo** come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più **elementi caratteristici della sua identità** fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

2. GDPR - trattamento [*processing*]

- qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

2. GDPR – titolare [*controller*]

- la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, **determina le finalità e i mezzi del trattamento di dati personali**; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

2. GDPR - responsabile [*processor*]

- la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che **tratta dati personali per conto del titolare del trattamento**.

3. GDPR – trasferimento dei dati

I. Tutte le disposizioni normative gravitano sul principio generale che **il livello di protezione delle persone fisiche garantito dal GDPR non deve essere pregiudicato** (art. 44).

II. Decisione della Commissione Europea. Il trasferimento è ammesso **se la Commissione ha deciso** che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono «**un livello di protezione adeguato**». In tal caso il trasferimento non necessita di autorizzazioni specifiche (art. 45).

3. GDPR – trasferimento dei dati

III. In mancanza di una decisione ai sensi dell'articolo 45, paragrafo 3, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un Paese terzo o un'organizzazione internazionale solo se ha fornito **«garanzie adeguate»** e a condizione che gli interessati dispongano di **diritti azionabili e mezzi di ricorso effettivi** (art. 46). Tra le «garanzie adeguate» non soggette ad autorizzazioni specifiche da parte di un'autorità di controllo figurano le **«norme vincolanti d'impresa»** disciplinate dall'art. 47 e le **«clausole tipo»** di protezione dei dati adottate dalla Commissione.

3. GDPR – trasferimento dei dati

IV. Deroghe in specifiche situazioni (art. 49). **In mancanza di una decisione di adeguatezza** ai sensi dell'articolo 45, paragrafo 3, **o di garanzie adeguate** ai sensi dell'articolo 46, l'art. 49 elenca una **serie di deroghe specifiche** che rendono ammissibile il trasferimento dei dati.

3. Max Schrems

https://en.wikipedia.org/wiki/Max_Schrems

- «**Maximilian Schrems** is an Austrian activist, lawyer, and author who became known for campaigns against Facebook for its privacy violations, including violations of European privacy laws and the alleged transfer of personal data to the US National Security Agency (NSA) as part of the NSA's PRISM program. Schrems is the founder of NOYB – European Center for Digital Rights»

By Manfred Werner - Tsui - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=46459241

3. Decisioni Commissione trasferimento USA – Safe Harbor

- La Commissione Europea, sulla base della disciplina della dir. 95/46, aveva emanato decisione 2000/520/CE che ammetteva il trasferimento dei dati personali verso gli USA sulla base di un accordo con questi ultimi denominato Safe Harbor (approdo sicuro)
- Maximilian Schrems, un attivista austriaco che difende i diritti e le libertà su Internet, avviava un reclamo al Data Protection Commissioner (Commissario per la protezione dei dati) irlandese concernente il fatto che Facebook Ireland Ltd trasferiva negli Stati Uniti i dati personali dei propri utenti e li conserva su server ubicati in quel paese.

3. Corte di Giustizia sentenza 6 ottobre 2015 C-362/14 (Scherems I)

- L’articolo 25, paragrafo 6, della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, come modificata dal regolamento (CE) n. 1882/2003 del Parlamento europeo e del Consiglio, del 29 settembre 2003, letto alla luce degli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell’Unione europea, deve essere interpretato nel senso che una decisione adottata in forza di tale disposizione, come la decisione 2000/520/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46 sull’adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti, con la quale la Commissione europea constata che un paese terzo garantisce un livello di protezione adeguato, **non osta a che un’autorità di controllo di uno Stato membro, ai sensi dell’articolo 28 di tale direttiva, come modificata, esamini la domanda di una persona relativa alla protezione dei suoi diritti e delle sue libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, qualora tale persona faccia valere che il diritto e la prassi in vigore in quest’ultimo non garantiscono un livello di protezione adeguato.**

3. Corte di Giustizia sentenza 6 ottobre 2015 C-362/14 (Scherems I)

- La decisione 2000/520 - Safe Harbor (approdo sicuro) è invalida.

