IL REG. (UE) 2019/881 E IL REG. (UE) 2016/679

CYBERSECURITY ACT / RGPD-GDPR

ESAME DEI PUNTI D'INTERAZIONE

NOME FILE: PEDICO ALDO - ANALISI INTERAZIONI TRA 2019-881 E 2016-679.DOCX

SOMMARIO

Titolo _____ Pag.

Premessa *3*
Scopo *3*
Sintesi *4*
Dettaglio *5*
Argomento: Sicurezza *5*
Argomento: Affidabilità tecnologica *6*
Argomento: Resilienza *7*
Argomento: Rischio *8*
Argomento: Progettazione *9*
Argomento: Certificazione *9*
Argomento: Sanzioni *9*
Conclusioni *10*

PREMESSA

Prendendo spunto dai princìpi enunciati nei Considerando di seguito riportati, ho voluto evidenziare i punti chiave dell'origine della mia analisi.

I Considerando 1 e 2 del Reg. (UE) 2016/679 citano:

> *(1) La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale .....*
>
> Ed ancora
>
> *(2) I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati di carattere personale ("dati personali") dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza .....*

I Considerando 2 e 3 del Reg. (UE) 2019/881 citano:

> *(2) .... La digitalizzazione e la connettività stanno diventando caratteristiche fondamentali di un numero di prodotti e servizi in costante aumento, e con l'avvento dell'Internet degli oggetti (Internet of Things – IoT) nel prossimo decennio dovrebbero essere disponibile in tutta l'Unione un numero estremamente elevato di dispositivi digitali connessi. Sebbene un numero crescente di dispositivi sia connesso a Internet, la sicurezza e la resilienza non sono sufficientemente integrate nella progettazione, il che rende inadeguata la cibersicurezza. In tale contesto, l'uso limitato della certificazione fa sì che gli utenti individuali, nelle organizzazioni e nelle aziende dispongano di informazioni insufficienti sulle caratteristiche dei prodotti TIC (ICT), dei servizi TIC e dei processi TIC in termini di cibersicurezza, il che mina la fiducia nelle soluzioni digitali. .....*
>
> *(3) L'incremento della digitalizzazione e della connettività comporta maggiori rischi connessi alla cibersicurezza, il che rende la società in generale più vulnerabile alle minacce informatiche e aggrava i pericoli cui sono esposte le persone, comprese quelle vulnerabili come i minori. Al fine di attenuare tali rischi, occorre prendere tutti i provvedimenti necessari per migliorare la cibersicurezza nell'Unione allo scopo di proteggere meglio dalle minacce informatiche le reti e i sistemi informativi, le reti di comunicazione, i prodotti digitali, i servizi e i dispositivi utilizzati da cittadini, organizzazioni e imprese, a partire dalle piccole e medie imprese (PMI), ...*

SCOPO

Scopo della mia analisi non è esprimere un esercizio accademico bensì fornire uno strumento pratico che permetta di capire i punti di interazione tra le due leggi e gli impatti pratici, questi necessari allo svolgimento delle attività sia legali sia tecniche.

Nei paragrafi successivi, ho riportato una tabella di sintesi che, a fronte di un argomento, evidenzia gli articoli in cui tale argomento è trattato in entrambe le leggi.

Successivamente, ho riportato in dettaglio gli articoli di legge evidenziando in rosso gli aspetti chiave oggetto dell'analisi.

SINTESI

Entrambi i regolamenti presentano delle interazioni logiche che necessitano di essere esaminate.

Di seguito, la tabella, in modo sintetico, mette a confronto gli articoli di legge che evidenziano concetti logici e pratici tra loro strettamente correlati.

