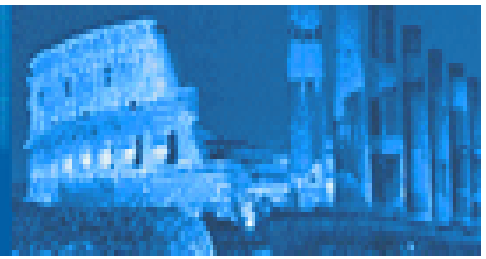


GDPR:
Focus on la profilazione dei dati personali

SEMINARIO SICUREZZA E PRIVACY ISACA Roma

3 Maggio 2017

Luciano Delli Veneri
Gloria Marcoccio

Relatori

Luciano Delli Veneri – luciano.delliveneri@gmail.com

Privacy e Compliance Manager con oltre 10 anni di esperienza nell'applicazione della normativa sulla privacy maturata inizialmente nella articolata realtà della TLC, con complessità rilevanti e, successivamente, curandone l'applicazione presso società del terziario, del settore energetico, Università. Ha progettato, implementato e governato i sistemi privacy aziendali curando direttamente gli adempimenti e la valutazione preventiva della compliance dei nuovi prodotti/servizi. Ha gestito le relazioni con il Garante assicurando i riscontri ai provvedimenti, ai ricorsi, alle richieste di informazioni e nelle visite ispettive. Ha conseguito la certificazione "Privacy Officer e Consulente della Privacy" con TÜV Italia.

Gloria Marcoccio – gloria.marcoccio@glory.it

Dottore ingegnere con master in Information Technology Laws, esperta nella applicazione in contesti operativi delle normative nazionali ed internazionali applicabili ai servizi della information & networked society. Consulente senior nel settore TLC e difesa con 30 anni di esperienza maturata in molteplici contesti operativi presso primarie organizzazioni internazionali, tra cui la Commissione Europea e gruppi multinazionali nel settore delle telecomunicazioni e della difesa. Ha scritto numerosi articoli riguardo la protezione dei dati e privacy, articoli scientifici in materia di data fusion e algoritmi per l'elaborazione dei dati. Lead Auditor ISO27001 e certificata "Privacy Officer e Consulente della Privacy " con TÜV Italia.

https://privacyblog.jimdo.com/

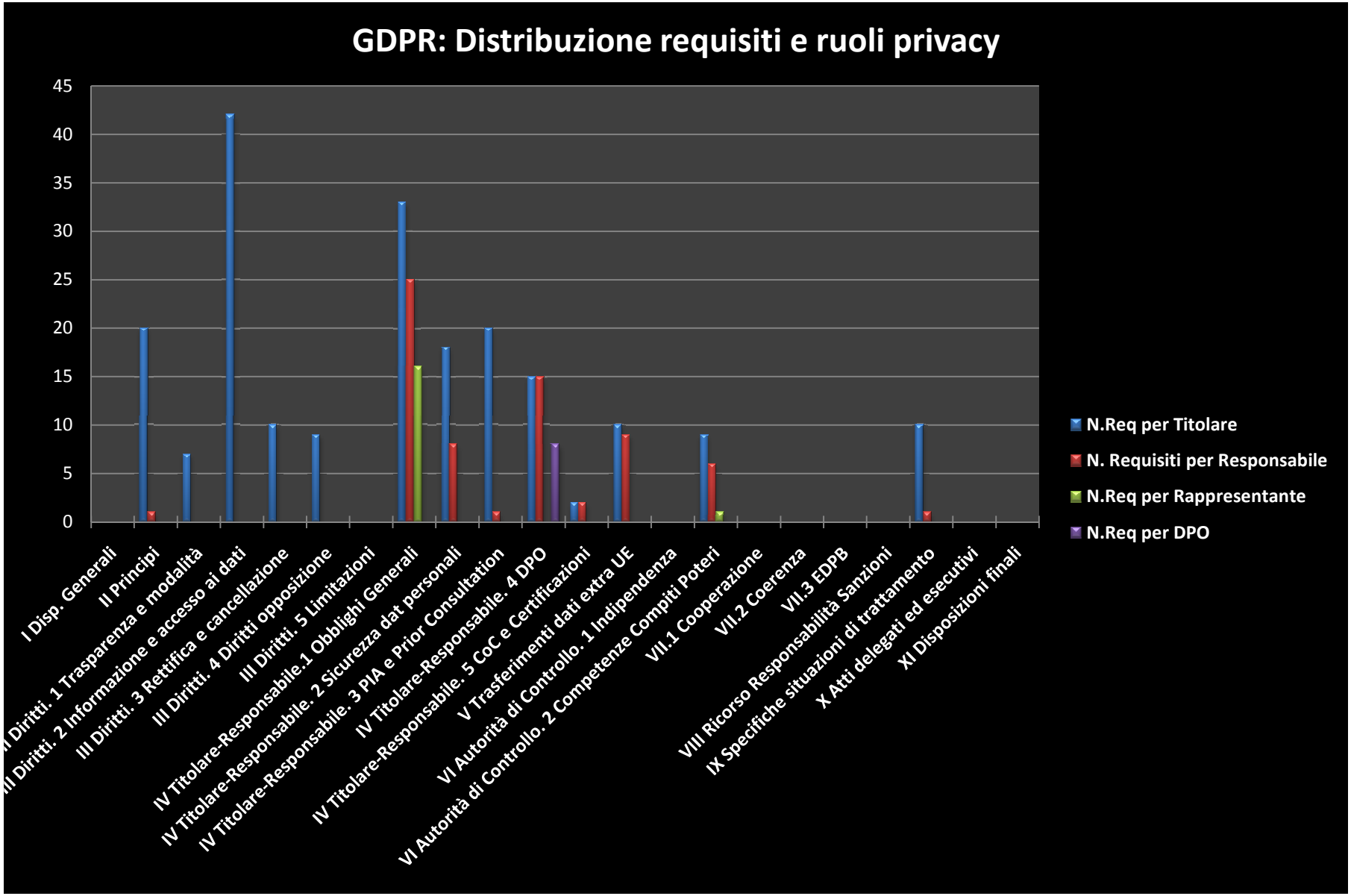
GDPR: 173 considerando, 99 articoli, più di 200 requisiti…

