GARANTE EUROPEO DELLA PROTEZIONE DEI DATI

Sintesi del parere del Garante europeo della protezione dei dati sulla strategia in materia di cibersicurezza e sulla direttiva NIS 2.0

(Il testo integrale del parere è disponibile in inglese, francese e tedesco sul sito del GEPD www.edps.europa.eu)

(2021/C 183/03)

Il 16 dicembre 2020 la Commissione europea ha adottato una proposta di direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148 («la proposta»). Parallelamente, la Commissione europea e l'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza hanno pubblicato una comunicazione congiunta al Parlamento europeo e al Consiglio dal titolo «La strategia dell'UE in materia di cibersicurezza per il decennio digitale» («la strategia»).

Il GEPD sostiene pienamente l'obiettivo generale della strategia di assicurare una rete Internet globale e aperta con forti garanzie per affrontare i rischi per la sicurezza e per i diritti fondamentali, riconoscendo il valore strategico di Internet e della sua governance e rafforzando l'azione dell'Unione al riguardo, in un modello multipartecipativo.

Il GEPD accoglie pertanto con altrettanto favore l'obiettivo della proposta di introdurre modifiche sistemiche e strutturali all'attuale direttiva NIS al fine di coprire una più ampia gamma di soggetti in tutta l'Unione, con misure di sicurezza più rigorose, tra cui la gestione obbligatoria del rischio, norme minime e pertinenti disposizioni in materia di vigilanza ed esecuzione. A tal proposito, il GEPD ritiene necessario integrare pienamente le istituzioni, gli uffici, gli organi e le agenzie dell'Unione nel quadro globale dell'UE in materia di cibersicurezza per conseguire un livello uniforme di protezione, includendo esplicitamente le istituzioni, gli uffici, gli organi e le agenzie dell'Unione nell'ambito di applicazione della proposta.

Il GEPD sottolinea inoltre l'importanza di integrare la prospettiva della protezione della vita privata e dei dati nelle misure di cibersicurezza derivanti dalla proposta o da altre iniziative della strategia in materia di cibersicurezza, al fine di assicurare un approccio olistico e consentire la realizzazione di sinergie nella gestione della cibersicurezza e nella protezione delle informazioni personali trattate. È altrettanto importante che qualsiasi potenziale limitazione del diritto alla protezione dei dati personali e della vita privata derivante da tali misure soddisfi i criteri di cui all'articolo 52 della Carta dei diritti fondamentali dell'Unione europea e, in particolare, che sia realizzata mediante una misura legislativa e sia necessaria e proporzionata.

Il GEPD si attende che la proposta non miri a incidere sull'applicazione delle norme vigenti dell'UE che disciplinano il trattamento dei dati personali, compresi i compiti e i poteri delle autorità di controllo indipendenti competenti a controllare il rispetto di tali atti. Ciò significa che tutti i sistemi e i servizi di cibersicurezza coinvolti nella prevenzione, individuazione e risposta alle minacce informatiche dovrebbero essere conformi all'attuale quadro in materia di protezione della vita privata e dei dati. A tale riguardo, il GEPD ritiene importante e necessario stabilire una definizione chiara e univoca del termine «cibersicurezza» ai fini della proposta.

Il GEPD formula raccomandazioni specifiche per assicurare che la proposta integri correttamente ed efficacemente la normativa dell'Unione vigente in materia di protezione dei dati personali, in particolare il regolamento generale sulla protezione dei dati e la direttiva relativa alla vita privata e alle comunicazioni elettroniche, anche coinvolgendo il GEPD e il comitato europeo per la protezione dei dati, ove necessario e istituendo meccanismi chiari per la collaborazione tra le autorità competenti nei diversi ambiti normativi.

Inoltre, le disposizioni sulla gestione dei registri di dominio di primo livello di Internet dovrebbero definire chiaramente l'ambito di applicazione e le condizioni regolamentari pertinenti. Anche il concetto di scansione proattiva dei sistemi informatici e di rete da parte dei CSIRT richiede ulteriori chiarimenti sulla portata e sui tipi di dati personali trattati. Si richiama l'attenzione sui rischi di possibili trasferimenti di dati non conformi connessi all'esternalizzazione dei servizi di cibersicurezza o all'acquisizione di prodotti per la cibersicurezza e alla relativa catena di approvvigionamento.

