UNIVERSITÀ DEGLI STUDI DI UDINE

CONSIGLIO NAZIONALE DEGLI INGEGNERI

In collaborazione con: ORDINE DEGLI INGEGNERI PROVINCIA DI PORDENONE; Ordine degli Ingegneri Monza e Brianza; NuMe RESEARCH LABORATORY FOR NEW MEDIA

Con il patrocinio di: C3i COMITATO ITALIANO INGEGNERIA DELL'INFORMAZIONE

Interesse nazionale e tutela dei dati personali

Webinar «CYBERSECURITY E RESILIENZA NAZIONALE: complessità, problemi e prospettive»

Giovedì 18 novembre 2021 – ore 15:00 – 18:30

Federico Costantini, DISG / UNIUD

Webinar C/O Gotomeeting

Interesse nazionale e tutela dei dati personali

1.- Il contesto e il problema

Sorveglianza e profilazione tra retorica dei «diritti dell'uomo» e pigrizia consumeristica

2.- I principi del GDPR

La tutela dell'interesse pubblico nel Regolamento (UE) 679/2016

3.- Le direttive «gemelle»

Cenni sulla disciplina derogatoria rispetto al GDPR contenuta nelle Direttive (UE) 680/2016 «Polizia» (D.Lgs. 51/2018) e 681/2016 «PRN» (D.Lgs. 53/2018)

4.- Cybersecurity e tutela dei dati personali

DIRETTIVA (UE) 2016/1148 «N.I.S.» (D. Lgs. 65/2018)
D.L. 105/2019 «perimetro di sicurezza nazionale cibernetica»
REGOLAMENTO (UE) 2019/881 «Cybersecurity Act»

5.- Videosorveglianza e dati biometrici

Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video

6.- Prospettive future e conclusioni provvisorie

COM/2018/640 final, Proposta di REGOLAMENTO (UE) relativo alla prevenzione della diffusione di contenuti terroristici online
COM/2020/823 final Proposta di DIRETTIVA relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148 c.d. NIS 2.0
COM/2020/825 final, Proposta di REGOLAMENTO relativo a un mercato unico dei servizi digitali (Digital Service Act)
COM/2020/829 final, Proposta di DIRETTIVA sulla resilienza dei soggetti critici
COM/2021/206 final, Proposta di REGOLAMENTO (Artificial Intelligence Act)

UNIVERSITÀ
DEGLI STUDI
DI UDINE

1.- Il contesto e il problema

Sorveglianza e profilazione tra retorica dei «diritti dell'uomo» e pigrizia consumeristica

- Proviamo a superare uno dei luoghi comuni in tema di cybersecurity
- Facciamo «Debunking» (?)
- Critichiamo la contrapposizione piuttosto comune tra due termini

«Giusto» difendersi da un governo un po' troppo attento a quello che facciamo!

Stato

Utente

«Giusto» sorvegliare un utente che, appena ne ha la possibilità (e la tecnologia) si dedica ad attività illecite!

Il controllo dell'informazione, in questo contesto,

- Si pone in termini assoluti (o tutto, o niente)
- Si pone in termini esclusivi (uno soltanto ne può essere titolare)
- Non distingue tra «pubblico» e «privato» (USA? Facebook? Google? Cina?)
- Non fornisce criteri definitivi di giustizia (dipende dalle preferenze del titolare)

- Un esempio concreto: l’informativa cookies
- «reality check» (?)
- Tutti sanno che quell’informativa riguarda dei diritti ma ... qualcuno la legge?
- Qualcuno dubita ancora di essere profilato su Internet?

Informativa

Noi e terze parti selezionate utilizziamo cookie o tecnologie simili per finalità tecniche e, con il tuo consenso, anche per altre finalità come specificato nella cookie policy.
Per quanto riguarda la pubblicità, noi e terze parti selezionate, potremmo *utilizzare dati di geolocalizzazione precisi* e *fare una scansione attiva delle caratteristiche del dispositivo ai fini dell'identificazione*, al fine di *archiviare e/o accedere a informazioni su un dispositivo* e trattare dati personali come i tuoi dati di utilizzo, per le seguenti finalità: *annunci e contenuti personalizzati, valutazione degli annunci e del contenuto, osservazioni del pubblico e sviluppo di prodotti*.
Puoi liberamente prestare, rifiutare o revocare il tuo consenso, in qualsiasi momento, accedendo al pannello delle preferenze pubblicitarie.
Puoi acconsentire all'utilizzo di tali tecnologie chiudendo questa informativa.