Regolamento Privacy Europeo n. 2016/679 (General Data Protection Regulation- GDPR)
E' entrato in vigore il: 24 Maggio 2016
Si applica a partire dal: 25 Maggio 2018

Autorità Italiana Garante per la Protezione dati personali
(Prima) Guida all'applicazione del Regolamento europeo in materia di protezione dei dati
Pubblicata: 28 Aprile 2016

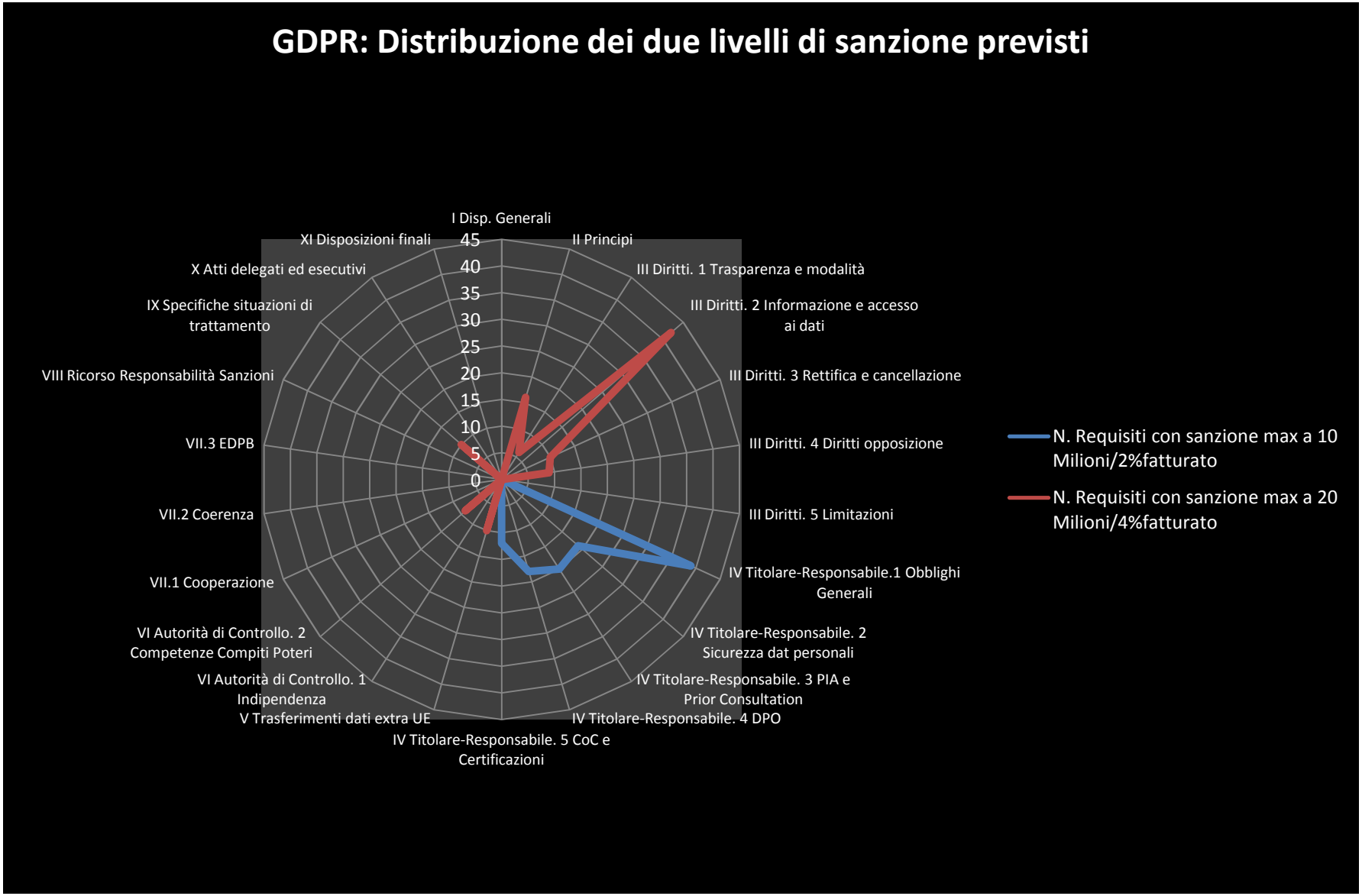
Viviamo in uno strano mondo….chi avrebbe mai previsto 20 anni fa che gli avvocati, tradizionalmente tecnofobici (ed infatti hanno scelto di studiare Legge) e gli ingegneri informatici (che amano considerare ogni possibilità analitica quando progettano un codice) sarebbero diventati inevitabilmente partner d'affari?

