Valutazione d’impatto sulla protezione dei dati nel sistema giudiziario e sicurezza dei dati

Stefano Leucci
26 novembre 2018
Centro Nexa per Internet e Società

—

Main goals:

- dimensione pratica collegata a dimensione giuridica;
- fornire un set di toolkit e risorse per approfondire in seguito;
- andare oltre la “semplice” compliance.

CORRIERE DELLA SERA

MILANO / CRONACA

0

765

IL CASO

Attacco hacker, tribunali in tilt. Timori per le mail dei magistrati

Nel mirino degli hacker il centro dati Telecom di Pomezia, dove in tre edifici l'azienda gestisce 4.200 server. Csm, consiglieri in allarme

di Luigi Ferrarella

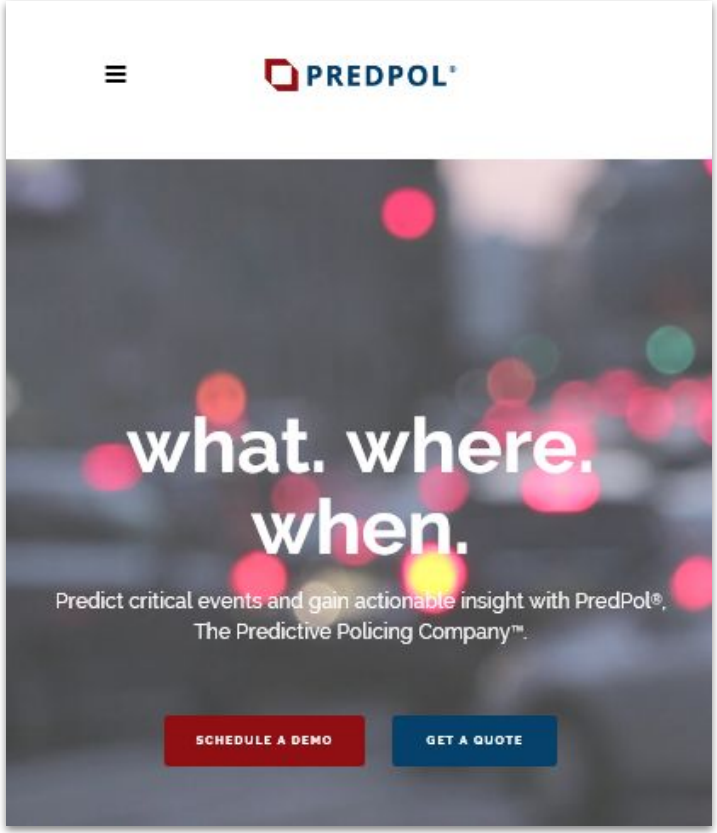
Corriere della Sera - 14 novembre 2018

—

Policing and biometric border control

COMPAS

Correctional Offender Management Profiling for Alternative Sanctions



Predicting crimes

Rischio

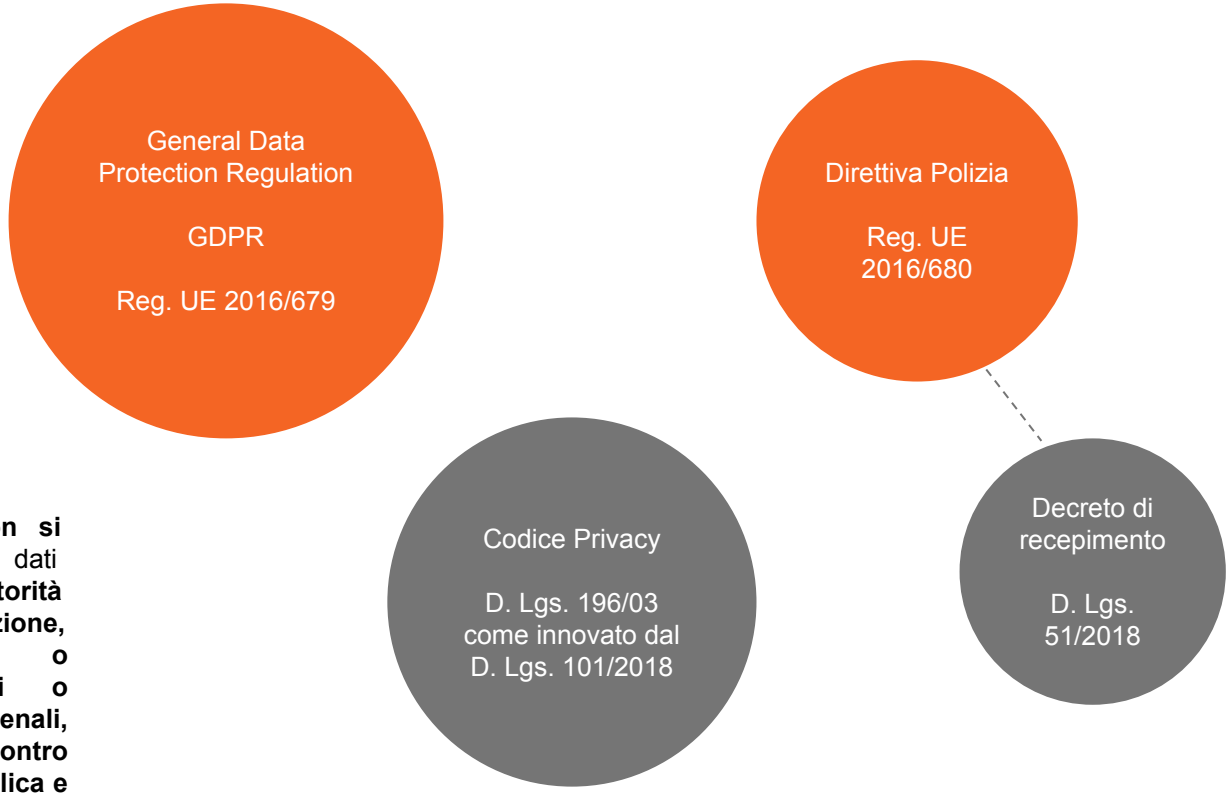
*Un rischio è uno scenario che descrive un evento e le sue conseguenze, valutate in termini di **probabilità** e **impatto**.*

Working Party Article 29 - WP248

Risk management