3. Decisioni Commissione trasferimento USA - Privacy schield

- A seguito della dichiarazione di invalidità della decisione 2000/520 sul porto sicuro, la Commissione emanava una seconda decisione (UE) 2016/1250 in data 16 luglio che recepiva un nuovo accordo tra USA e UE denominato «privacy schield UE-USA» (scudo UE-USA per la privacy).

3. Corte di Giustizia UE sentenza 16 luglio 2020 C-311/18 (Schrems II)

- L’articolo 46, paragrafo 1, e l’articolo 46, paragrafo 2, lettera c), del regolamento 2016/679 devono essere interpretati nel senso che le garanzie adeguate, i diritti azionabili e i mezzi di ricorso effettivi richiesti da tali disposizioni devono garantire che i diritti delle persone i cui dati personali sono trasferiti verso un paese terzo sul fondamento di clausole tipo di protezione dei dati godano di un livello di protezione sostanzialmente equivalente a quello garantito all’interno dell’Unione da tale regolamento, letto alla luce della Carta dei diritti fondamentali dell’Unione europea. A tal fine, la valutazione del livello di protezione garantito nel contesto di un trasferimento siffatto **deve, in particolare, prendere in considerazione** tanto le **clausole contrattuali convenute tra il titolare del trattamento o il responsabile del trattamento stabiliti nell’Unione e il destinatario del trasferimento** stabilito nel paese terzo interessato quanto, per quel che riguarda un eventuale accesso delle autorità pubbliche di tale paese terzo ai dati personali così trasferiti, **gli elementi rilevanti del sistema giuridico di quest’ultimo**, in particolare quelli enunciati all’articolo 45, paragrafo 2, di detto regolamento.

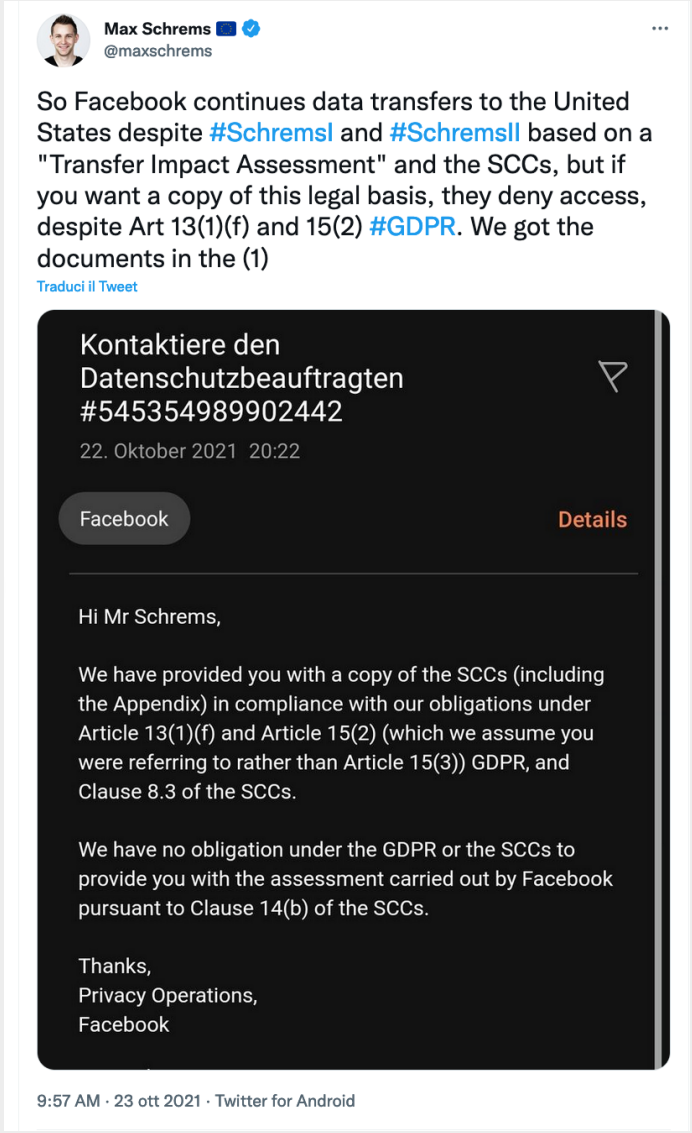
3. Corte di Giustizia UE sentenza 16 luglio 2020 C-311/18 (Schrems II)