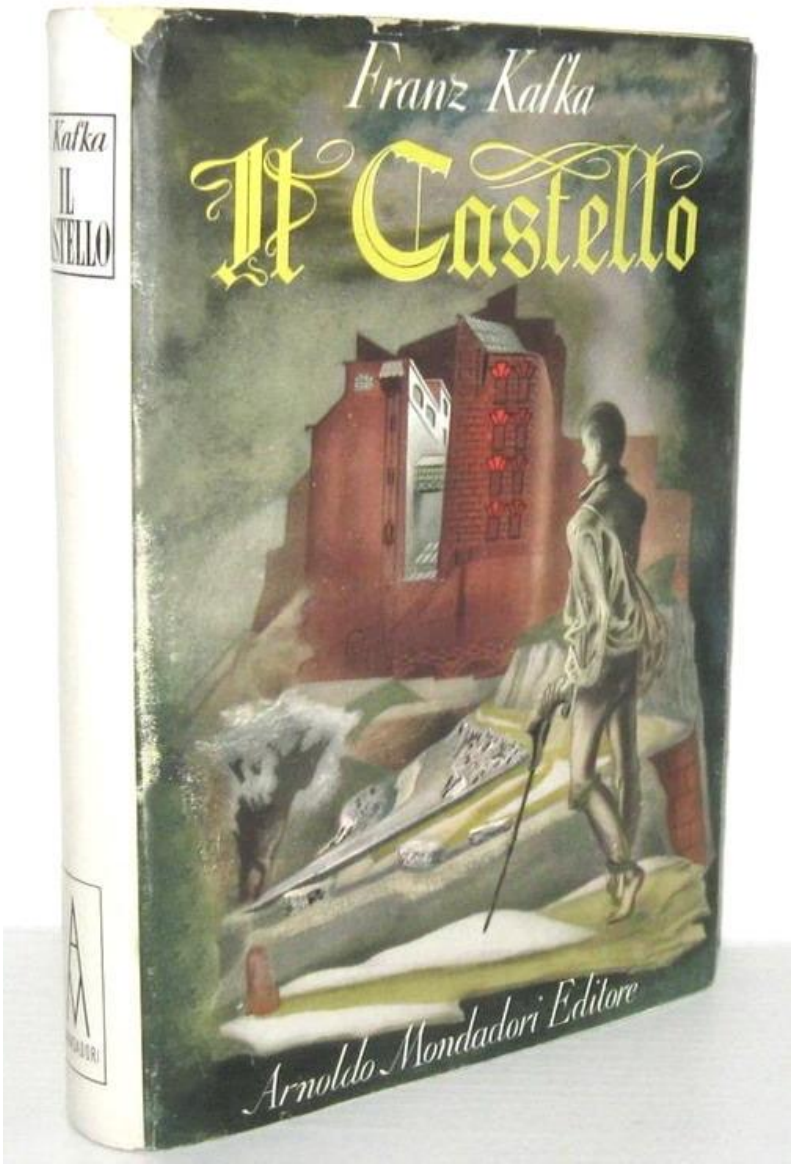
Scegli e personalizza **Accetta**

I dati personali sono qualcosa di molto più complesso, non risolvibile da una semplice contrapposizione come si pensa comunemente…

Essi rappresentano una proiezione dell'individualità (la «traccia digitale»), ma dicono qualcosa anche …

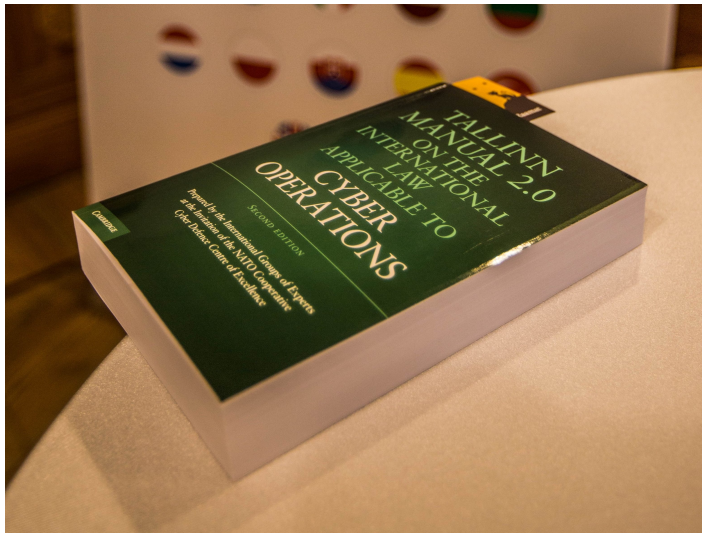
- Del nostro rapporto con il potere (le «istituzioni)
- Del nostro rapporto con noi stessi (la parte «oscura»)

Tutto questo sfugge al controllo dell'individuo ma anche (per ora) del potere costituito



https://www.libriantichionline.com/novecento/franz_kafka_castello_1948

Il fatto è che il «castello» deve comunque esser difeso dagli attacchi esterni...