L'insieme di attività volte a dirigere e governare un'organizzazione con riferimento al rischio.

Working Party Article 29 - WP248



Art. 2, comma 2, GDPR:

Il presente regolamento **non si applica** ai trattamenti di dati personali effettuati dalle **autorità competenti** a fini di **prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse**.

Rischi informatici - misure di sicurezza

GDPR - Art. 32

Tenendo conto

- dello stato dell'arte,
- dei costi di attuazione,
- nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento
- come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche

il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio [...]

Dir. Polizia - Art. 29

Gli Stati membri dispongono che il titolare e il responsabile, tenuto conto

- dello stato dell'arte,
- dei costi di attuazione,
- nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento,
- come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche,

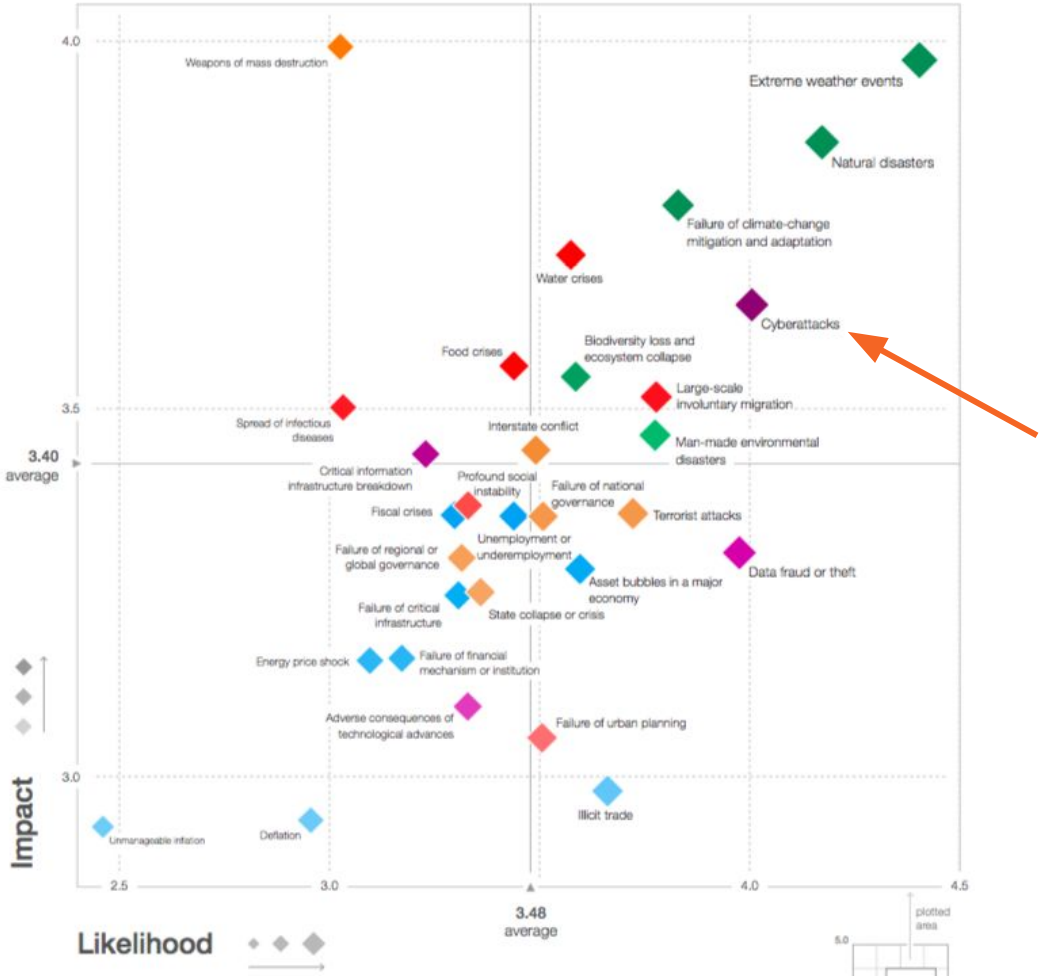
mettano in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, in particolare riguardo al trattamento di categorie particolari di dati personali di cui all'articolo 10.

