LUISS

Alessandro del Ninno

Il GDPR come presupposto e presidio per l'AI Act.

Relazione al Convegno ePrivacy XXXII «Privacy, AI e Security: un trinomio complesso» – Edizione estate 2023 – Roma 15 Giugno 2023

La proposta di Regolamento Generale UE sull’Intelligenza Artificiale (AI Act): a che punto siamo?

PROPOSTA DI REGOLAMENTO GENERALE UE SULL'INTELLIGENZA ARTIFICIALE

Il **25 novembre 2022** il Consiglio dell'UE ha approvato una versione di compromesso della proposta di Regolamento Generale UE sull'intelligenza artificiale (*AI Act*).

Il nuovo compromesso, **il quarto in totale**, è stato discusso in occasione della riunione del Consiglio dello scorso **6 dicembre 2022** in cui è stata espressa la posizione comune del Consiglio sull'AI Act (che è una proposta della **Commissione UE**, originariamente presentata il 21 aprile 2021).

Il Parlamento europeo ha adottato la sua posizione il **14 Giugno 2023 nella seduta plenaria** sul corpus di norme sull'IA aprendo la strada ai negoziati interistituzionali (**trilogo**) destinati a finalizzare la prima legge completa al mondo sull'intelligenza artificiale**.**

I negoziati del trilogo si intensificheranno una volta che la Spagna assumerà la presidenza di turno del Consiglio a luglio, poiché **Madrid ha fatto del completamento della legge sull'IA e della sua definitiva approvazione entro la fine del 2023 la sua massima priorità digitale**.

PROPOSTA DI REGOLAMENTO GENERALE UE SULL'INTELLIGENZA ARTIFICIALE

Le principali modifiche apportate al testo dell'AI Act dal Parlamento europeo.

I deputati hanno introdotto diverse altre modifiche significative al testo, a partire **dalla definizione di IA allineata a quella dell'OCSE.**

L'elenco delle **pratiche di AI proibite** è stato esteso alle **tecniche subliminali,** alla **categorizzazione biometrica,** alla **polizia predittiva**, ai **database di riconoscimento facciale** eliminati da Internet e il **software di riconoscimento delle emozioni** è vietato nelle forze dell'ordine, nella gestione delle frontiere, sul posto di lavoro e nell'istruzione.

È stato aggiunto un ulteriore livello per le applicazioni di IA che rientrano nella **categoria ad alto rischio**,. I **sistemi di raccomandazione** dei principali social media sono stati aggiunti come ad alto rischio, al pari dei **sistemi AI generativi di fondazione**.

Gli obblighi dei fornitori di IA ad alto rischio in materia di gestione del rischio, **governance dei dati** e documentazione tecnica sono stati resi più prescrittivi. Sono stati introdotti nuovi requisiti per condurre **valutazioni d'impatto sui diritti fondamentali e monitorare l'impatto ambientale**.

L’approccio basato sul rischio: applicazione pratica degli articoli 5 e 24 GDPR.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
APPROCCIO BASATO SUL RISCHIO

Articolo 24 - Responsabilità del titolare del trattamento

1. Tenuto conto della **natura**, **dell'ambito di applicazione**, del **contesto** e delle **finalità del trattamento**, **nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche**, il titolare del trattamento **mette in atto misure tecniche e organizzative adeguate** per garantire**, ed essere in grado di dimostrare**, che il trattamento è effettuato conformemente al presente regolamento. **Dette misure sono riesaminate e aggiornate qualora necessario.**

2. Se ciò è **proporzionato** rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono **l'attuazione di politiche adeguate in materia di protezione dei dati** da parte del titolare del trattamento.

3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 **può essere utilizzata** come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
APPROCCIO BASATO SUL RISCHIO

«***Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche***»….

Articolo 25 GDPR (privacy by design – privacy by default)
Articolo 30.5 GDPR (Registro delle attività di trattamento per imprese con meno di 250 dipendenti, se trattamento presenta rischi)
Articolo 32 (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)
Articolo 35 (DPIA in caso di «rischio elevato»)
Articolo 39.2 (Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo)
Articolo 49 (informativa all'interessato che acconsente al trasferimento dopo aver valutato i rischi)

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
APPROCCIO BASATO SUL RISCHIO

Quali sono i rischi rispetto ai quali svolgere l'assessment ai fini della conformità?