GDPR: 173 considerando, 99 articoli, più di 200 requisiti…

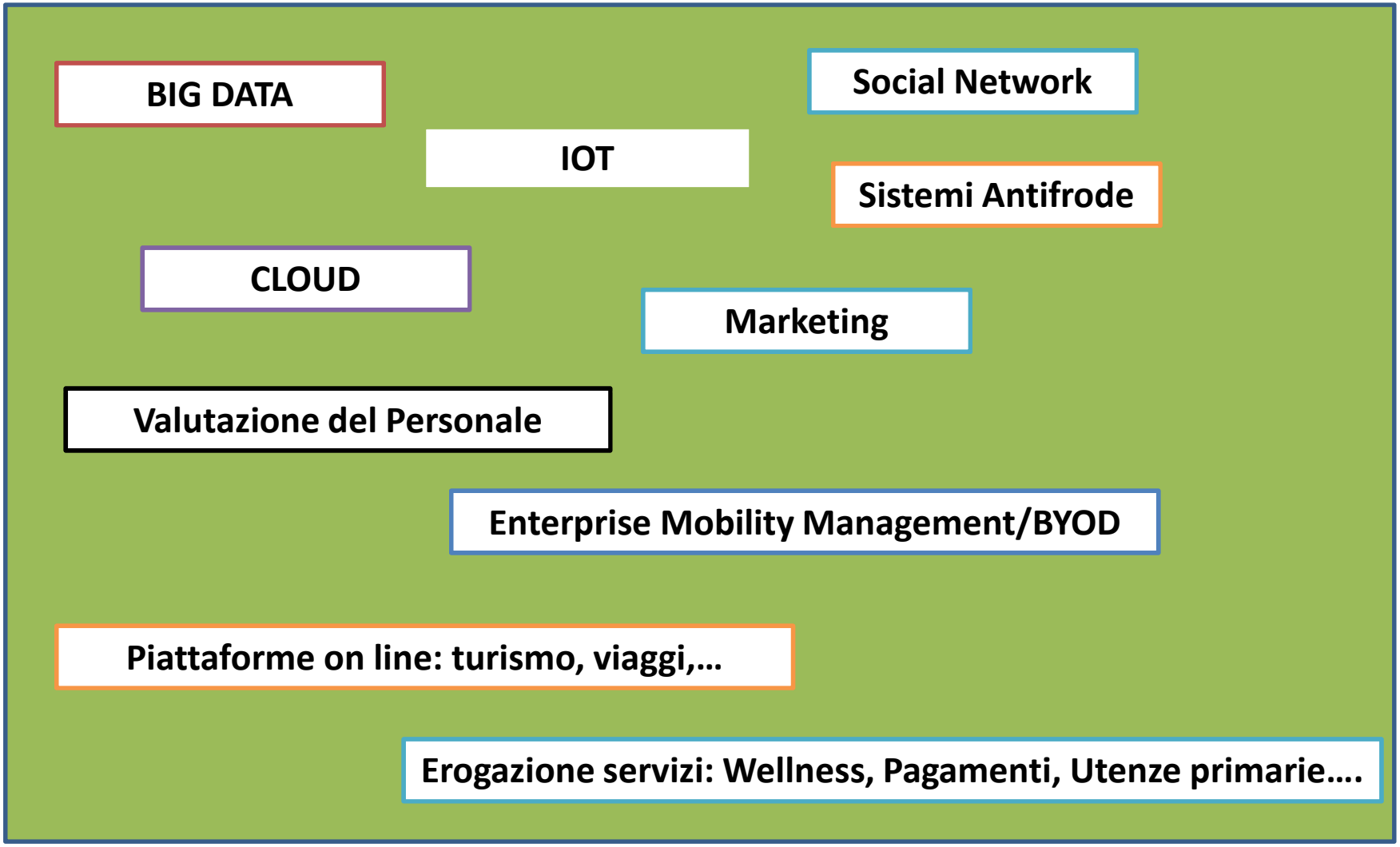


Luciano Delli Veneri
Gloria Marcoccio

GDPR: 173 considerando, 99 articoli, più di 200 requisiti…



Profilazione: innumerevoli contesti di applicazione



La Profilazione nella vigente normativa privacy - pre GDPR

Assenza di una definizione di legge

A livello EU

Art 15 Decisioni individuali automatizzate Direttiva 95/46/EC

Art 5 (3) Direttiva 2002/58/EC (sull'installazione di cookie e similari)

WP29 "Parere 2/2010 sulla pubblicità comportamentale online"

WP 29 "Parere 9/2014 sull'applicazione della direttiva 2002/58/EC al devicefingerprinting"

A livello Italiano

Art. 14. "Definizione di profili e della personalità dell'interessato" D.Lgs 196/03

Art. 122"Informazioni raccolte nei riguardi del contraente o dell'utente" D.Lgs 196/03

Provvedimento Garante Privacy 'Fidelity card' e garanzie per i consumatori. Le regole del Garante per i programmi di fidelizzazione - 24 febbraio 2005"

Provvedimento Garante Privacy "Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie - 8 maggio 2014"

"Linee guida in materia di trattamento di dati personali per profilazione on line - 19 marzo 2015" emesse dal Garante Privacy

La Profilazione nella vigente normativa privacy - pre GDPR - Italia

Notifica al Garante Privacy *per 'trattamenti effettuati mediante l'ausilio di strumenti elettronici volti a definire profili di consumatori o ad analizzarne abitudini e scelte in ordine ai prodotti acquistati (artt. 37, comma 1, lett. d), e 163 del D.Lgs 196/03)'*

Rispetto dei principi di cui all'Art 11 D.Lgs 196/03 (liceità, pertinenza, non eccedenza,…)

Base di liceità del trattamento: di norma il consenso dell'Interessato (Informato, Libero,…), ex Art. 23 D.Lgs 196/03

Diritto dell'Interessato di opporsi

- ***per motivi legittimi, ancorché pertinenti allo scopo della raccolta , ex Art. 7.4.a) D.Lgs 196/03(*)***
- ***a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale ex Art. 7.4.b) D.Lgs 196/03***

Necessità di Verifica Preliminare ex Art 17 D.Lgs 196/03 se la profilazione comporta il trattamento di dati personali - non sensibili, non giudiziari - che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare

Profilazioni basate su dati sensibili e/o giudiziari necessitano di preventiva Autorizzazione da parte del Garante privacy

Misure di sicurezza ex Art 31 D.Lgs 196/03, Misure minime Allegato B D.Lgs 196/03 e Provvedimento del Garante Privacy sulla figura dell'Amministratore di Sistema

(*) salvo che la determinazione sia stata adottata in occasione della conclusione o dell'esecuzione di un ***contratto****, in* ***accoglimento di una proposta dell'interessato*** *o sulla base di adeguate garanzie individuate dal presente codice o da un provvedimento del Garante ai sensi* ***dell'articolo 17. D.Lgs 196/03***

WP29 “Parere 2/2010 sulla pubblicità comportamentale online”

A proposito di profilazione:

La pubblicità comportamentale prevede il tracciamento degli utenti durante la navigazione in rete e, nel tempo, la creazione di profili che vengono successivamente utilizzati per fornire agli utenti contenuti pubblicitari che rispondono ai loro interessi.