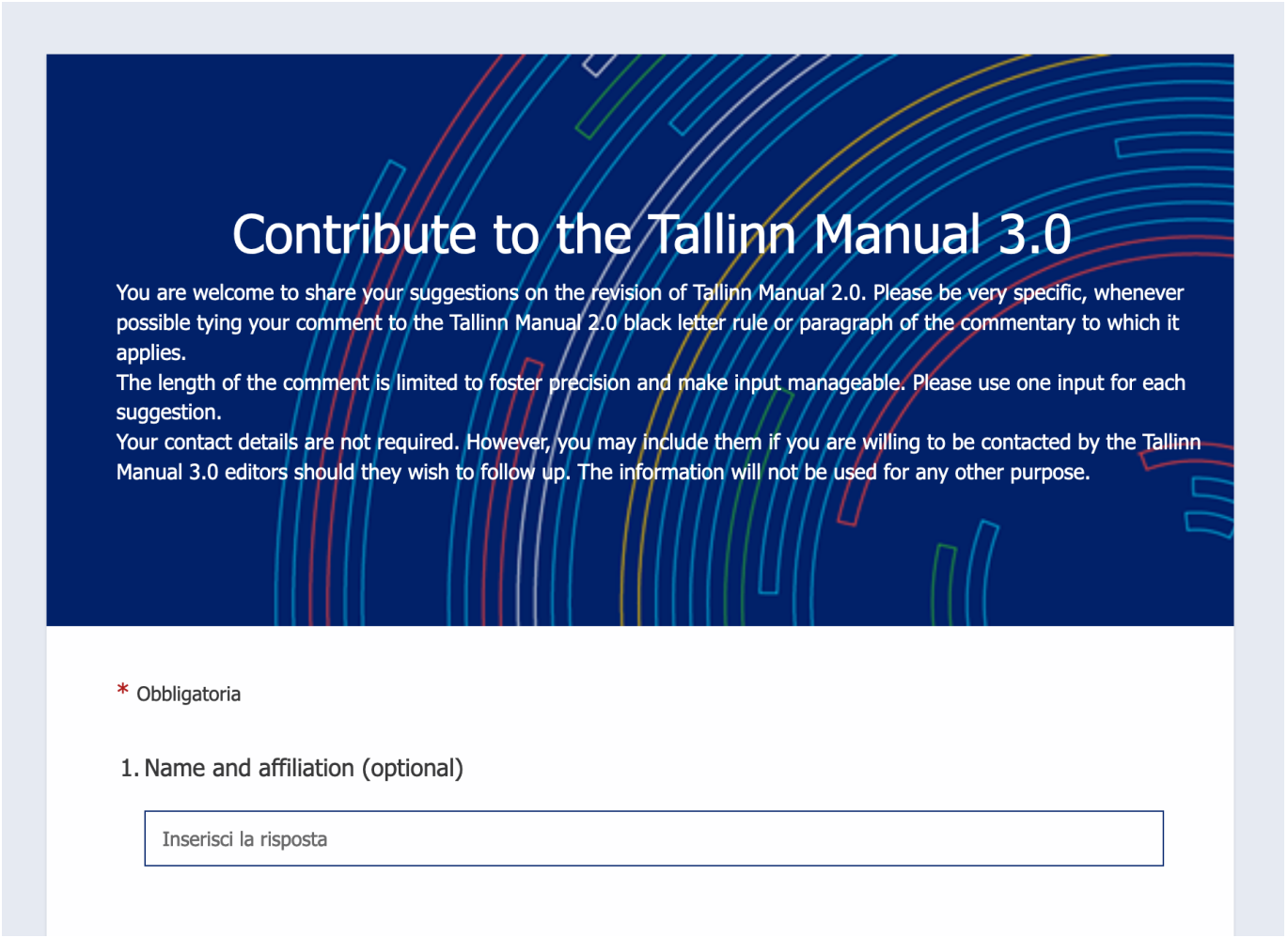


Resoconto dell'attacco subito dall'Estonia
https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

Prima versione del «Manuale di Tallin» 2013
https://ccdcoe.org/research/tallinn-manual/

Seconda versione: «Manuale di Tallin 2.0» 2017
https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/CBAADC9E56434C6F3013069C944EA8BF

Terza versione: «Manuale di Tallin 3.0» (in corso di elaborazione)
https://ccdcoe.org/research/tallinn-manual/



https://customervoice.microsoft.com/Pages/ResponsePage.aspx?id=Soev6_HZQE6E0qvVZ2coeDgkvv4LP1FBg_gf1jtxncZUMDdXVEcwSUdZUzU3RVRXQkhFTFZNMlpBUi4u

UNIVERSITÀ DEGLI STUDI DI UDINE

2.- I principi del GDPR

La tutela dell'interesse pubblico nel Regolamento (UE) 679/2016

Partiamo dalla «base giuridica», ossia ciò che legittima il trattamento dei dati personali.

Art. 6 Liceità del trattamento

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**;

[…]

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;

[…]

-> il trattamento per finalità pubblicistiche è legittimo a prescindere dal consenso (non esiste «privacy» nel senso originariamente inteso!!)

[…]

2. Gli Stati membri possono mantenere o introdurre **disposizioni** più specifiche per **adeguare** l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), **determinando con maggiore precisione**

- **requisiti specifici** per il trattamento e
- **altre misure** atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui al capo IX.