—

World Economic Forum 2018

The Global Risks

- Nuovi approcci alla tecnologia (IoT, BigData, BYOD, Smart Working)
- Nuove metodologie di attacco (Ransomware, cryptoware)
- Nuovo potenziale disruptive (larga scala e infezione immediata di reti)



Fonte: The Global Risks - Report 2018 13th Edition - http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

—

ENISA Threat Landscape Report 2017

15 Top Cyber-Threats and Trends

January 2018

https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

Top Threats 2016	Assessed Trends 2016	Top Threats 2017	Assessed Trends 2017	Change in ranking
1. Malware	↑	1. Malware	⊃	→
2. Web based attacks	↑	2. Web based attacks	↑	→
3. Web application attacks	↑	3. Web application attacks	↑	→
4. Denial of service	↑	4. Phishing	↑	↑
5. Botnets	↑	5. Spam	↑	↑
6. Phishing	⊃	6. Denial of service	↑	↓
7. Spam	↓	7. Ransomware	↑	↑
8. Ransomware	⊃	8. Botnets	↑	↓
9. Insider threat	⊃	9. Insider threat	⊃	→
10. Physical manipulation/damage/ theft/loss	↑	10. Physical manipulation/damage/ theft/loss	⊃	→
11. Exploit kits	↑	11. Data breaches	↑	↑
12. Data breaches	↑	12. Identity theft	↑	↑
13. Identity theft	↓	13. Information leakage	↑	↑
14. Information leakage	↑	14. Exploit kits	↓	↓
15. Cyber espionage	↓	15. Cyber espionage	↑	→

Legend: Trends: ↓ Declining, ⊃ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Misurazione dei rischi informatici

- se il rischio varia rapidamente, anche la misurazione dev’essere quanto più continua;
- gli strumenti di misurazione devono essere snelli e adattabili a diversi contesti.

ENISA Methodology - Handbook on Security of Personal Data Processing - December 2017
https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

Valutazione degli impatti

Si tratta di una valutazione qualitativa, tenendo presente tutti i paramentri indicati dal GDPR (tipi di dati personali trattati e di soggetti, volumi).

In particolare, tre aspetti devono essere misurati:

- **perdita di confidenzialità**: valutazione dell'impatto che un accesso non autorizzato può avere su un individuo;
- **perdita di integrità**: valutazione che una modifica non autorizzata può avere su un individuo;
- **perdita di disponibilità**: impatto che una distruzione o una perdita di dati può avere su un individuo.

enisa
European Network and Information Security Agency

Valutazione delle probabilità

Misurare le probabilità di avvenimento di una minaccia, in merito alle seguenti quattro dimensioni:

- sistemi tecnici e di rete (hardware e software);
- processi e procedure;
- persone e fornitori coinvolti nel trattamento;
- settore di attività svolta.