- L'articolo 58, paragrafo 2, lettere f) e j), del regolamento 2016/679 deve essere interpretato nel senso che, a meno che esista una decisione di adeguatezza validamente adottata dalla Commissione europea, **l'autorità di controllo competente è tenuta a sospendere o a vietare un trasferimento di dati verso un paese terzo effettuato sulla base di clausole tipo di protezione dei dati adottate dalla Commissione, qualora detta autorità di controllo ritenga, alla luce del complesso delle circostanze proprie di tale trasferimento, che le suddette clausole non siano o non possano essere rispettate in tale paese terzo e che la protezione dei dati trasferiti richiesta dal diritto dell'Unione, segnatamente dagli articoli 45 e 46 di tale regolamento e dalla Carta dei diritti fondamentali, non possa essere garantita con altri mezzi**, ove il titolare del trattamento o il responsabile del trattamento stabiliti nell'Unione non abbiano essi stessi sospeso il trasferimento o messo fine a quest'ultimo.

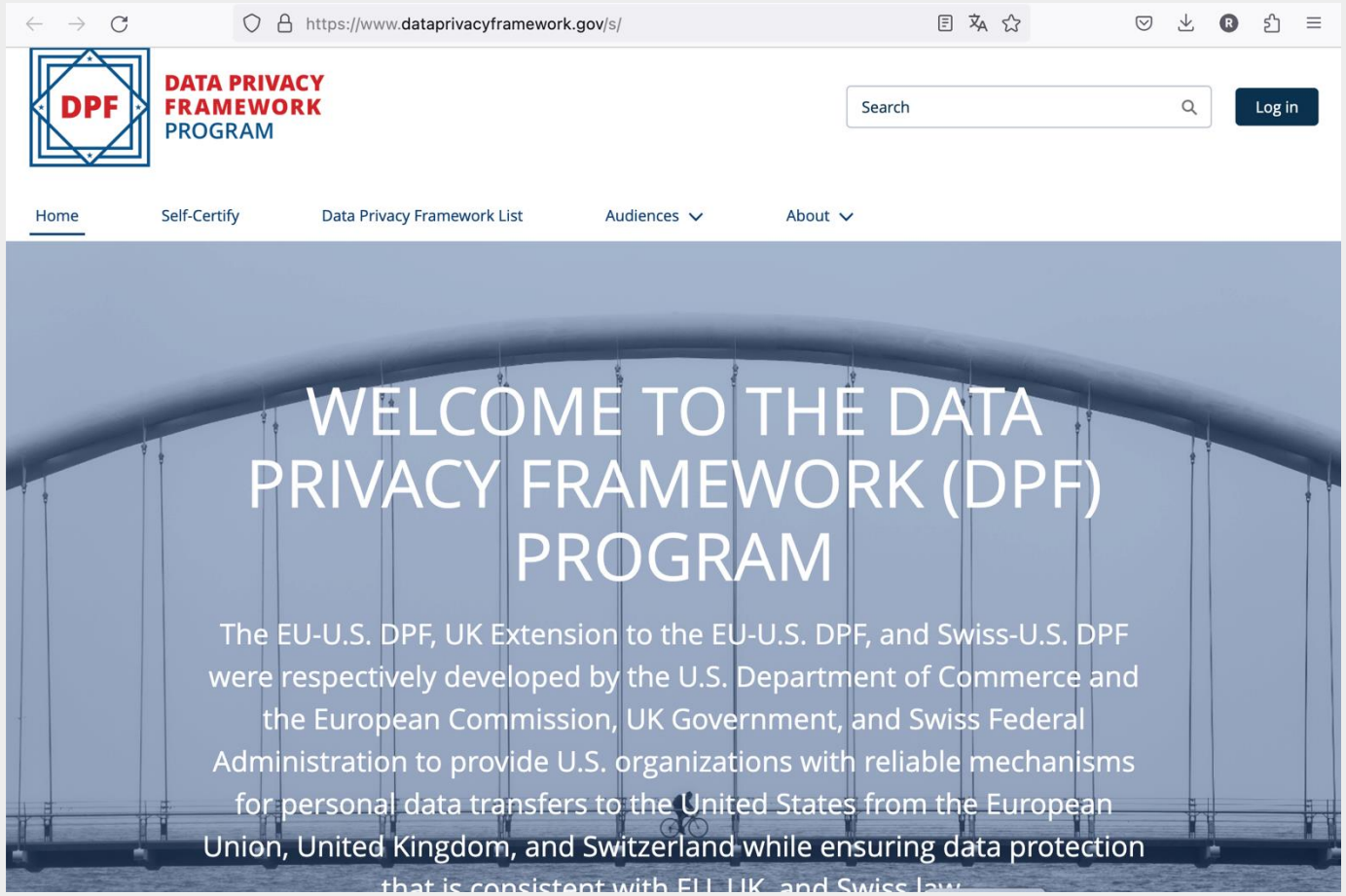
3. Corte di Giustizia UE sentenza 16 luglio 2020 C-311/18 (Schrems II)