RIFERIMENTI INCROCIATI		
ARGOMENTO	REG. (UE) 2019/881 CYBERSECURITY ACT *Articoli*	REG. (UE) 2016/679 RGPD-GDPR *Articoli*
SICUREZZA	1 *in particolare; tutto il testo di legge;*	5; 32; 35; 40; 45;
AFFIDABILITÀ TECNOLOGICA	*CONCETTI: di base, sostanziale, elevata* 2; 52; 53; 54;	32;
RESILIENZA	1; 4;	32;
RISCHIO	5; 52;	33; 34; 35; 40;
PROGETTAZIONE	51;	25;
CERTIFICAZIONE E ORGANISMI	56;	24; 42; 43;
SANZIONI	65;	83; 84;

TABELLA DI SINTESI

DETTAGLIO

ARGOMENTO: *SICUREZZA*

REG. (UE) 2019/881	REG. (UE) 2016/679 RGPD-GDPR
Articolo 1 - Oggetto e ambito di applicazione 1. *Allo scopo di garantire il buon funzionamento del mercato interno perseguendo nel contempo un elevato livello di cibersicurezza, ciberresilienza e fiducia all'interno dell'Unione, il presente regolamento stabilisce: ....*	Articolo 5 - Principi applicabili al trattamento di dati personali 1. *Dati personali sono:* *lett. f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).* Articolo 32 - Sicurezza del trattamento 1. *..... 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 ...* 2. *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.* Articolo 35 - Valutazione d'impatto sulla protezione dei dati 7. *La valutazione contiene almeno:* *lett. d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità ...* Articolo 40 - Codici di condotta 2. *Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono elaborare i codici di condotta, ... a:* *lett. h) le misure e le procedure di cui agli articoli 24 e 25 e le misure volte a garantire la sicurezza del trattamento di cui all'articolo 32;* Articolo 45 - Trasferimento sulla base di una decisione di adeguatezza 1. *Il trasferimento di dati personali verso un paese terzo o un'organizzazione ....* 2. *Nel valutare l'adeguatezza del livello di protezione, ... i seguenti elementi:* *lett. a) lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), ...*

Considerazioni.

In entrambe le leggi, la sicurezza è il punto principale. Tale punto il GDPR lo considera lo strumento per garantire il dato personale mentre il 2019/881 estende il perimetro anche a tutti i dati e trattamenti che appartengono al sistema composto dalle tecnologie per le comunicazioni e comunicazioni informatiche.

ARGOMENTO: AFFIDABILITÀ TECNOLOGICA

REG. (UE) 2019/881

Articolo 2 - Definizioni

21) «livello di affidabilità»: base per la fiducia nel fatto che un prodotto TIC, servizio TIC o processo TIC soddisfa i requisiti di sicurezza di uno specifico sistema europeo di certificazione della cibersicurezza ..;

Articolo 52 - Livelli di affidabilità dei sistemi europei di certificazione della cibersicurezza

1. I sistemi europei di certificazione della cibersicurezza possono specificare per i prodotti TIC, i servizi TIC e i processi TIC uno o più dei seguenti livelli di affidabilità: «di base», «sostanziale» o «elevato». Il livello di affidabilità è commisurato al livello del rischio associato al previsto uso del prodotto TIC, servizio TIC o processo TIC, in termini di probabilità e impatto di un incidente.

2. I certificati europei di cibersicurezza e le dichiarazioni UE di conformità si riferiscono a qualsiasi livello di affidabilità specificato nel sistema europeo di certificazione della cibersicurezza ...

5. Un certificato europeo di cibersicurezza o una dichiarazione UE di conformità che si riferisca al livello di affidabilità «di base» assicura che .. rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo i rischi di base noti di incidenti e attacchi informatici ..

6. Un certificato europeo di cibersicurezza che si riferisca al livello di affidabilità «sostanziale» ... rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo i rischi noti connessi alla cibersicurezza e i rischi di incidenti e di attacchi informatici causati da soggetti dotati di abilità e risorse limitate ....

7. Un certificato europeo di cibersicurezza che si riferisca al livello di affidabilità «elevato» .... rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, ...

Articolo 53 - Autovalutazione della conformità

1. ... conformità sotto la sola responsabilità del fabbricante o del fornitore di prodotti TIC, servizi TIC o processi TIC. Tale autovalutazione della conformità è consentita unicamente in relazione ai prodotti TIC, servizi TIC e processi TIC che presentano un basso rischio corrispondenti al livello di affidabilità «di base».