2 metodi principali per costruire profili utenti:

i) profili predittivi - stabiliti per deduzione attraverso l’osservazione del comportamento individuale e collettivo dell’utente nel corso del tempo, in particolare monitorando le pagine visitate e i messaggi pubblicitari visualizzati o cliccati

ii) profili espliciti - creati a partire da dati personali che l'interessato stesso ha fornito a un servizio web, per esempio all’atto della registrazione.

I due metodi possono essere combinati

Le reti pubblicitarie costruiscono i profili predittivi combinando tecniche di tracciamento, tecnologie basate sui cookie e software di estrapolazione dati. Anche l’ubicazione dell'interessato è un’informazione fondamentale per definire il profilo del target.

Il parere del WP29 sul Device fingerprinting

Device fingerprint :
"una serie di informazioni che identificano un dispositivo o un'istanza applicativa"

Il presente parere intende rispondere ad un numero crescente di segnalazioni secondo cui terzi stanno esplorando attivamente la possibilità di utilizzare tecnologie alternative ai cookie per vari scopi, per sottrarsi all'obbligo del consenso di cui all'articolo 5, paragrafo 3 della Direttiva 2002/58/EC (E-Privacy Directive). In particolare, viene esaminata la combinazione di una serie di informazioni al fine di identificare in modo univoco particolari dispositivi o istanze applicative, il cosiddetto "device fingerprinting".

A differenza dei cookie HTTP, l'utilizzo delle informazioni connesse ai device fingerprinting può risultare meno evidente.

L'utilizzo del device fingerprinting in luogo dei cookies ai fini della On Line Behavioral Advertising richiede il preventivo consenso

Garante privacy “Linee guida in materia di trattamento di dati personali per profilazione on line - 19 marzo 2015”

Riguardano la profilazione di utenti on line con distinzione utenti tra AUTENTICATI e NON AUTENTICATI

Rivolte a tutti i soggetti stabiliti su territorio nazionale che forniscono **servizi on line, quali motori di ricerca, posta elettronica, mappe on line, social network, pagamenti elettronici, cloud computing.**

Risultano essere **in gran parte riprese dal provvedimento di luglio 2014 del Garante nei riguardi di Google**

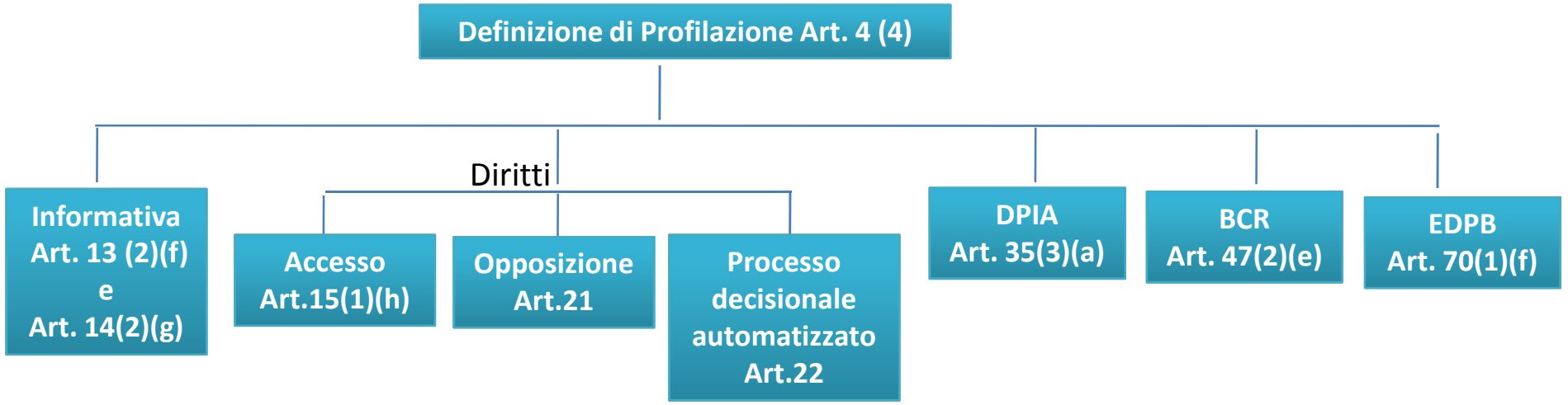
il Garante Privacy ha concesso oltre 18 mesi di tempo a Google per adeguarsi con la seguente motivazione:
"Il Garante è consapevole delle difficoltà tecnico-operative connesse all'implementazione delle misure cui Google è tenuta ai fini dell'adempimento delle prescrizioni di cui al presente provvedimento, in quanto si tratta di modifiche relative ad una molteplicità di funzionalità rese disponibili su una pluralità di piattaforme tecnologiche e sistemi operativi, peraltro di non trascurabile complessità tecnica. In considerazione di quanto sopra, è dunque ipotizzabile un arco temporale di adeguamento sufficientemente ampio, quantificabile nell'ordine dei 18 mesi...”

Garante privacy “Linee guida in materia di trattamento di dati personali per profilazione on line - 19 marzo 2015”

Punti di attenzione

- manca una definizione puntuale di profilazione e di quale sia il set di dati la cui “elaborazione” possa essere classificata tale;
- non vengono fornite indicazioni in merito ai tempi di conservazione dei dati personali ma vi è un semplice rinvio art. 11, comma 1, lett. e), del Codice;
- non è indicato tra gli obblighi comunque esistenti quello relativo alla “notificazione” ex art. 37 del Codice della finalità di profilazione;
- il consenso dell’utente non registrato è riferibile al “device” e quindi non al singolo utilizzatore (es. internet cafè, postazioni condivise, etc);
- il passaggio da “utente” a “utente autenticato” potrebbe “modificare le scelte in ordine alla profilazione” .....