- La decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy, è invalida.

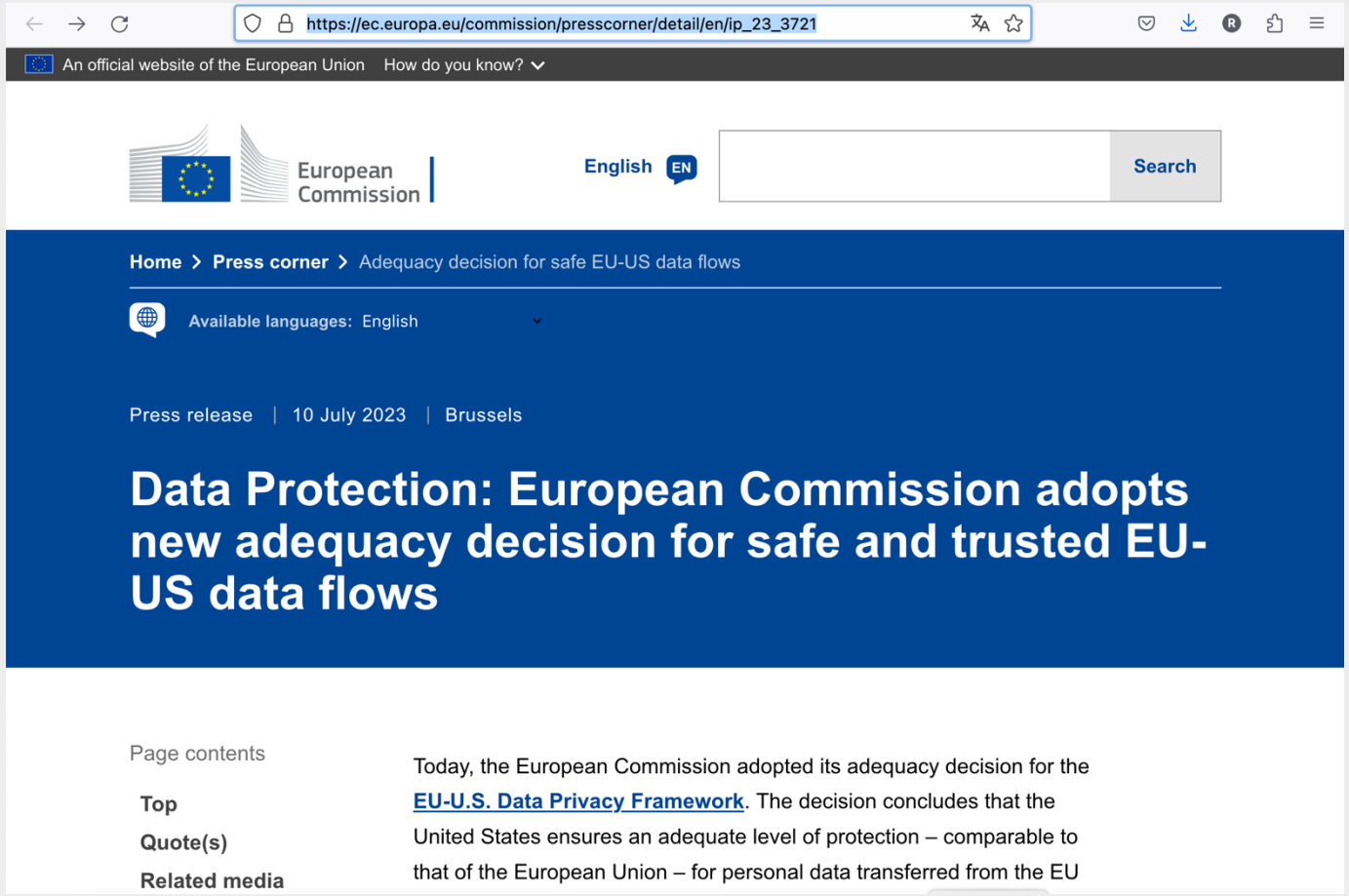
3. Com’è andata a finire?