*I rischi per i diritti e le libertà delle persone fisiche, **aventi probabilità e gravità diverse**, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati* **(Considerando 75)**

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
APPROCCIO BASATO SUL RISCHIO

Rischio diretto per la persona

1.trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, trattamenti di dati personali suscettibili di cagionare discriminazioni, furto o usurpazione d'identità;
2.trattamenti di dati personali suscettibili di cagionare perdite finanziarie;
3.trattamenti di dati personali suscettibili di cagionare pregiudizio alla reputazione;
4.trattamenti di dati personali suscettibili di cagionare perdita di riservatezza dei dati personali protetti da segreto professionale;, decifratura non autorizzata della pseudonimizzazione;
5.trattamenti di dati personali suscettibili di cagionare qualsiasi altro danno economico o sociale significativo;
6.trattamenti di dati personali di dati di particolare natura o relativi a condanne e reati, rischiosi *per se* (con approccio svolto legislativamente a monte)
7.trattamenti di dati personali suscettibili di privare gli interessati dei loro diritti e delle loro libertà;
8.trattamenti di dati personali suscettibili di impedire agli interessati l'esercizio del controllo sui dati personali che li riguardano
9.trattamenti di profilazione;
10.trattamenti dei dati di soggetti vulnerabili;
11.trattamenti di una notevole quantità di dati personali e un vasto numero di interessati.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
APPROCCIO BASATO SUL RISCHIO

Come svolgere nella pratica l'approccio *risk based*?

La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato ***in base a una valutazione oggettiva*** *mediante cui* ***si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato*** **(Considerando 76)**

Es: 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 (**Art. 34 GDPR**)

Es: 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** (valutazione in negativo del rischio).

.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI N. 2016/679
APPROCCIO BASATO SUL RISCHIO

Il rischio di sicurezza

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla **distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale**, a dati personali trasmessi, conservati o comunque trattati.

I sistemi di Intelligenza Artificiale e l’approccio risk based come scelta legislativa per la regolamentazione dei sistemi IA.

PROPOSTA DI REGOLAMENTO GENERALE UE SULL'INTELLIGENZA ARTIFICIALE

Definizione di rischio nell'AI Act

Partiamo dalla definizione: con questo termine, si intende "**la combinazione della probabilità che si verifichi un pericolo che causa un danno e il grado di gravità di tale danno**".

L'Artificial Intelligence Act **ne prevede quattro:**

"rischio minimo o nullo", in cui secondo la Commissione europea rientra la "stragrande maggioranza" dei sistemi attualmente utilizzati nell'Ue;

"rischio limitato", da applicare ai sistemi con "obblighi specifici di trasparenza";

"rischio alto", che si riscontra all'interno di infrastrutture critiche o nei contesti lavorativi ed educativi in cui il risultato di esami o risposte potrebbe essere determinato dall'IA;

"rischio inaccettabile", ovvero tutto ciò che rappresenta una chiara minaccia per l'essere umano, inclusa l'assegnazione di punteggi sociali da parte dei governi a strumenti che utilizzato l'assistenza vocale che incoraggia comportamenti pericolosi, i sistemi di identificazione biometrica in tempo reale e a distanza, come il riconoscimento facciale.

PROPOSTA DI REGOLAMENTO GENERALE UE SULL'INTELLIGENZA ARTIFICIALE

I sistemi di AI ad alto rischio

Sono i sistemi di intelligenza artificiale **che influiscono negativamente sulla sicurezza o sui diritti fondamentali** e saranno suddivisi in due categorie:

1) I sistemi di intelligenza artificiale utilizzati in prodotti **soggetti alla direttiva dell'UE sulla sicurezza generale dei prodotti**. Questi includono giocattoli, aviazione, automobili, dispositivi medici e ascensori.
2) I sistemi di intelligenza artificiale che rientrano in **aree specifiche previste dall'Allegato III** e che dovranno essere registrati in un database dell'UE:

- ✓ identificazione e categorizzazione biometrica di persone naturali
- ✓ gestione e funzionamento di infrastrutture critiche
- ✓ istruzione e formazione professionale
- ✓ occupazione, gestione dei lavoratori e accesso all'autoimpiego
- ✓ accesso e fruizione di servizi privati (credit scoring, assicurazioni, etc) e servizi pubblici e vantaggi
- ✓ forze dell'ordine
- ✓ gestione delle migrazioni, asilo e controllo delle frontiere
- ✓ assistenza nell'interpretazione e applicazione legale della legge
- ✓ Sistemi di raccomandazione on line
- ✓ AI generativa

PROPOSTA DI REGOLAMENTO GENERALE UE SULL'INTELLIGENZA ARTIFICIALE

L'IA generativa, come ChatGPT, dovrà rispettare requisiti di trasparenza:

- rivelare che il contenuto è stato generato da un'intelligenza artificiale
- progettare il modello in modo da impedire la generazione di contenuti illegali
- pubblicare riepiloghi dei dati con **diritti d'autore utilizzati** per l'addestramento.

PROPOSTA DI REGOLAMENTO GENERALE UE SULL'INTELLIGENZA ARTIFICIALE

Quale comparazione è possibile effettuare tra l'approccio risk based richiesto dal Regolamento 679/2016 e quella di cui alla proposta di regolamento sull'IA?

Il GDPR non richiama parametri fissi nella individuazione dei rischi e nella loro classificazione: sostanzialmente, introduce una prima e generica distinzione tra *"rischi aventi probabilità e gravità diverse"* ancorando poi l'approccio risk based alle due categorie del "*rischio*" e del "*rischio elevato*", tipologie a cui il Legislatore ricollega obblighi e adempimenti diversificati.

L'approccio risk based che ritroviamo invece nella proposta di Regolamento UE sull'Intelligenza Artificiale si connota per una maggiore chiarezza pratica che sottrae a valutazioni soggettive la corretta individuazione del rischio connesso alla operatività di un sistema IA immesso sul mercato o semplicemente messo in uso. Si intende dire che la individuazione di un *"alto rischio"* connesso ai sistemi IA non è lasciata agli operatori e alle loro valutazioni soggettive da documentare (come – per i trattamenti di dati personali – accade per Titolari e Responsabili), ma è fatta direttamente dal Legislatore, che:

1. elenca addirittura tali sistemi nello specifico Allegato III;
2. fissa un duplice criterio generale per cui sono da considerarsi ad alto rischio in ogni caso i sistemi IA che sono componenti di sicurezza di apparati o sono essi stessi prodotti regolamentati dalla **normativa di armonizzazione elencata nell'Allegato II**.

PROPOSTA DI REGOLAMENTO GENERALE UE SULL'INTELLIGENZA ARTIFICIALE

Quindi non c'è spazio interpretativo per la valutazione del rischio, con il Legislatore del Regolamento IA che in un certo senso avoca a sé la individuazione della tipologia di rischio e anche l'aggiornamento periodico dei parametri e dei criteri legislativi e tecnologici applicati (si pensi alla **revisione biennale dell'Allegato III cui procederà la Commissione** o all'articolo 7 che prescrive – alla Commissione – i criteri interpretativi per gli aggiornamenti periodici dell'elenco dei sistemi IA ad alto rischio o per la **eliminazione dall'elenco di quelli che non pongono più significativi rischi per la salute, la sicurezza e i diritti fondamentali**).

In pratica: per individuare se un sistema IA sia o meno ad alto rischio, all'operatore non resta che fare una mera comparazione formale tra il suo sistema, i sistemi menzionati dalla legislazione di armonizzazione di cui all'Allegato II o i sistemi elencati per categorie in Allegato III.

Poi – certamente – i diversi approcci risk based del GDPR e del Regolamento IA hanno anche dei rilevanti punti di contatto, se non di sovrapposizione: ad esempio, i trattamenti di dati personali implicati dai sistemi IA alto rischio elencati all'Allegato III del Regolamento comporteranno sempre il "rischio elevato" per i diritti e le libertà fondamentali degli interessati di cui al GDPR; oppure, laddove nella fase di addestramento o di operatività di un sistema IA vengano in considerazione volumi considerevoli di dati (dataset) o di persone interessate, ecco che questa altro non è se uno dei parametri che il GDPR fissa per l'individuazione del "rischio elevato".

Il GDPR come presupposto e presidio dell’AI Act: i punti di contatto.