Importante definire le giuste domande per valutare le probabilità in base al contesto di applicazione.

enisa
European Network and Information Security Agency

Valutazione del rischio

IMPACT LEVEL

THREAT OCCURRENCE PROBABILITY	Low	Medium	High / Very High
Low			
Medium			
High			

Legend

Low Risk *Medium Risk* *High Risk*

enisa
European Network and Information Security Agency

Misure di sicurezza adeguate

- In base al **contesto applicativo**, ad ogni livello di rischio è collegato un set di misure di sicurezza;
- solo analizzando **caso per caso** ogni sistema di trattamento di dati personali si possono identificare misure veramente necessarie, proporzionate al rischio;
- solo tramite **periodiche revisioni** del modello di sicurezza può essere garantito una tendenza allo stato dell'arte disponibile sul mercato.

Probabilità x Impatto = Rischio inerente - Contromisure = Rischio residuo

enisa
European Network and Information Security Agency

Misure di sicurezza nel sistema giudiziario

Per **Avvocati**:

“L'avvocato è inoltre soggetto al **segreto professionale assoluto** e deve, ancor più per questo motivo, assicurare la sicurezza dei dati affidatigli”.

Il GDPR e l’Avvocato:
https://www.consiglionazionaleforense.it/documents/20182/445621/IL+GDPR+E+L%27AVVOCATO/ef231b75-2066-43df-8d88-570bf0ea98b3

Per gli **enti amministrativi**:

Misure minime di sicurezza ICT per le pubbliche amministrazioni

Le misure minime di sicurezza ICT emanate dall’AgID intendono **contrastare le minacce informatiche più frequenti della pubblica amministrazione italiana**.

https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

Per le “**Autorità competenti**” (art. 29 comma 2, Dir. Polizia):

- controllo dell'accesso alle attrezzature
- controllo dei supporti di dati
- controllo della conservazione
- controllo dell'utente
- controllo dell'accesso ai dati
- controllo della trasmissione
- controllo dell'introduzione
- controllo del trasporto
- recupero
- affidabilità
- integrità

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

Art. 33 - GDPR
(Art. 30 - Dir. Polizia)

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.**

Art. 34 - GDPR
(Art. 31 - Dir. Polizia)

Quando la violazione dei dati personali è suscettibile di presentare **un rischio elevato per i diritti e le libertà delle persone fisiche**, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

Working Party Article 29 - Guidelines on Personal data breach notification under Regulation 2016/679 - WP250
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

Valutazione d’impatto sulla protezione dei dati (DPIA)

DPIA is a process for building and demonstrating compliance.

Working Party Article 29 - WP248

Data Protection Impact Assessment

Art. 35 - GDPR

Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un **rischio elevato per i diritti e le libertà delle persone fisiche**, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

Art. 27 - Dir. Polizia

Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, può presentare un **rischio elevato per i diritti e le libertà delle persone fisiche**, gli Stati membri dispongono che il titolare del trattamento effettui, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

Asset di partenza: Registro dei trattamenti

quando

chi

come

...prima di procedere al trattamento...

**...quando un tipo di trattamento [...]
può presentare un rischio elevato
per i diritti e le libertà delle persone fisiche...**

quando

chi

come

Nove criteri del WP29:

- valutazione o assegnazione di un punteggio
- processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
- monitoraggio sistematico
- dati sensibili o dati aventi carattere altamente personale
- trattamento di dati su larga scala
- creazione di corrispondenze o combinazione di insiemi di dati
- dati relativi a interessati vulnerabili
- uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative
- quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Esempi in cui DPIA è necessaria:

- Un ospedale che tratta i dati genetici e sanitari dei propri pazienti (sistema informativo ospedaliero)
- L'uso di un sistema di telecamere per monitorare il comportamento di guida sulle autostrade. Il titolare del trattamento prevede di utilizzare un sistema intelligente di analisi video per individuare le auto e riconoscere automaticamente le targhe.
- Un'azienda che monitora sistematicamente le attività dei suoi dipendenti, controllando anche la postazione di lavoro dei dipendenti, le loro attività in Internet, ecc.
- Un'istituzione che crea una banca dati antifrode e di gestione del rating del credito a livello nazionale.

quando

chi

come

quando

chi

come

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

ALLEGATO 1 AL PROVVEDIMENTO N. 467 DELL'11 OTTOBRE 2018 [doc. web n. 9058979]

(Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018)

Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto

Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 [doc. web: 9058979]
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9058979

quando

chi

come

DPIA non necessaria se:

- trattamento non comporta rischi elevati;
- è già stata svolta DPIA per un trattamento simile;
- le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018;
- **qualora un trattamento trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro**, tale diritto disciplini il trattamento specifico o sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica;
- qualora il trattamento sia incluso nell'elenco facoltativo (stabilito dall'autorità di controllo) delle tipologie di trattamento per le quali non è richiesta.