3. https://www.dataprivacyframework.gov/s/

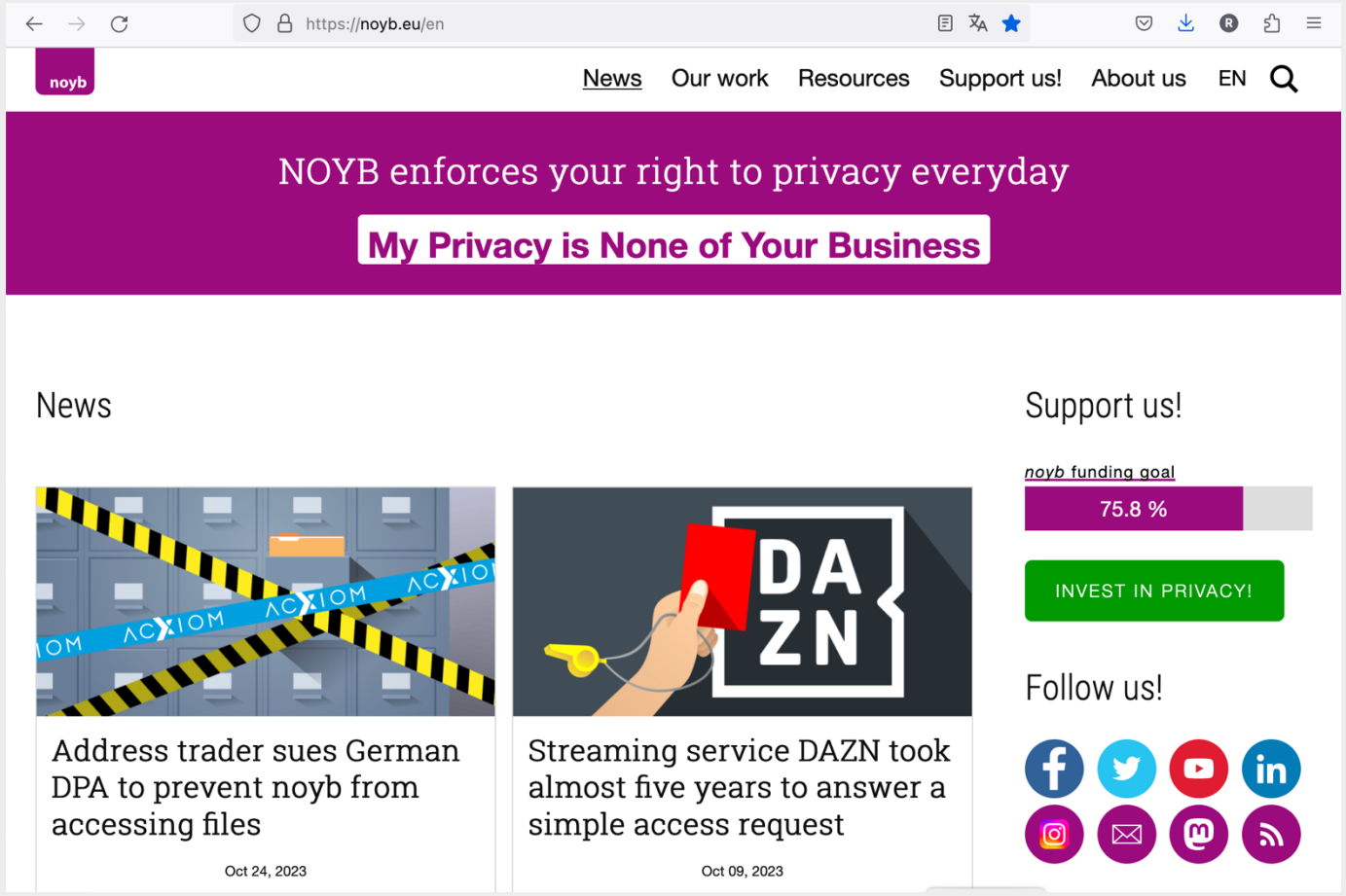


3.https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721



3. Come sta andando a finire?

3. Come sta andando a finire?



3. Caso e problema 1 – Una possibile soluzione

- Ordinanza ingiunzione nei confronti di Università Commerciale “Luigi Bocconi” di Milano - 16 settembre 2021 [9703988]

- https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9703988

3. Problema 1

- L’impiego da parte della Bocconi di un sistema di supervisione (proctoring) nell’ambito dello svolgimento delle verifiche scritte degli studenti, al fine di identificare questi ultimi e/o di verificarne il corretto comportamento durante lo svolgimento della prova d’esame costituisce violazione della disciplina di protezione dei dati personali?

3. GPDP 16 settembre 2021 [9703988]

- La correttezza e la trasparenza del trattamento: l'informativa
- L'assenza di base giuridica per il trattamento di dati biometrici degli studenti (no consenso; no disposizione normativa)
- L'analisi del comportamento degli studenti nel corso della prova d'esame (profilazione)
- Protezione dei dati fin dalla progettazione e per impostazione predefinita, minimizzazione e limitazione della conservazione
- Trasferimenti internazionali di dati personali (→ USA)
- La valutazione di impatto sulla protezione dei dati