3. La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita:

a) dal diritto **dell'Unione**; o

b) dal diritto dello **Stato membro** cui è soggetto il titolare del trattamento.

[…]

-> la normativa UE può contenere degli adattamenti all'interno di determinati Stati membri, ma non delle deroghe

[…]

La **finalità** del trattamento è determinata in tale base giuridica o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è **necessaria** per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Tale base giuridica **potrebbe contenere** disposizioni **specifiche** per adeguare l'applicazione delle norme del presente regolamento, tra cui:

- le **condizioni** generali relative alla liceità del trattamento da parte del titolare del trattamento;
- le **tipologie** di dati oggetto del trattamento;
- gli **interessati**;
- i **soggetti** cui possono essere **comunicati** i dati personali e le **finalità** per cui sono comunicati;
- le **limitazioni della finalità**, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le **misure** atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX.

Il diritto dell'Unione o degli Stati membri persegue un **obiettivo di interesse pubblico** ed è **proporzionato** all'obiettivo legittimo perseguito.

-> l'adattamento delle norme interne al GDPR deve avvenire con una serie di cautele volte a consentire un controllo di compatibilità (e quindi di costituzionalità)

Limitazioni ai diritti dell'interessato (1) diritto all'oblio

Articolo 17 Diritto alla cancellazione («diritto all'oblio»)

[…]

3. I paragrafi 1 e 2 **non si applicano** nella misura in cui il trattamento sia necessario:

a) per l'esercizio del diritto alla libertà di espressione e di informazione;

b) per l'adempimento di un **obbligo legale** che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un **compito svolto nel pubblico interesse** oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

c) per motivi di **interesse pubblico nel settore della sanità pubblica** in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;

d) a fini di **archiviazione nel pubblico interesse**, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o

e) per l'accertamento, l'esercizio o la difesa di un diritto in **sede giudiziaria**.

-> da notare che l'interesse pubblico limita l'oblio dell'interessato

Limitazioni ai diritti dell'interessato (2) profilazione

Articolo 22 Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

1. L'interessato ha il diritto di non essere sottoposto a una **decisione basata unicamente sul trattamento automatizzato**, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

2. Il paragrafo 1 **non si applica** nel caso in cui la decisione:

a) sia **necessaria** per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;

b) sia **autorizzata** dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì **misure adeguate** a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;

c) si basi sul **consenso esplicito** dell'interessato.

[…]

-> la profilazione può essere autorizzata dall'ordinamento, pur con certi limiti

Limitazioni ai diritti dell'interessato (2) profilazione

Articolo 23 Limitazioni

1. Il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento **può limitare, mediante misure legislative**, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'articolo 5, **nella misura** in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22, **qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata** in una società democratica per salvaguardare:

a) la sicurezza nazionale;

b) la difesa;

c) la sicurezza pubblica;

d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la **salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica**;

e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale;

[…]

Limitazioni ai diritti dell'interessato (3) limitazioni generali

Articolo 23 Limitazioni

[…]

2. In particolare **qualsiasi misura legislativa** di cui al paragrafo 1 contiene **disposizioni specifiche** riguardanti **almeno**, se del caso:

a) le **finalità** del trattamento o le categorie di trattamento;

b) le **categorie** di dati personali;

c) la portata delle **limitazioni** introdotte;

d) le garanzie per **prevenire** abusi o l'accesso o il trasferimento illeciti;

e) **l'indicazione precisa** del titolare del trattamento o delle categorie di titolari;

f) i periodi di **conservazione** e le garanzie applicabili tenuto conto della natura, dell'ambito di applicazione e delle finalità del trattamento o delle categorie di trattamento;

g) i **rischi** per i diritti e le libertà degli interessati; e

h) il diritto degli interessati di essere **informati della limitazione**, **a meno che ciò possa compromettere la finalità della stessa.**

Ulteriori indicazioni concernenti la base giuridica: D. Lgs. 196/2003 modificato successivamente alla piena vigenza del GDPR

Art. 2-ter D. Lgs. 196 /2003 Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

1. La base giuridica prevista **dall'articolo 6, paragrafo 3, lettera b),** del regolamento e' costituita **esclusivamente** da una norma di **legge** o, nei casi previsti dalla legge, di **regolamento**.

1-bis. Il trattamento dei dati personali da parte **di un'amministrazione pubblica** di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, ivi comprese le Autorita' indipendenti e le amministrazioni inserite nell'elenco di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, nonche' da parte di una societa' a controllo pubblico statale di cui all'articolo 16 del decreto legislativo 19 agosto 2016, n. 175, con esclusione per le societa' pubbliche dei trattamenti correlati ad attivita' svolte in regime di libero mercato, **e' sempre consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri a essa attribuiti**.