Esempi in cui DPIA non è necessaria:

- Un trattamento di "dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato" (considerando 91)
- Una rivista online che utilizza una lista di distribuzione per inviare una selezione quotidiana generica ai suoi abbonati.
- Un sito web di commercio elettronico che visualizza annunci pubblicitari per parti di auto d'epoca che comporta una limitata profilazione basata sugli articoli visualizzati o acquistati sul proprio sito web.

quando

chi

come

quando

chi

come

Titolare del trattamento svolge la DPIA.

Responsabile del trattamento supporta il Titolare nei casi in cui è coinvolto.

Data Protection Officer è consultato dal Titolare in merito alla metodologia e ne monitora lo svolgimento.

Soggetti interessati sono interessati per raccoglierne le opinioni e i punti di vista.

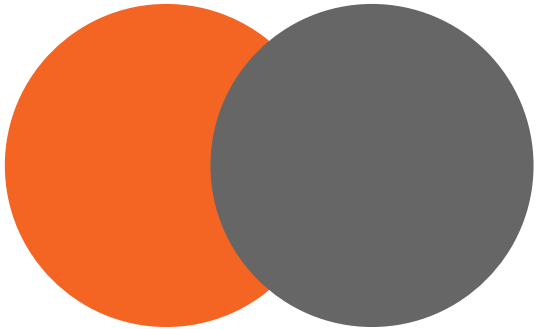
quando

chi

come

Cyber risk vs Privacy risk

Il sistema di eGate biometrico può essere sicuro dal punto di vista cyber, ma potrebbe impedire ad un soggetto di salire su un aereo a causa di un bias nell'algoritmo di identificazione.



	Cyber risk	***Privacy risk***
obiettivo	rischi per l’organizzazione (interni)	rischi per i diritti e le libertà delle persone fisiche (esterni)
asset	sistema, processo o servizio IT	trattamento di dati personali
parametri	minacce	azioni problematiche sui dati
contromisure	misure di sicurezza tecniche e/o organizzative	controlli, parametri e misure di sicurezza tecniche e / organizzative (anche in comune con cyber risk)

quando

chi

come

Loss of Opportunity		
Employment Discrimination	E.g. Filtering job candidates by race or genetic/health information E.g. Filtering candidates by work proximity leads to excluding minorities	**Differential Access to Job Opportunities**
Insurance & Social Benefit Discrimination	E.g. Higher termination rate for benefit eligibility by religious group E.g. Increasing auto insurance prices for night-shift workers	**Differential Access to Insurance & Benefits**
Housing Discrimination	E.g. Landlord relies on search results suggesting criminal history by race E.g. Matching algorithm less likely to provide suitable housing for minorities	**Differential Access to Housing**
Education Discrimination	E.g. Denial of opportunity for a student in a certain ability category E.g. Presenting only ads on for-profit colleges to low-income individuals	**Differential Access to Education**

Future of Privacy Forum - Distilling the harms
https://fpf.org/wp-content/uploads/2018/11/Curriculum-2_DDF-1_FPF-Automated-Decision-Making-Harms-and-Mitigation-Charts.pdf

quando

chi

come

Economic Loss		
Credit Discrimination E.g. Denying credit to all residents in specified neighborhoods ("redlining")	E.g. Not presenting certain credit offers to members of certain groups	**Differential Access to Credit**
Differential Pricing of Goods and Services E.g. Raising online prices based on membership in a protected class	E.g. Presenting product discounts based on "ethnic affinity"	**Differential Access to Goods and Services**
	Narrowing of Choice E.g. Presenting ads based solely on past "clicks"	**Narrowing of Choice for Groups**

Future of Privacy Forum - Distilling the harms
https://fpf.org/wp-content/uploads/2018/11/Curriculum-2_DDF-1_FPF-Automated-Decision-Making-Harms-and-Mitigation-Charts.pdf

quando

chi

come

Social Detriment

Network Bubbles
E.g. Varied exposure to opportunity or evaluation based on “who you know”

Filter Bubbles
E.g. Algorithms that promote only familiar news and information

Dignitary Harms
E.g. Emotional distress due to bias or a decision based on incorrect data

Stereotype Reinforcement
E.g. Assumption that computed decisions are inherently unbiased

Constraints of Bias
E.g. Constrained conceptions of career prospects based on search results

Confirmation Bias
E.g. All-male image search results for “CEO,” all-female results for “teacher”