Articolo 54 - Elementi dei sistemi europei di certificazione della cibersicurezza

1. Un sistema europeo di certificazione della cibersicurezza comprende almeno i seguenti elementi:

b) una chiara descrizione dello scopo del sistema e delle modalità con cui le norme, i metodi di valutazione e i livelli di affidabilità selezionati corrispondono alle esigenze degli utenti del sistema previsti;

REG. (UE) 2016/679 RGPD-GDPR

Articolo 32 - Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte .... 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, che comprendono, tra le altre, se del caso:

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

Considerazioni

Il 2019/881 introduce:

1. *il concetto di "affidabilità" a tre contesti: prodotto, servizio e processo; questo principio si correla con il "garantire un livello di sicurezza adeguato al rischio" descritto nell'articolo 32 del 2016/679*
2. *la definizione di "affidabilità «di base», «sostanziale», «elevata»";*
3. *il principio di "conformità";*
4. *il principio di "responsabilità del fabbricante o del fornitore" di prodotti, servizi o processi; questo principio è di fondamentale importanza per l'innesco di un cambiamento di mentalità nel sistema economico-sociale.*

ARGOMENTO: *RESILIENZA*

REG. (UE) 2019/881	REG. (UE) 2016/679 RGPD-GDPR
Articolo 1 - Oggetto e ambito di applicazione *1. Allo scopo di garantire il buon funzionamento del mercato interno perseguendo nel contempo un elevato livello di cibersicurezza, ciberresilienza e fiducia all'interno dell'Unione, il presente regolamento stabilisce: ..;* Articolo 4 - Obiettivi *3. L'ENISA sostiene lo sviluppo delle capacità e la preparazione ..... nel miglioramento della protezione delle loro reti e dei loro sistemi informativi, nello sviluppo e nel miglioramento delle capacità di ciberresilienza e di risposta, nonché nello sviluppo di abilità e competenze nel campo della cibersicurezza.*	Articolo 32 - Sicurezza del trattamento *2. Tenendo conto dello stato dell'arte .... 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 ...:* *c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;*

Considerazioni

Il 2019/881 introduce: la definizione di "ciberresilienza"; questo principio si correla con la "capacità di ripristinare" descritta nell'articolo 32 del 2016/679.

ARGOMENTO: *RISCHIO*

REG. (UE) 2019/881	REG. (UE) 2016/679 RGPD-GDPR
Articolo 5 - Sviluppo e attuazione delle politiche e della normativa dell'Unione *L'ENISA contribuisce allo sviluppo e all'attuazione delle politiche e della normativa dell'Unione:* *2) assistendo gli Stati membri nell'attuazione uniforme delle politiche e della normativa dell'Unione in materia di cibersicurezza, ..,, fornendo consigli e migliori pratiche su questioni quali la gestione del rischio, la segnalazione degli incidenti e la condivisione delle informazioni ..;* Articolo 52 - Livelli di affidabilità dei sistemi europei di certificazione della cibersicurezza *1. .... Il livello di affidabilità è commisurato al livello del rischio associato al previsto uso del prodotto TIC, servizio TIC o processo TIC, in termini di probabilità e impatto di un incidente..;* *4. .. Il certificato .., il cui obiettivo è ridurre il rischio di incidenti di cibersicurezza, o prevenirli..;*	Articolo 33 - Notifica di una violazione dei dati personali all'autorità di controllo Articolo 34 - Comunicazione di una violazione dei dati personali all'interessato Articolo 35 - Valutazione d'impatto sulla protezione dei dati *1. Quando un tipo di trattamento, .., può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, ...* *lett. c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e...* *lett. d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati ..* Articolo 40 - Codici di condotta *2. Le associazioni e gli altri organismi .. possono elaborare i codici di condotta, .., allo scopo di precisare l'applicazione del presente regolamento, ad esempio relativamente a:* *lett. i) la notifica di una violazione (incidente!) dei dati personali alle autorità di controllo e la comunicazione di tali violazioni dei dati personali all'interessato;*

Considerazioni

Il 2019/881 introduce:

1. *il principio di "gestione del rischio"; questo principio si correla con la "valutazione dei rischi" descritta nell'articolo 35 del 2016/679;*
2. *il principio di "segnalazione degli incidenti"; in caso di incidente potrebbe significare che questo principio si correli con la "Notifica" descritta nell'articolo 33, con la "Comunicazione" descritta nell'articolo 34, con la "Notifica" descritta nell'articolo 33, con la "notifica di una violazione" descritta nell'articolo 40 del 2016/679;*
3. *il principio di "probabilità e impatto di un incidente" e "il cui obiettivo è ridurre il rischio di incidenti di cibersicurezza, o prevenirli"; questo principio si correla con la "Valutazione d'impatto sulla protezione dei dati" descritta nell'articolo 35 del 2016/679.*