IL GDPR COME PRESUPPOSTO E PRESIDIO DELL'AI ACT

Art. 3 – Definizioni AI Act

"dati di addestramento": i dati utilizzati per addestrare un sistema di IA adattandone i parametri che può apprendere;

"dati di convalida": i dati utilizzati per fornire una valutazione del sistema di IA addestrato e per metterne a punto, tra l'altro, i parametri che non può apprendere e il processo di apprendimento, al fine di evitare l'eccessivo adattamento ai dati di addestramento (overfitting), considerando che il set di dati di convalida può essere un set di dati distinto o essere costituito da una partizione fissa o variabile del set di dati di addestramento;

"dati di prova": i dati utilizzati per fornire una valutazione indipendente del sistema di IA addestrato e convalidato al fine di confermarne le prestazioni attese prima della sua immissione sul mercato o messa in servizio;

"dati di input": i dati forniti a un sistema di IA o direttamente acquisiti dallo stesso, in base ai quali il sistema produce un output;

"dati biometrici": i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, quali l'immagine facciale o i dati dattiloscopici.

IL GDPR COME PRESUPPOSTO E PRESIDIO DELL'AI ACT

«La proposta di Regolamento Generale UE sull'Intelligenza Artificiale ***non pregiudica il regolamento generale sulla protezione dei dati (regolamento (UE) 2016/679)*** *e la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie (direttiva (UE) 2016/680) e li* ***integra con una serie di regole armonizzate applicabili alla progettazione, allo sviluppo e all'utilizzo di determinati sistemi di IA ad alto rischio*** *nonché di* ***restrizioni concernenti determinati usi dei sistemi di identificazione biometrica remota****. Essa integra inoltre il diritto dell'Unione in vigore in materia di non discriminazione con requisiti specifici che mirano* ***a ridurre al minimo il rischio di discriminazione algoritmica****, in particolare in relazione alla progettazione e alla qualità dei set di dati utilizzati per lo sviluppo dei sistemi di IA, integrati con obblighi relativi alle prove, alla gestione dei rischi, alla documentazione e alla sorveglianza umana durante l'intero ciclo di vita dei sistemi di IA»*

IL GDPR COME PRESUPPOSTO E PRESIDIO DELL'AI ACT

Considerando 58-bis AI Act

È opportuno chiarire che il presente regolamento ***lascia impregiudicati gli obblighi dei fornitori e degli utenti dei sistemi di IA nel loro ruolo di titolari del trattamento o responsabili del trattamento derivanti dal diritto dell'Unione in materia di protezione dei dati personali, nella misura in cui la progettazione, lo sviluppo o l'uso di sistemi di IA comportino il trattamento di dati personali.***

IL GDPR COME PRESUPPOSTO E PRESIDIO DELL'AI ACT

Considerando 41 AI Act

*«Il **fatto che un sistema di IA sia classificato come ad alto rischio a norma del presente regolamento non dovrebbe essere interpretato come un'indicazione del fatto che l'utilizzo del sistema sia lecito** a norma di altri atti giuridici dell'Unione o del diritto nazionale compatibile con il diritto dell'Unione, **ad esempio in materia di protezione dei dati personali**, uso di poligrafi e strumenti analoghi o di altri sistemi atti a rilevare lo stato emotivo delle persone fisiche. **Qualsiasi siffatto utilizzo dovrebbe continuare a verificarsi solo in conformità ai requisiti applicabili risultanti dalla Carta e dagli atti applicabili di diritto derivato dell'Unione e di diritto nazionale**. Il presente regolamento non dovrebbe essere inteso come un **fondamento giuridico per il trattamento dei dati personali**, comprese, ove opportuno, **categorie particolari di dati personali,** salvo quando diversamente disposto in modo specifico dal presente regolamento».*

IL GDPR COME PRESUPPOSTO E PRESIDIO DELL'AI ACT

Art. 10, comma 5, AI Act (Sistema di governance dei dati)

*Nella misura in cui ciò sia **strettamente necessario al fine di garantire il monitoraggio, il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio**, i fornitori di tali sistemi possono trattare categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del regolamento (UE) 2016/679, all'articolo 10 della direttiva (UE) 2016/680 e all'articolo 10, paragrafo 1, del regolamento (UE) 2018/1725, fatte salve le tutele adeguate per i diritti e le libertà fondamentali delle persone fisiche, comprese le limitazioni tecniche all'utilizzo e al riutilizzo delle misure più avanzate di sicurezza e di tutela della vita privata, quali la pseudonimizzazione o la cifratura, qualora l'anonimizzazione possa incidere significativamente sulla finalità perseguita*.