Profilazione e GDPR



Profilazione: cosa prevede il GDPR

Definizione

*"qualsiasi forma di trattamento **automatizzato** di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il **rendimento professionale**, **la situazione economica**, la **salute**, le **preferenze personali**, gli **interessi**, l'**affidabilità**, il **comportamento**, l'**ubicazione** o gli **spostamenti** di detta persona fisica "*

Cosa cambia rispetto alla Direttiva o al Codice privacy

Il concetto di profilazione non è più circoscritto alla propensione al consumo di prodotti e all'utilizzo di servizi ma il perimetro viene significativamente esteso facendovi rientrare **l'Interessato (persona fisica) e quanto a lui direttamente riferibile (età, sesso, situazione economica, stato familiare, etc.) ma anche quanto lo circonda o con cui interagisce, inclusa la sua geolocalizzazione**

Profilazione: cosa prevede il GDPR

(Considerando 71)

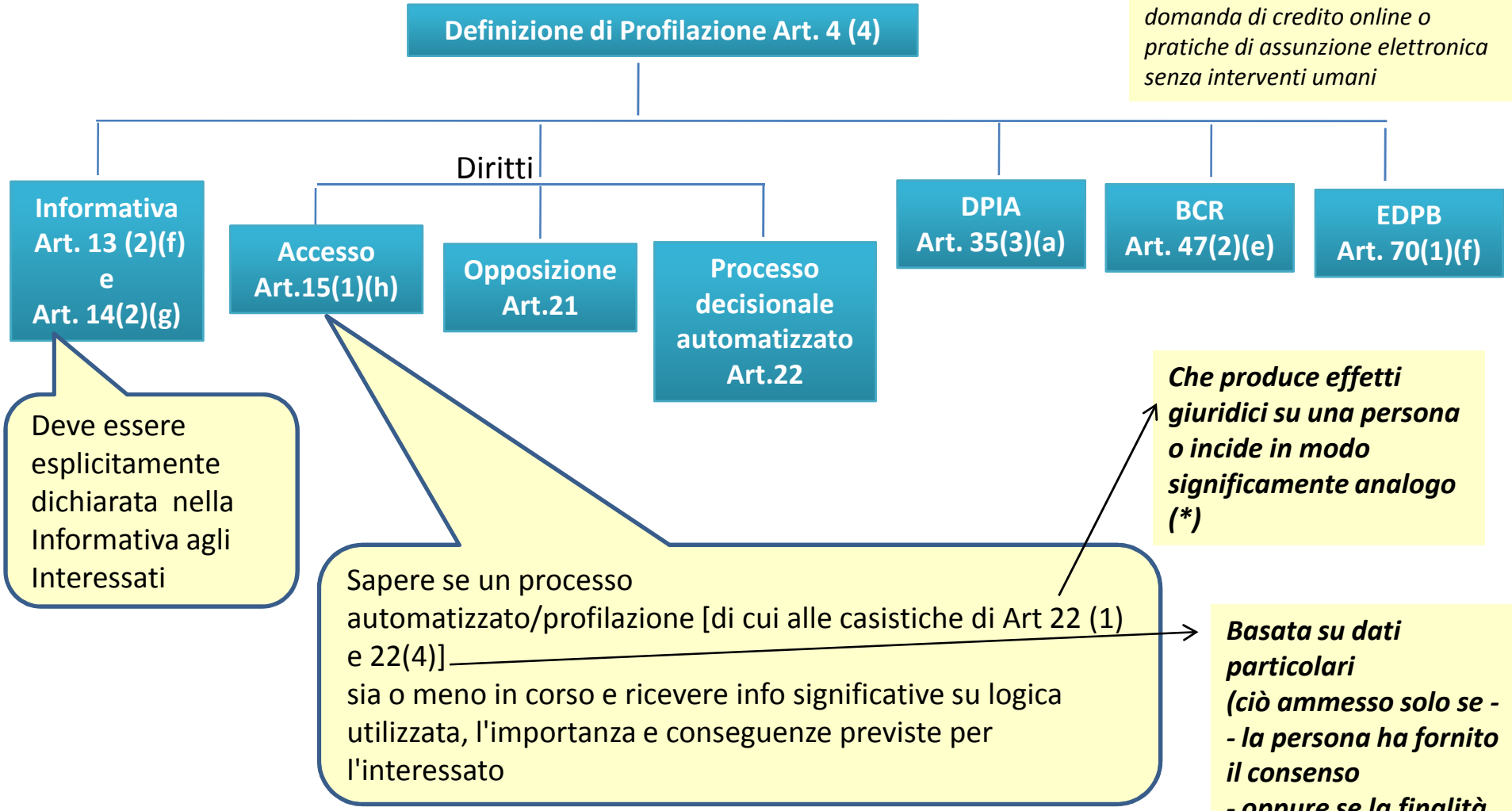
Ai fini di un trattamento corretto e trasparente verso l'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il Titolare:

- utilizzi procedure matematiche o statistiche appropriate per la profilazione
- metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare
  - che siano rettificati i fattori che comportano inesattezze dei dati
  - sia minimizzato il rischio di errori
  - sia garantita la sicurezza dei dati personali tenendo presenti i potenziali rischi esistenti per gli interessi e i diritti dell'Interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti.