Future of Privacy Forum - Distilling the harms
https://fpf.org/wp-content/uploads/2018/11/Curriculum-2_DDF-1_FPF-Automated-Decision-Making-Harms-and-Mitigation-Charts.pdf

quando

chi

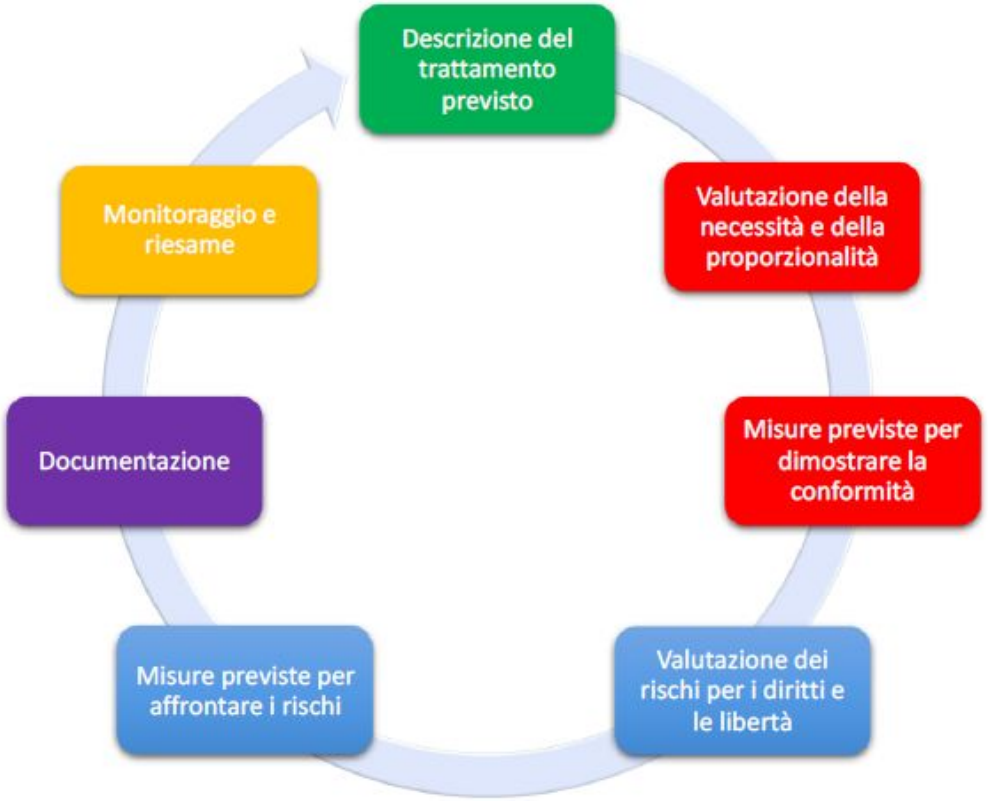
come

Future of Privacy Forum - Distilling the harms
https://fpf.org/wp-content/uploads/2018/11/Curriculum-2_DDF-1_FPF-Automated-Decision-Making-Harms-and-Mitigation-Charts.pdf