ARGOMENTO: PROGETTAZIONE

REG. (UE) 2019/881	REG. (UE) 2016/679 RGPD-GDPR
Articolo 51 - Obiettivi di sicurezza dei sistemi europei di certificazione della cibersicurezza *I sistemi europei di certificazione della cibersicurezza sono progettati per conseguire, se del caso, almeno i seguenti obiettivi di sicurezza:* *lett. i) i prodotti TIC, i servizi TIC e i processi TIC devono essere sicuri fin dalla progettazione e per impostazione predefinita;*	Articolo 25 - Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita

Considerazioni

Il 2019/881 introduce:

1. *il principio di "progettazione" dei sistemi e "sicuri fin dalla progettazione e per impostazione predefinita"; questo principio si correla con l'articolo 25 del 2016/679.*

ARGOMENTO: CERTIFICAZIONE

REG. (UE) 2019/881	REG. (UE) 2016/679 RGPD-GDPR
Articolo 56 - Certificazione della cibersicurezza	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. ... 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. Articolo 42 – Certificazione Articolo 43 – Organismi di certificazione

Considerazioni

Il principio di "Certificazione della cibersicurezza" di prodotti, servizi o processi; questo principio è di fondamentale importanza per l'innesco di un cambiamento di mentalità nel sistema economico-sociale.

ARGOMENTO: *SANZIONI*

REG. (UE) 2019/881	REG. (UE) 2016/679 RGPD-GDPR
Articolo 65 - Sanzioni	Articolo 83 – Condizioni generali per infliggere sanzioni amministrative pecuniarie Articolo 84 – Sanzioni

Considerazioni

CONCLUSIONI

L'esame dei punti d'interazione, esposto in precedenza, fa emergere diversi principi e tra questi ne esistono due che ritengo, a mio avviso, di estrema importanza; tali principi riguardano i prodotti, i servizi o i processi delle TIC (Tecnologie Informazione e Comunicazione).

I due principi sono:

1. "Responsabilità del fabbricante o del fornitore";
2. "Certificazione della cibersicurezza";

entrambi i principi sono di fondamentale importanza poiché sono alla base di un innesco del cambiamento di mentalità nel sistema economico-sociale.

Le responsabilità del fabbricante o del fornitore impongono investimenti per adottare tutte le misure necessarie alla protezione dei dati e dei sistemi, sino a spingere i Titolari del trattamento a certificare i prodotti, servizi o processi interni al sistema di gestione aziendale. Le società che intraprenderanno tale iniziativa molto probabilmente incrementeranno nel futuro le posizioni di mercato.

L'Unione Europea, con i regolamenti introdotti, ha iniziato a stabilire una soluzione di continuità legislativa che implica doveri a tutela dei diritti del cittadino, come dichiarato nel considerando 3 del Reg. (UE) 2019/881:

> *"…. Al fine di attenuare tali rischi, occorre prendere tutti i provvedimenti necessari per migliorare la cibersicurezza nell'Unione allo scopo di proteggere meglio dalle minacce informatiche le reti e i sistemi informativi, le reti di comunicazione, i prodotti digitali, i servizi e i dispositivi utilizzati da cittadini, organizzazioni e imprese, a partire dalle piccole e medie imprese (PMI), …"*

Se è vero che il danno economico è nell'immediato più facile da quantificare, il danno d'immagine potrebbe col tempo rivelarsi ben maggiore. Diventa quindi indispensabile la presa di coscienza da parte dei Titolari del trattamento che il danno non si limiti solo agli altri ma possa coinvolgere chiunque ed in qualsiasi momento, con costi elevati sia per le sanzioni ricevute sia per i danni subiti e cagionati.

Quindi, i Titolari del trattamento non si potranno più permettere di rimanere indifferenti e dovranno prendere in seria considerazione il fatto che prevenire è meglio che curare.