Considerando 44 AI Act

*E' opportuno che i fornitori siano in grado di trattare anche categorie particolari di dati personali, come **questione di interesse pubblico rilevante ai sensi dell'articolo 9, paragrafo 2, lettera g)** al fine di garantire il monitoraggio, il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio.*

IL GDPR COME PRESUPPOSTO E PRESIDIO DELL'AI ACT

Considerando 72-bis AI Act

Il presente regolamento ***dovrebbe fornire la base giuridica ai partecipanti allo spazio di sperimentazione normativa per l'IA*** *per utilizzare i dati personali raccolti per altre finalità ai fini dello sviluppo di determinati sistemi di IA di interesse pubblico nell'ambito dello spazio di sperimentazione normativa per l'IA, in linea con l'articolo 6, paragrafo 4, e l'articolo 9, paragrafo 2, lettera g), del regolamento (UE) 2016/679.* ***Tutti gli altri obblighi dei titolari del trattamento e i diritti degli interessati ai sensi del regolamento (UE) 2016/679 restano applicabili.***

IL GDPR COME PRESUPPOSTO E PRESIDIO DELL'AI ACT

GDPR, AI ACT E TRATTAMENTO DI DATI BIOMETRICI

Considerando 24 AI ACT

Qualsiasi trattamento di dati biometrici e di altri dati personali interessati dall'uso di sistemi di IA **a fini di identificazione biometrica per finalità diverse dalle attività di contrasto**, l'articolo 9, paragrafo 1, del regolamento (UE) 2016/679 vieta il trattamento di dati biometrici intesi a identificare in modo univoco una persona fisica, a meno che non si applichi una delle situazioni di cui al secondo paragrafo di tale articolo.

IL GDPR COME PRESUPPOSTO E PRESIDIO DELL'AI ACT

I principi fondamentali del trattamento dei dati personali (art. 5 GDPR) e il Considerando 44-bis dell'AI Act.

Nell'applicare i principi di cui all'articolo 5 del regolamento (UE) 2016/679 in particolare il principio della minimizzazione dei dati, per quanto riguarda ***i set di dati di addestramento, convalida e prova di cui al presente regolamento****, si dovrebbe tenere debitamente conto dell'intero ciclo di vita del sistema di IA*

IL GDPR COME PRESUPPOSTO E PRESIDIO DELL'AI ACT

La profilazione degli interessati operata da sistemi di AI

Considerando 58-bis AI Act

È opportuno chiarire che ***gli interessati continuano a godere di tutti i diritti e le garanzie loro conferiti dal diritto dell'Unione sulla protezione dei dati personali, compresi i diritti connessi al processo decisionale esclusivamente automatizzato relativo alle persone fisiche, compresa la profilazione****. Norme armonizzate per l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di IA istituiti a norma del presente regolamento dovrebbero facilitare l'effettiva attuazione e consentire l'esercizio dei diritti degli interessati e di altri mezzi di ricorso garantiti dal diritto dell'Unione in materia di protezione dei dati personali nonché degli altri diritti fondamentali.*

Art. 22 GDPR.

Considerando 72-bis AI Act

Il presente regolamento **non dovrebbe costituire una base giuridica ai sensi dell'articolo 22, paragrafo 2, lettera b)**, del regolamento (UE) 2016/679.

IL GDPR COME PRESUPPOSTO E PRESIDIO DELL'AI ACT

La Valutazione di impatto del GDPR nell'AI Act

Art. 29, comma 6, AI Act

Gli utenti di sistemi di IA ad alto rischio usano le informazioni fornite a norma dell'articolo 13 **per adempiere al loro obbligo di effettuare una valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 del regolamento (UE) 2016/679.**

LUISS

Email: adelninno@luiss.it

WWW: www.alessandrodelninno.it

Canale You Tube: https://www.youtube.com/user/AvvDelNinno

Linkedin: https://www.linkedin.com/in/alessandrodelninno/

Piattaforma di corsi FAD in streaming:
https://www.alessandrodelninno.it/corsi.php