La **finalità del trattamento**, se non espressamente prevista da una norma di legge o, nei casi previsti dalla legge, di regolamento**,** **è indicata** **dall'amministrazione**, dalla societa' a controllo pubblico **in coerenza** al compito svolto o al potere esercitato,

- assicurando adeguata pubblicita'

- **all'identita'** del titolare del trattamento,
- alle **finalita'** del trattamento

- e fornendo ogni **altra informazione necessaria** ad assicurare un trattamento **corretto e trasparente** con riguardo ai soggetti interessati e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano.

-> comma 1 bis introdotto con il recente DECRETO-LEGGE 8 ottobre 2021, n. 139: delegificazione delle finalità

3.- Le direttive «gemelle»

Cenni sulla disciplina derogatoria rispetto al GDPR contenuta nelle Direttive (UE) 680/2016 «Polizia» (D.Lgs. 51/2018) e 681/2016 «PRN» (D.Lgs. 53/2018)

Direttiva (UE) 680/2016 «Polizia» (D.Lgs. 51/2018)

Art. 1 Oggetto e ambito di applicazione

[…]

3. Il presente decreto **non si applica** ai trattamenti di dati personali:

a) effettuati nello svolgimento di attivita' concernenti **la sicurezza nazionale** o rientranti nell'ambito di applicazione del titolo V, capo 2, del trattato sull'Unione europea e per tutte le attivita' che non rientrano nell'ambito di applicazione del diritto dell'Unione europea;

b) effettuati da istituzioni, organi, uffici e agenzie **dell'Unione europea**.

-> escludiamo dalla considerazione

Direttiva (UE) 681/2016 «PRN» (D.Lgs. 53/2018)

Art. 3 Finalità dei trattamenti

1. I dati PNR raccolti a norma del presente decreto sono trattati a fini di prevenzione e repressione dei **reati di terrorismo e dei reati gravi**, secondo quanto previsto all'articolo 6, comma 2, lettere b), c) e d).

2. I dati API raccolti e resi disponibili agli Uffici incaricati dei controlli di polizia di frontiera a norma del presente decreto sono trattati al fine di **migliorare i controlli alle frontiere esterne e prevenire l'immigrazione illegale**. In caso di ripristino temporaneo dei controlli di frontiera alle frontiere interne il trattamento dei dati API e' esteso anche ai voli intra-UE.

-> l'ambito di applicazione è limitato ma pertinente

Direttiva (UE) 681/2016 «PRN» (D.Lgs. 53/2018)

Caratteristiche specifiche della disciplina:

- Stretta limitazione degli accessi
- Rigoroso ricorso ai log
- Trasferimento dei dati al Sistema Informatico con modalità «push»
- Coordinamento tra privato (vettori) e pubblico (FF.OO.)
- Coordinamento tra Stati
- Pseudonimizzazione successiva ad una determinata finestra temporale (6 mesi)

-> l'ambito di applicazione è limitato ma pertinente

-> da notare la reticolarità dell'organizzazione

UNIVERSITÀ DEGLI STUDI DI UDINE

4.- Cybersecurity e tutela dei dati personali

DIRETTIVA (UE) 2016/1148 «N.I.S.» (D. Lgs. 65/2018)

D.L. 105/2019 «perimetro di sicurezza nazionale cibernetica»

REGOLAMENTO (UE) 2019/881 «Cybersecurity Act»

DIRETTIVA (UE) 2016/1148 «N.I.S.» (D. Lgs. 65/2018)

Art. 2 Trattamento dei dati personali

1. Il trattamento dei dati personali in applicazione del presente decreto e' effettuato ai sensi del decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni.

-> ... E il GDPR (che è un Regolamento UE)?

DIRETTIVA (UE) 2016/1148 «N.I.S.» (D. Lgs. 65/2018)

Art. 7 (Autorita' nazionale competente e punto di contatto unico).

1. L'Agenzia per la cybersicurezza nazionale e' designata quale autorita' nazionale competente NIS per i settori e sottosettori di cui all'allegato II e per i servizi di cui all'allegato III.

[…]

2. L'autorita' nazionale competente NIS e' responsabile dell'attuazione del presente decreto con riguardo ai settori di cui all'allegato II e ai servizi di cui all'allegato III e vigila sull'applicazione del presente decreto a livello nazionale, esercitando altresi' le relative potesta' ispettive e sanzionatorie.

[…]

6. L'Agenzia per la cybersicurezza nazionale, in qualita' di autorita' nazionale competente NIS e di punto di contatto unico, consulta, conformemente alla normativa vigente, l'autorita' di contrasto ed il Garante per la protezione dei dati personali e collabora con essi.

[…]

-> ... Importante a livello istituzionale la consultazione

DIRETTIVA (UE) 2016/1148 «N.I.S.» (D. Lgs. 65/2018)

Art. 13 Attuazione e controllo

[…]

5. Nei casi di incidenti che comportano violazioni di dati personali, l'autorita' competente NIS opera in stretta cooperazione con il Garante per la protezione dei dati personali.