Il GEPD accoglie con favore l'invito a promuovere l'uso della cifratura, in particolare la cifratura end-to-end, e ribadisce la sua posizione sulla cifratura quale tecnologia critica e insostituibile per un'efficace protezione dei dati e della vita privata, la cui elusione priverebbe il meccanismo di qualsiasi capacità di protezione a causa del suo eventuale uso illecito e della perdita di fiducia nei controlli di sicurezza. A tal fine, è opportuno chiarire che nessuna disposizione della proposta dovrebbe essere interpretata come un'approvazione dell'indebolimento della cifratura end-to-end mediante soluzioni di «backdoor» o analoghe.

1. **Introduzione e contesto**

1. Il 16 dicembre 2020 la Commissione europea ha adottato una proposta di direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148 ([1]) («la proposta»).

2. Lo stesso giorno la Commissione europea e l'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza hanno emesso una comunicazione congiunta al Parlamento europeo e al Consiglio dal titolo «La strategia dell'UE in materia di cibersicurezza per il decennio digitale» («la strategia») ([2]).

3. La strategia mira a rafforzare l'autonomia strategica dell'Unione nel settore della cibersicurezza e a migliorarne la resilienza e la risposta collettiva, nonché a costruire un'Internet globale e aperta con forti linee guida per affrontare i rischi per la sicurezza e per i diritti e le libertà fondamentali dei cittadini europei ([3]).

4. La strategia contiene proposte di iniziative normative, di investimento e politiche in tre settori di intervento dell'UE: 1) resilienza, sovranità tecnologica e leadership, 2) sviluppo delle capacità operative volte alla prevenzione, alla dissuasione e alla risposta e 3) promozione di un ciberspazio globale e aperto.

5. La proposta costituisce una delle iniziative normative della strategia, in particolare nel settore della resilienza, sovranità tecnologica e leadership.

6. Secondo la relazione, l'obiettivo della proposta è modernizzare il quadro giuridico esistente, vale a dire la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio («direttiva NIS) ([4]). La proposta mira a basarsi e abrogare l'attuale direttiva NIS, che è stata il primo strumento legislativo a livello dell'UE sulla cibersicurezza, e prevede misure giuridiche volte a incrementare il livello complessivo di cibersicurezza nell'Unione. La proposta tiene conto della crescente digitalizzazione del mercato interno avvenuta negli ultimi anni e del panorama in rapida evoluzione delle minacce alla cibersicurezza, fenomeni amplificati dall'inizio della crisi legata alla COVID-19. La proposta mira ad affrontare diverse carenze individuate nella direttiva NIS e ad aumentare il livello di ciberresilienza di tutti i settori, pubblici e privati, che svolgono una funzione importante per l'economia e la società.

7. Gli elementi essenziali della proposta sono i seguenti:

   (i) ampliamento dell'ambito di applicazione dell'attuale direttiva NIS aggiungendo nuovi settori sulla base della loro criticità per l'economia e la società;

   (ii) rafforzamento dei requisiti di sicurezza per le imprese e i soggetti contemplati, imponendo un approccio di gestione del rischio che preveda un elenco minimo di elementi di sicurezza di base che devono essere applicati;

   (iii) gestione della sicurezza delle catene di approvvigionamento e delle relazioni con i fornitori, imponendo alle singole imprese di affrontare i rischi di cibersicurezza nelle catene di approvvigionamento e nelle relazioni con i fornitori;

   (iv) rafforzamento della cooperazione tra le autorità degli Stati membri e le istituzioni, gli uffici, gli organi e le agenzie dell'Unione nella gestione delle attività connesse alla cibersicurezza, compresa la gestione delle crisi di cibersicurezza.

8. Il 14 gennaio 2021 il GEPD ha ricevuto una richiesta di consultazione formale da parte della Commissione europea sulla «Proposta di direttiva del Parlamento europeo e del Consiglio recante misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148».