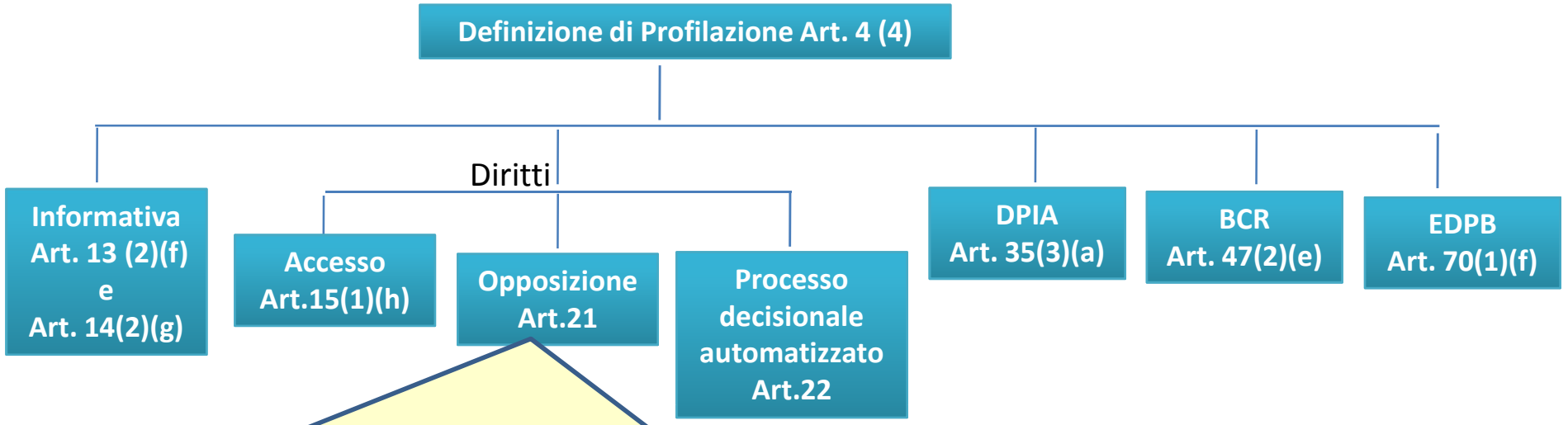
La profilazione non dovrebbe riguardare i minori

Profilazione e GDPR

(*)Ad esempio (Considerando 71): il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani



Profilazione e GDPR



In caso di **finalità di INTERESSE PUBBLICO o liceità di trattamento basata su LEGITTIMO INTERESSE:**

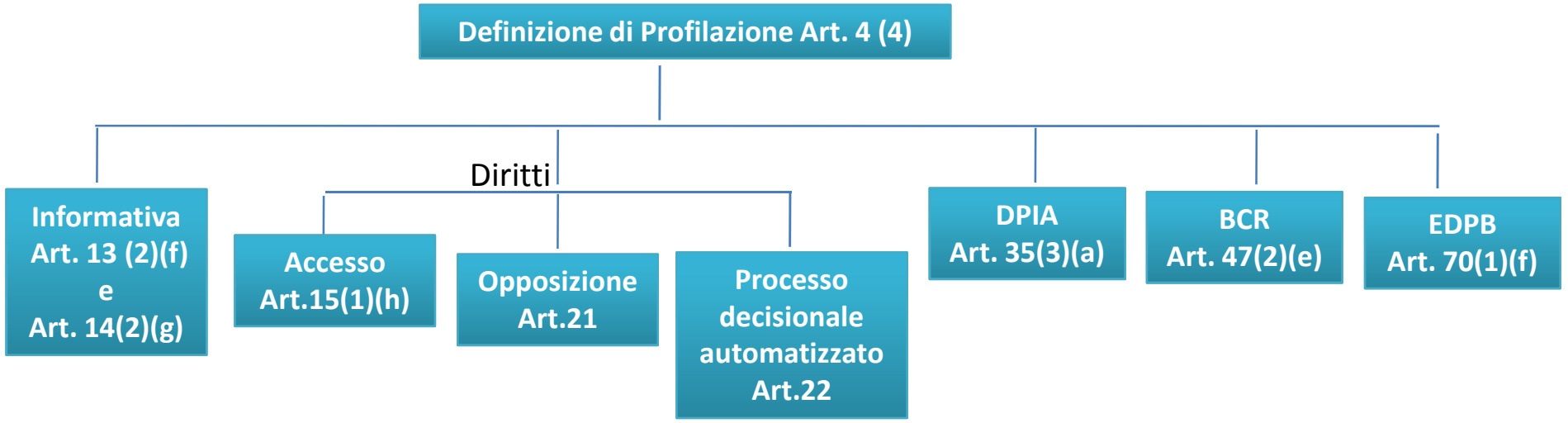
Diritto di opporsi **in qualsiasi momento**, per motivi connessi alla sua situazione particolare, al trattamento dei dati inclusa la profilazione

Il Titolare non tratta ulteriormente i dati **a meno che non dimostri l'esistenza di motivi** legittimi cogenti che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Marketing diretto: l'interessato ha il diritto di opporsi **in qualsiasi momento** al trattamento inclusa la profilazione

Questi diritti sono esplicitamente evidenziati all'interessato in modo separato da qualsiasi altra informazione, al momento della prima comunicazione con l'interessato.