-> anche qui si tratta di una cooperazione di carattere istituzionale

REGOLAMENTO (UE) 2019/881 «Cybersecurity Act»

Articolo 7 Cooperazione operativa a livello di Unione

1. L'ENISA sostiene la cooperazione operativa tra gli Stati membri, le istituzioni, gli organi e gli organismi dell'Unione e tra i portatori di interessi.

2. L'ENISA **coopera** a livello operativo e stabilisce sinergie con le istituzioni, gli organi e gli organismi dell'Unione, compresa la CERT-UE, con i servizi che si occupano della **criminalità informatica** e con le autorità di vigilanza che si occupano della tutela della **vita privata e della protezione dei dati personali**, al fine di affrontare questioni di interesse comune, anche:

a) scambiando conoscenze e migliori pratiche;

b) fornendo consulenza ed emanando orientamenti sulle questioni pertinenti relative alla cibersicurezza;

c) stabilendo le disposizioni pratiche per l'esecuzione di compiti specifici, previa consultazione della Commissione.

-> Ancora cooperazione di carattere istituzionale

UNIVERSITÀ DEGLI STUDI DI UDINE

5.- Videosorveglianza e dati biometrici

Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video

«La videosorveglianza non è di per sé indispensabile se esistono altri mezzi per raggiungere lo scopo che ci si prefigge. Altrimenti si rischia di **modificare le norme culturali** con la conseguenza di **ammettere come regola l'assenza di privacy**»

Principi del GDPR applicabili in generale-> art. 5

- **Necessità**
  - **«esistono alternative»? (es: vigilanti)**
- **Trasparenza**
  - **Informazione di primo livello (segnaletica)**
  - **Informazione di secondo livello (QR code sulla segnaletica)**

«Necessità allo scopo di eseguire un compito nell'interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (articolo 6, paragrafo 1, lettera e)).

41. I dati personali potrebbero essere trattati mediante la videosorveglianza a norma dell'articolo 6, paragrafo 1, lettera e), se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (13). **Può darsi che l'esercizio di pubblici poteri non consenta tale trattamento, ma altri fondamenti di liceità**, per esempio obiettivi di «salute e sicurezza» per la protezione di visitatori e dipendenti, possono fornire un margine limitato per il trattamento, in ogni caso tenendo conto degli obblighi previsti dal RGPD e dei diritti degli interessati.

42. Gli Stati membri **possono mantenere o introdurre una normativa nazionale specifica in materia di videosorveglianza per adattare l'applicazione delle norme del RGPD**, determinando con maggiore precisione specifici requisiti per il trattamento, purché siano conformi ai principi stabiliti dal RGPD (ad esempio, limitazione della conservazione, proporzionalità)». (Linee guida, pag. 14)

Distinzione di fondo sulla videosorveglianza:

- **Dati personali -> «dati comuni»**

  Base giuridica = art. 6 GDPR + art. 2 ter D.Lgs. 196/2003

- **+ Riconoscimento facciale -> Dati biometrici -> «dati particolari»**

  Base giuridica = art. 9 GDPR + art. 2 sexies D.Lgs. 196/2003

Dati personali -> «dati comuni»

Attualmente la videosorveglianza ordinaria ha un regime giuridico duplice che dipende dai casi e dal tipo di tecnologia

- Registrazione -> archiviazione 24 ore / 48 ore / 7 giorni

- Operatore che vigila in tempo reale -> archiviazione + pronto intervento

+ Riconoscimento facciale -> Dati biometrici -> «dati particolari»

Distinzione tra i dati:

- **Dati grezzi (video)**

- **Modelli (pattern di riconoscimento facciale relativi ai singoli individui, generati automaticamente)**

+ Riconoscimento facciale -> Dati biometrici -> «dati particolari»

Definizione normativa, art. 4 (14) GDPR: «dati biometrici»

«i dati personali ottenuti da un **trattamento tecnico specifico** relativi alle caratteristiche **fisiche**, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano **l'identificazione univoca**, quali l'immagine facciale o i dati dattiloscopici»;

Definizione analitica Linee guida videosorveglianza EDPB (pag. 19)

- **natura** dei dati: dati relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica;
- **mezzi e modalità** del trattamento: dati «ottenuti da un trattamento tecnico specifico»;
- **finalità del trattamento**: i dati devono essere utilizzati al fine di identificare in modo univoco una persona fisica

+ Riconoscimento facciale -> Dati biometrici -> «dati particolari»

Articolo 9 Trattamento di categorie particolari di dati personali

1. **È vietato** trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, **dati biometrici intesi a identificare in modo univoco una persona fisica**, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

2. Il paragrafo 1 **non si applica** se si verifica uno dei seguenti casi:

a) l'interessato ha prestato il proprio **consenso esplicito** al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;

[…]

g) il trattamento è necessario per **motivi di interesse pubblico rilevante** sulla base del diritto dell'Unione o degli Stati membri, che deve essere

- **proporzionato** alla finalità perseguita,
- rispettare **l'essenza** del diritto alla protezione dei dati e
- prevedere **misure appropriate** e **specifiche** per tutelare i diritti fondamentali e gli interessi dell'interessato;