3. Cass. Civile Ord. Sez. 1 Num. 12967 Anno 2024

- In tema di trattamento dei dati personali, ai sensi dell'art.9 del Reg (UE) 2016/679, ricorre un trattamento di dati biometrici, come definiti dall'art. 4, n.14 del Regolamento 2016/679, quando i dati personali sono ottenuti mediante un trattamento tecnico automatizzato specifico, realizzato con un software che, sulla base di riprese e analisi delle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, le elabora, evidenziando comportamenti o elementi anomali, e che perviene a un esito conclusivo, costituito da una elaborato video/foto che consente (o che conferma) l'identificazione univoca della persona fisica, restando irrilevante la circostanza che l'esito finale del trattamento sia successivamente sottoposto alla verifica finale di una persona fisica.

3. Cass. Civile Ord. Sez. 1 Num. 12967 Anno 2024

- Con la sentenza del 16 luglio 2020 relativa alla causa C-311/18, la Corte di Giustizia europea ha dichiarata invalida la decisione 2016/1250 della Commissione sull'adeguatezza della protezione offerta dal regime del Privacy Shield, lo scudo UE-USA per la protezione dei dati personali oggetto di trasferimento verso gli Stati Uniti. Essa ha giudicato, invece, valida la decisione 2010/87 relativa alle Clausole Contrattuali Tipo (SCC) per il trasferimento di dati personali a destinatari stabiliti in Paesi terzi.