Profilazione e GDPR

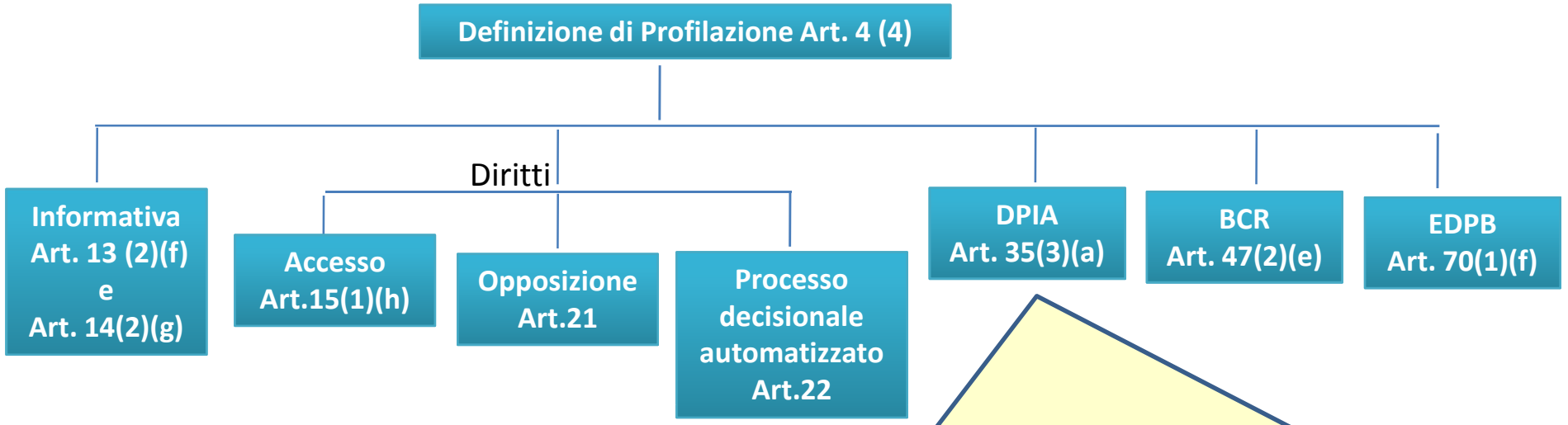


Divieto di basare una decisione unicamente sul trattamento automatizzato/profilazione se ciò produce **effetti giuridici** che riguardano **o** che incidano in **modo analogo significativamente** sull'Interessato.
Casi di deroga al divieto:
a) Decisione necessaria per conclusione o esecuzione di un **contratto** tra Interessato e Titolare(*)
b) Decisione autorizzata da **legge** UE o nazionale
c) Decisione basata sul **consenso** esplicito dell'interessato (*)

(*) il Titolare applica misure appropriate per tutelare almeno il diritto di ottenere l'intervento umano, di esprimere la propria opinione e di contestare la decisione.

Le decisioni possono basarsi sui dati sensibili (origine razziale, opinioni politiche, religiose, org. sindacali, dati genetici/biometrici/relativi alla salute/orientamento e vita sessuale) **solo se** il trattamento è soggetto a **consenso oppure è per interesse pubblico ed in ogni caso devono essere attuate misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.**

Profilazione e GDPR

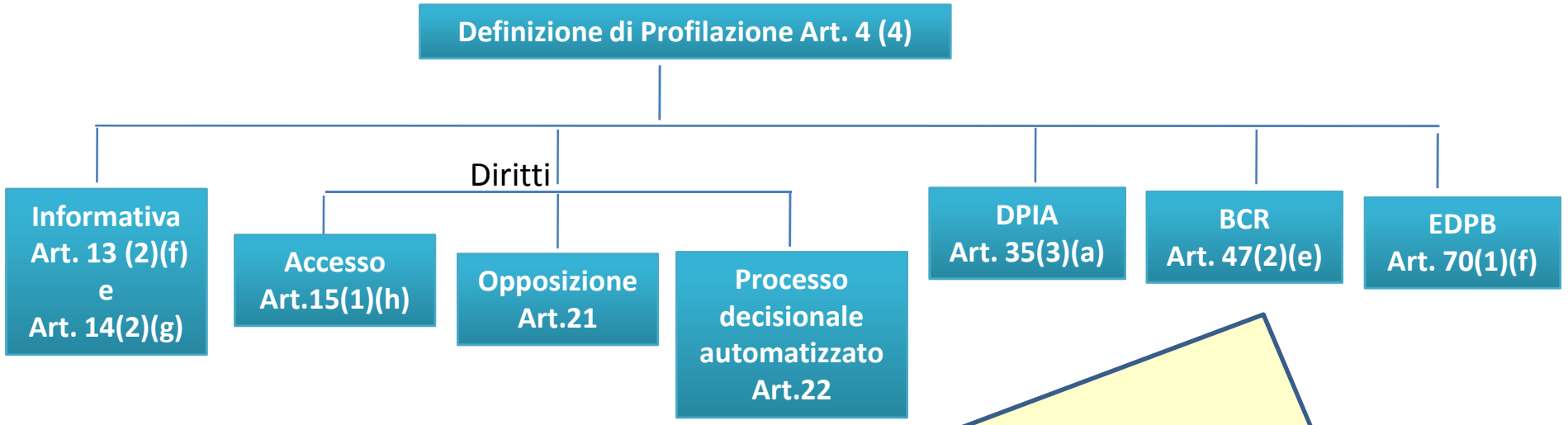


Se un trattamento, che prevede l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione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

La valutazione d'impatto sulla protezione dei dati è richiesta in particolare nel caso di

a)una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche

Profilazione e GDPR



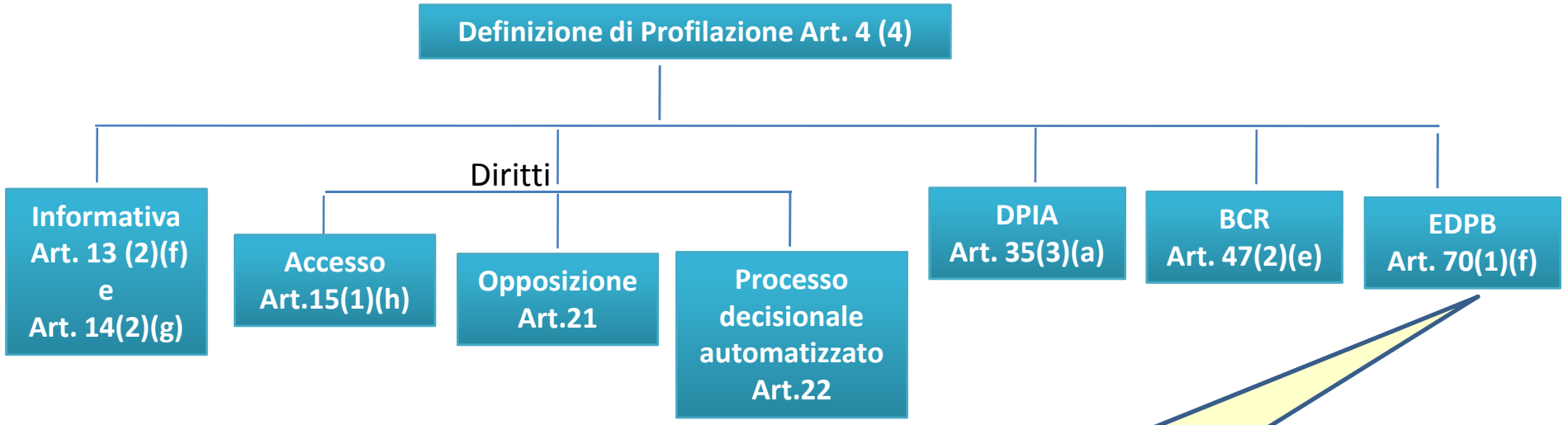
Le norme vincolanti d'impresa (Binding Corporate Rules, in relazione ai trasferimenti di dati extra UE, in ambito gruppi internazionali) devono precisare, tra l'altro:

....

e) i diritti dell'interessato in relazione al trattamento e i mezzi per esercitarli, compresi il diritto di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione ai sensi dell'articolo 22, …

.....