[…]

+ Riconoscimento facciale -> Dati biometrici -> «dati particolari»

Articolo 9 Trattamento di categorie particolari di dati personali

[…]

i) il trattamento è necessario per **motivi di interesse pubblico nel settore della sanità pubblica**, quali la protezione da **gravi minacce per la salute a carattere transfrontaliero** o la **garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria** e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

j) il trattamento è necessario a fini di **archiviazione nel pubblico interesse**, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

-> il trattamento per finalità pubblicistiche è legittimo a prescindere dal consenso anche nel caso di dati «particolari (attenzione alla lettera i), che riguarda anche il COVID19)

Ulteriori indicazioni sulla base giuridica -> D. Lgs. 196/2003

Art. 2-sexies (Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante).

1. I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, **necessari per motivi di interesse pubblico rilevante** ai sensi del paragrafo 2, lettera g), del medesimo articolo, **sono ammessi** qualora siano

- **previsti** dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento
- che **specifichino**
  - i tipi di dati che possono essere trattati,
  - le operazioni eseguibili e
  - **il motivo di interesse pubblico rilevante,**
  - nonche' le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

-> qui si specifica come devono avvenire le previsioni di legge che autorizzano il trattamento di dati particolari

Ulteriori indicazioni sulla base giuridica -> D. Lgs. 196/2003

Art. 2-sexies (Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante).

[…]

2. Fermo quanto previsto dal comma 1, si considera rilevante

l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie:

[…]

h) svolgimento delle funzioni di controllo, indirizzo politico, **inchiesta parlamentare** o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalita' direttamente connesse all'espletamento di un mandato elettivo;

[…]

3. Per i dati genetici, **biometrici** e relativi alla salute il trattamento avviene **comunque** nel rispetto di quanto previsto **dall'articolo 2-septies**.

-> qui si specifica che anche gli organi istituzionali di controllo elettivo devono avere accesso ai dati particolari, ma quando si tratta di dati biometrici occorrono ulteriori cautele

Ulteriori indicazioni sulla base giuridica -> D. Lgs. 196/2003

Art. 2-septies *Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute.*

1. -> rif. Provvedimento del Garante che stabilisce misure di garanzia

2. Il provvedimento che stabilisce le misure di garanzia di cui al comma 1 e' adottato con **cadenza almeno biennale** e tenendo conto:

a) delle linee guida, delle raccomandazioni e delle migliori prassi pubblicate dal **Comitato europeo per la protezione dei dati** e delle **migliori prassi** in materia di trattamento dei dati personali;

b) dell'evoluzione scientifica e tecnologica nel settore oggetto delle misure;

c) dell'interesse alla libera circolazione dei dati personali nel territorio dell'Unione europea.

3. Lo schema di provvedimento e' sottoposto a consultazione pubblica per un periodo non inferiore a sessanta giorni

[…]

-> provvedimento generale del Garante + consultazione pubblica come garanzia formale e procedurale di condivisione sociale

-> ruolo della comunità degli esperti -> Linee guida, best practices

Ulteriori indicazioni sulla base giuridica -> D. Lgs. 196/2003

Art. 2-septies ***Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute.***

[…]

5. Le misure di garanzia sono adottate in relazione a ciascuna categoria dei dati personali di cui al comma 1, avendo riguardo alle **specifiche finalita' del trattamento** e possono individuare, in conformita' a quanto previsto al comma 2, **ulteriori condizioni** sulla base delle quali il trattamento di tali dati e' consentito. In particolare, le misure di garanzia individuano

- le **misure di sicurezza**, ivi comprese quelle tecniche di cifratura e di pseudonomizzazione,
- le **misure di minimizzazione**,
- le **specifiche modalita' per l'accesso selettivo** ai dati e per rendere le informazioni agli interessati, nonche'
- le eventuali **altre misure necessarie** a garantire i diritti degli interessati.

[…]

Ulteriori indicazioni sulla base giuridica -> D. Lgs. 196/2003

Art. 2-septies *Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute.*

[…]

7. Nel rispetto dei principi in materia di protezione dei dati personali, con riferimento agli obblighi di cui all'articolo 32 del Regolamento, **e' ammesso l'utilizzo dei dati biometrici con riguardo alle procedure di accesso fisico e logico ai dati da parte dei soggetti autorizzati**, nel rispetto delle misure di garanzia di cui al presente articolo.