quando

chi

come



quando

chi

come

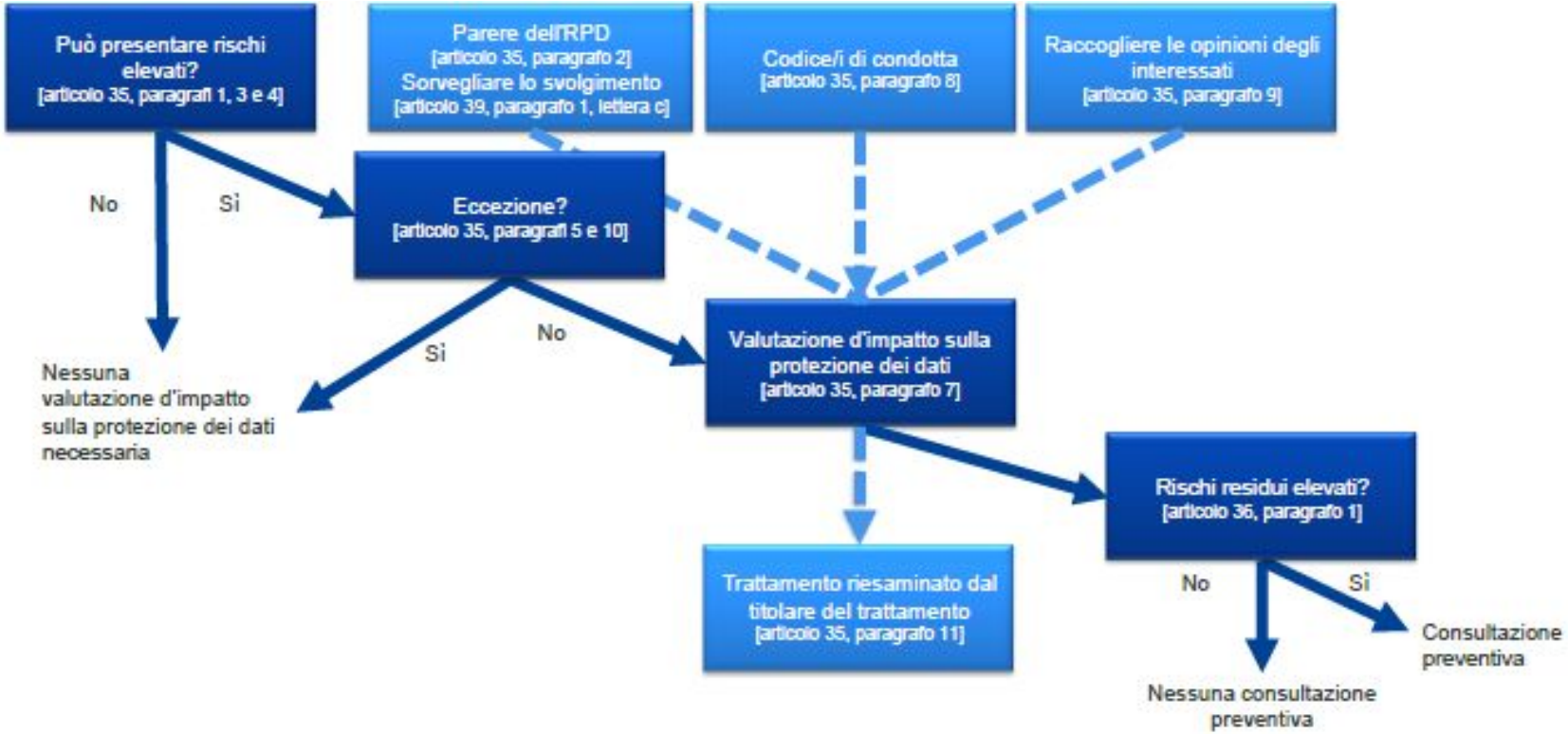
Metodologie

Metodologie generali - Garanti Europei:

- **Germania**: Standard Data Protection Model, V.1.0 – Trial version, 201631 https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- **Spagna**: Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD), Agencia española de protección de datos (AGPD), 2014. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- **Francia**: Privacy Impact Assessment (PIA), Commission nationale de l'informatique et des libertés (CNIL), 2015. https://www.cnil.fr/fr/node/15798
- **UK**: Conducting privacy impact assessments code of practice, Information Commissioner's Office (ICO), 2014. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Metodologie specifiche:

- Privacy and Data Protection Impact Assessment Framework for RFID Applications - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems - http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf
- ISO/IEC 2913434



Flusso logico - WP29

DPIA nel settore giudiziario

Per **Avvocati**:

“Le DPIA consentono all’avvocato di prendere coscienza di trattare dati personali e sensibili del cliente, e di prevedere per essi l’adozione di misure di sicurezza adeguate”

Il GDPR e l’Avvocato:
https://www.consiglionazionaleforense.it/documents/20182/445621/IL+GDPR+E+L%27AVVOCATO/ef231b75-2066-43df-8d88-570bf0ea98b3

Per gli **enti amministrativi**:

- unica base legale del trattamento per enti pubblici è l’obbligo di legge;
- dunque la DPIA non indaga il SE, ma il COME;
- strumento consigliato per accountability.