Profilazione e GDPR



European Data Protection Board (evoluzione del WP29 anche con importanti compiti decisionali), può, di propria iniziativa o, se del caso, su richiesta della Commissione:

definire linee guida, raccomandazioni e *best practice* per specificare **ulteriormente i criteri e le condizioni delle decisioni basate sulla profilazione** ai sensi dell'articolo 22, paragrafo 2

a) Decisione necessaria per conclusione o esecuzione di un **contratto** tra Interessato e Titolare(*)
b) Decisione autorizzata da **legge** UE o nazionale
c) Decisione basata sul **consenso** esplicito dell'interessato

Profilazione &GDPR: alcuni punti di attenzione

1) **Profilazione, cambio di finalità e legittimo interesse**

2) **Profilazione di dati di altri Interessati**

3) **I dati personali risultato di una Profilazione e loro Portabilità**

……..

Profilazione: GDPR vs e-privacy Directive

La Direttiva 2002/58 EU (e-privacy), destinata a regolamentare il mondo dei servizi di comunicazione elettronica fornisce le prime indicazioni in merito agli aspetti di profilazione dei "navigatori" mediante l'utilizzo dei cookie.

La Direttiva 2009/136/ EU ha aggiornato la Direttiva "e-privacy" in particolare per quanto riguarda l'impiego dei cookie imponendo un regime ancora più stringente in ordine al loro impiego ed alle modalità con le quali gli Interessati devono essere informati per poter scegliere liberamente.

Profilazione: GDPR vs e-privacy Directive

Art. 5 c.3 (come modificato dalla Direttiva 2009/136/UE)

Gli Stati membri assicurano che ~~l'uso di reti di comunicazione elettronica per archiviare~~ **l'archiviazione di** informazioni ~~o per avere~~ oppure l'accesso a informazioni **già** archiviate nell'apparecchiatura terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente in questione **abbia espresso preliminarmente il proprio consenso, dopo essere** ~~sia~~ stato informato in modo chiaro e completo, a norma della direttiva 95/46/CE, tra l'altro sugli scopi del trattamento ~~e che gli sia offerta la possibilità di rifiutare tale trattamento da parte del responsabile del trattamento~~. Ciò non vieta l'eventuale archiviazione tecnica o l'accesso al solo fine di effettuare ~~o facilitare~~ la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria **al fornitore di** a fornire un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente **a erogare tale servizio**".

Profilazione: GDPR vs e-privacy Directive

La posizione del WP Art29

Il WP ritiene non applicabile ai cookie un sistema di "opt-out" per la raccolta del consenso.

In particolare:

- **non** ritiene sufficiente **l'impostazione del browser di rifiuto dei cookie**, perché poco conosciuta e comunque parziale (se il cookie è già presente resta registrato);
- **non** considera valido il consenso manifestato attribuendo tale significato alla "**inattività**" dell'utente (l'intenzione dell'interessato è presunta o implicita).

Profilazione: GDPR vs e-privacy Directive

La posizione del WP Art29

Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting (WP 224):

- fingerprint is as "a set of information elements that identifies a device or application instance"
- device fingerprinting presents serious data protection concerns for individuals;
- a number of online services have proposed device fingerprinting as an alternative to HTTP cookies for the purpose of providing analytics or for tracking without the need for consent under Article 5(3);

Profilazione: GDPR vs e-privacy Directive

La posizione del WP Art29

Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting (WP 224):

- article 5(3) of the ePrivacy Directive sets the requirement for consent from the user for any party which intends to store or access information stored in the user's terminal device, **even if that information is not yet considered to be personal data**.
- where device fingerprinting requires the storage of, or access to, (a set of) information on the user's device then consent will be required (unless a valid exemption applies).

Profilazione: GDPR vs e-privacy Directive

La proposta della Commissione di nuovo ePrivacy Regulation

Dalle consultazioni pubbliche condotte (apr-lug 2016) e sulla base delle successive analisi è stata scelta la soluzione di una "**Measured reinforcement of privacy/confidentiality and simplification**" che si traduce nella previsione di una semplificazione per la gestione dei cookies (e degli altri strumenti di analisi della navigazione web).

La Commissione ritiene che:

"By centralising the consent in software such as internet browsers and prompting users to choose their privacy settings and expanding the exceptions to the cookie consent rule, a significant proportion of businesses would be able to do away with cookie banners and notices, thus leading to potentially significant cost savings and simplification"

Profilazione: GDPR vs e-privacy Directive

La proposta di ePrivacy Regulation: la opinion 247 del WP ART29

- Working Party believes that general settings of browsers and other software, including operating systems, apps and software interfaces for Internet of Things-connected devices (i.e. not on the basis of specific granular controls) cannot be a valid measure for providing consent;
- It should be clarified that the offering of the possibility to block (third party) cookies under Art. 10 of the Proposed Regulation takes precedence over the exception for web audience measuring under Art. 8(1)

Fine intervento su
GDPR:
Focus on la profilazione dei dati personali

Per eventuali approfondimenti sui temi trattati

Luciano Delli Veneri – luciano.delliveneri@gmail.com

Gloria Marcoccio – gloria.marcoccio@glory.it