8. I dati personali di cui al comma 1 non possono essere diffusi.

-> deroga normativa per utilizzi limitati

Recenti pronunciamenti contro il riconoscimento facciale

21/6/2021 EDPB + Garante europeo

https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_it

6/10/2021 Risoluzione Parlamento Europeo

https://www.europarl.europa.eu/news/en/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance

UNIVERSITÀ DEGLI STUDI DI UDINE

6.- Prospettive future e conclusioni provvisorie

COM/2018/640 final, Proposta di REGOLAMENTO (UE) relativo alla prevenzione della diffusione di contenuti terroristici online

COM/2020/823 final Proposta di DIRETTIVA relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148 c.d. NIS 2.0

COM/2020/825 final, Proposta di REGOLAMENTO relativo a un mercato unico dei servizi digitali (Digital Service Act)

COM/2020/829 final, Proposta di DIRETTIVA sulla resilienza dei soggetti critici

COM/2021/206 final, Proposta di REGOLAMENTO (Artificial Intelligence Act)

La proposta di Regolamento (UE) «Legge sull'Intelligenza artificiale» -> art. 5

1.Sono **vietate** le pratiche di intelligenza artificiale seguenti:

[…]

d)l'uso di **sistemi di identificazione biometrica remota "in tempo reale"** in spazi accessibili al pubblico a fini di attività di **contrasto**, **a meno che e nella misura in cui** tale uso sia **strettamente necessario** per uno dei seguenti obiettivi:

- i)la ricerca mirata di potenziali **vittime** specifiche di reato, compresi i minori scomparsi;
- ii)la prevenzione di una **minaccia** specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico;
- iii)il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o un sospettato di un reato di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI del Consiglio 62 , punibile nello Stato membro **interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni**, come stabilito dalla legge di tale Stato membro.

La proposta di Regolamento (UE) «Legge sull'Intelligenza artificiale» -> art. 5

[…]

2.L'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto per uno qualsiasi degli obiettivi di cui al paragrafo 1, lettera d), tiene conto dei seguenti elementi:

a)la **natura** della situazione che dà luogo al possibile uso, in particolare la gravità, la probabilità e l'entità del danno causato dal mancato uso del sistema;

b)le **conseguenze** dell'uso del sistema per i diritti e le libertà di tutte le persone interessate, in particolare la gravità, la probabilità e l'entità di tali conseguenze.

L'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto per uno qualsiasi degli obiettivi di cui al paragrafo 1, lettera d), **rispetta inoltre le tutele e le condizioni necessarie e proporzionate in relazione all'uso**, in particolare per quanto riguarda le **limitazioni temporali, geografiche e personali.**

La proposta di Regolamento (UE) «Legge sull'Intelligenza artificiale» -> art. 5

[…]

3.Per quanto riguarda il paragrafo 1, lettera d), e il paragrafo 2, **ogni singolo uso** di un sistema di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto è subordinato

- **a un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente dello Stato membro in cui deve avvenire l'uso,**
- **rilasciata su richiesta motivata e in conformità alle regole dettagliate del diritto nazionale di cui al paragrafo 4**.

Tuttavia, in una **situazione di urgenza** debitamente giustificata, è possibile iniziare a usare il sistema senza autorizzazione e richiedere l'autorizzazione **solo durante o dopo** l'uso.

L'autorità giudiziaria o amministrativa competente rilascia l'autorizzazione **solo se ha accertato**, sulla base di prove oggettive o indicazioni chiare che le sono state presentate, che l'uso del sistema di identificazione biometrica remota "in tempo reale" in questione **è necessario e proporzionato** al conseguimento di uno degli obiettivi di cui al paragrafo 1, lettera d), come indicato nella richiesta. Nel decidere in merito alla richiesta, l'autorità giudiziaria o amministrativa competente tiene conto degli elementi di cui al paragrafo 2.

[…]

La proposta di Regolamento (UE) «Legge sull'Intelligenza artificiale» -> art. 5
Articolo 5

[…]

4.Uno Stato membro **può decidere di prevedere la possibilità** di autorizzare in tutto o in parte l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, **entro i limiti e alle condizioni di cui al paragrafo 1, lettera d), e ai paragrafi 2 e 3**. Tale Stato membro stabilisce nel proprio diritto nazionale le **necessarie regole** dettagliate per la richiesta, il rilascio, l'esercizio delle autorizzazioni di cui al paragrafo 3, nonché per le attività di controllo ad esse relative. Tali regole **specificano i**noltre

- per quali degli **obiettivi** elencati al paragrafo 1, lettera d), compresi i reati di cui al punto iii),
- le **autorità competenti** possono essere autorizzate ad utilizzare tali sistemi a fini di attività di contrasto.

Take away

1.- privacy (Stato v.s. individuo, «diritti assoluti») -> dati personali («data governance», procedure, controlli istituzionali, consultazioni pubbliche)

2.- Unione Europea come contesto normativo

3.- la sicurezza informatica come **presupposto** della tutela dei dati personali

4.- la sicurezza cibernetica come elemento **imprescindibile** della sicurezza informatica

5.- non contano le tecnologie in quanto tali, **contano le «pratiche»**, ossia come le tecnologie vengono concretamente utilizzate

6.- la dimensione etica si integra nel problema della qualità tecnologica (**design** tecnologico)

7.- cosa significa nel concreto «necessario» o «proporzionato»? Necessità di ulteriore elaborazione in futuro

</>