3. Cass. Civile Ord. Sez. 1 Num. 12967 Anno 2024

- A seguito di questa decisione è intervenuto tra l'Università Bocconi e la società Respondus un accordo di modifica sottoscritto in data 18 agosto 2020, con il quale sono state recepite le clausole contrattuali tipo dettate nella Decisione della Commissione europea del 5 febbraio 2010 n. 87/UE.

3. Cass. Civile Ord. Sez. 1 Num. 12967 Anno 2024

Segnatamente, il Tribunale, sul rilievo che l'allegato si compone di due appendici, di cui la prima descrive il tipo di trattamento e la seconda indica le misure tecniche- organizzative implementate da Responsus e da Amazon Web Service, sub-responsabile di Respondus, ha ritenuto corrette le clausole allegate mediante semplice rinvio *per relationem*, sia sul piano formale che sul piano sostanziale, osservando che il rispetto delle stesse era idoneo a garantire agli interessati una tutela adeguata rispetto agli standard europei.

3. Cass. Civile Ord. Sez. 1 Num. 12967 Anno 2024

- Va, quindi, evidenziato che la clausola 4, par. 1, lett. c) e la clausola 5, lett. c) delle clausole standard, prevedono espressamente che le misure di sicurezza debbano essere appunto “indicate nell’appendice 2” e che nella stessa appendice 2 si specifica che essa “costituisce parte integrante delle clausole contrattuali e deve essere compilata e sottoscritta dalle parti”, contemplando una specifica sezione, denominata «Descrizione delle misure tecniche e organizzative di sicurezza attuate dall’importatore in conformità della clausola 4, lettera d), e della clausola 5, lettera c) (o del documento/atto legislativo allegato)» e che tali disposizioni hanno efficacia anche con riferimento all’ “interessato”, che non è parte contraente, ma terzo beneficiario.

3. Cass. Civile Ord. Sez. 1 Num. 12967 Anno 2024

- Alla luce di tali disposizioni, risulta errata al tesi del Tribunale secondo la quale il contenuto delle clausole contrattuali recanti le misure di sicurezza può essere determinato tramite rinvio ad un documento esterno al contratto stesso […]

3. Cass. Civile Ord. Sez. 1 Num. 12967 Anno 2024

trasferimento o messo fine a quest'ultimo.». Si deve, in proposito osservare che, nel caso in esame, la mancata esplicitazione delle misure di sicurezza nell'allegato 2, in difformità da quanto da questo previsto, la complessità, non contestata, della modalità di accesso informatico alle misure di sicurezza e l'incertezza sul contenuto delle stesse, come evidenziate dall'Autorità di controllo, sono circostanze che avrebbero dovuto essere espressamente valutate dal Tribunale in ordine all'applicabilità dell'art.58, par. 2, lett. f) e j), del regolamento 2016/679.

Riferimenti

- R. Ducato et al., Emergency Remote Teaching: a study of copyright and data protection policies of popular online services (Part II), Kluwer Copyright Blog, June 4, 2020
- M.C. Pievatolo, Teledidattica: proprietaria e privata o libera e pubblica, in Roars, 8 giugno, 2020

Riferimenti

- R. Caso, M.C. Pievatolo, A liberal infrastructure in a neoliberal world: the Italian case of GARR, in Journal of Intellectual Property, Information Technology and Electronic Commerce – JIPITEC 14 (2) 2023, preprint available at Zenodo, https://doi.org/10.5281/zenodo.7561821
- P. Guarda, G. Bincoletto, Diritto comparato della privacy, Milano, Ledizioni, 2023, 357 ss., https://zenodo.org/records/7805085
- A. Catalano, La didattica del capitalismo della sorveglianza: profili giuridici, Trento Law and Technology Research Group, Student Paper Series; 90. Trento: Università degli Studi di Trento, https://zenodo.org/records/10047844

Roberto Caso

E-mail:
roberto.caso@unitn.it

Web:
http://www5.unitn.it/People/it/Web/Persona/PER0000633#INFO
http://lawtech.jus.unitn.it/
https://www.robertocaso.it/

Copyright