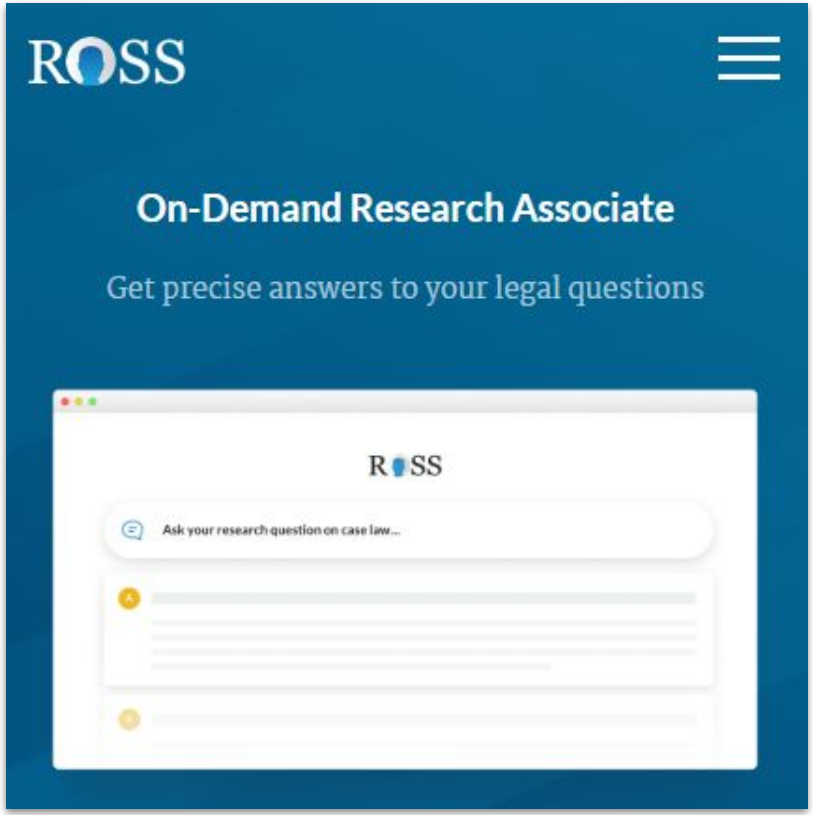
—

kira

It's How You Know

What's In Your Contracts

Kira is a powerful machine learning software that identifies, extracts, and analyzes text in your contracts and other documents.



Anche se...

Policing and biometric border control

—

Support The Guardian

Contribute → Subscribe →

Sign in

The Guardian

News | Opinion | Sport | Culture | Lifestyle

Australia World **AU politics** Environment Football Indigenous Australia More

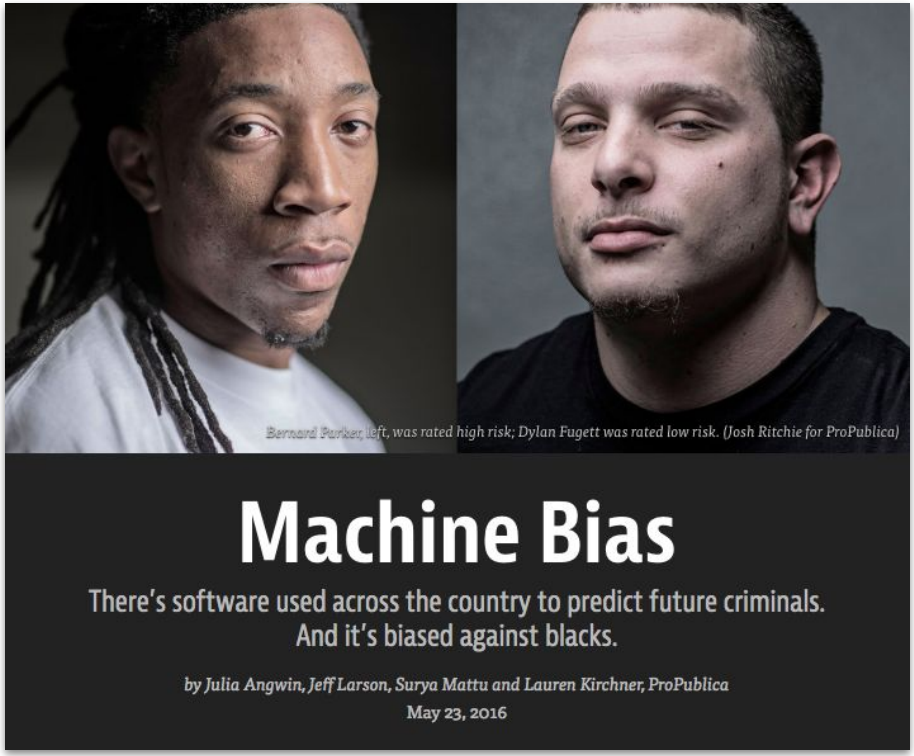
Facial recognition

Facial matching system risks racial bias, Human Rights Law Centre warns

Submission says bill would disproportionately affect ethnic minorities, and damage freedom of assembly and expression

● Sign up to receive the top stories from Guardian Australia every morning

Policing and biometric border control



Predicting crimes

In conclusione

- computer scientist = social scientist?
- strumento di **governo** della predominanza tecnologica e degli effetti **sociali** e delle implicazioni **etiche**;
- strumento di avvicinamento tra mondo delle **regole giuridiche e informatiche**.

Grazie.