3. **Conclusioni**

77. Alla luce di quanto sopra, il GEPD formula le seguenti raccomandazioni.

Per quanto riguarda la strategia in materia di cibersicurezza

— tenere conto del fatto che il primo passo per attenuare i rischi per la protezione dei dati e la vita privata associati alle nuove tecnologie per il miglioramento della cibersicurezza, come l'IA, consiste nell'applicare i requisiti in materia di protezione dei dati fin dalla progettazione e per impostazione predefinita di cui all'articolo 25 del regolamento generale sulla protezione dei dati, che contribuiranno a integrare le garanzie adeguate, quali la pseudonimizzazione, la cifratura, l'esattezza dei dati, la minimizzazione dei dati, nella progettazione e nell'uso di tali tecnologie e sistemi;

— tenere conto dell'importanza di integrare la prospettiva della protezione della vita privata e dei dati nelle politiche e nelle norme in materia di cibersicurezza nonché nella gestione tradizionale della cibersicurezza, al fine di garantire un approccio olistico e consentire sinergie alle organizzazioni pubbliche e private nella gestione della cibersicurezza e nella protezione delle informazioni che trattano senza inutili moltiplicazioni di sforzi;

— valutare e pianificare l'utilizzo delle risorse da parte delle IUE per rafforzare la loro capacità di cibersicurezza, anche nel pieno rispetto dei valori dell'UE;

— tenere conto delle dimensioni della protezione della vita privata e dei dati nella cibersicurezza investendo in politiche, prassi e strumenti in cui la prospettiva della protezione della vita privata e dei dati sia integrata nella gestione tradizionale della cibersicurezza e che preveda garanzie efficaci in materia di protezione dei dati nel trattamento dei dati personali nell'ambito delle attività di cibersicurezza.

Per quanto riguarda l'ambito di applicazione della strategia e della proposta per le istituzioni, gli uffici, gli organi e le agenzie dell'Unione

— tenere conto delle esigenze e del ruolo delle IUE affinché siano integrate in questo quadro globale della cibersicurezza a livello dell'UE come entità che godono dello stesso elevato livello di protezione di quelle degli Stati membri;

— includere esplicitamente le istituzioni, gli uffici, gli organi e le agenzie dell'Unione nell'ambito di applicazione della proposta.

Per quanto riguarda il rapporto con la normativa dell'Unione vigente in materia di protezione dei dati personali

— chiarire all'articolo 2 della proposta che la normativa dell'Unione in materia di protezione dei dati personali, in particolare il regolamento generale sulla protezione dei dati e la direttiva relativa alla vita privata e alle comunicazioni elettroniche, si applica a qualsiasi trattamento di dati personali che rientra nell'ambito di applicazione della proposta (invece che solo in contesti specifici); e

— chiarire inoltre in un considerando che la proposta non mira incidere sull'applicazione delle norme vigenti dell'UE che disciplinano il trattamento dei dati personali, compresi i compiti e i poteri delle autorità di controllo indipendenti competenti a controllare il rispetto di tali atti.

Per quanto riguarda la definizione di cibersicurezza

— chiarire il diverso uso dei termini «cibersicurezza» e «sicurezza delle reti e dei sistemi informativi»; utilizzare il termine «cibersicurezza» in generale e il termine «sicurezza delle reti e dei sistemi informativi» solo quando il contesto lo consente (ad esempio un contesto puramente tecnico, senza tenere conto dell'impatto anche sugli utenti dei sistemi e su altre persone).

Per quanto riguarda i nomi di dominio e i dati di registrazione («dati WHOIS»)

— specificare chiaramente cosa si intende per «informazioni pertinenti» per identificare e contattare i titolari dei nomi di dominio e i punti di contatto che amministrano i nomi di dominio sotto i TLD;

— chiarire in modo più dettagliato quali categorie di dati di registrazione del dominio (che non costituiscono dati personali) debbano essere oggetto di pubblicazione;

— chiarire ulteriormente quali soggetti (pubblici o privati) potrebbero costituire *«legittimi richiedenti l'accesso»*;

— chiarire se i dati personali in possesso dei registri TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio per il TLD debbano essere accessibili anche a soggetti al di fuori del SEE e, in caso affermativo, stabilire chiaramente le condizioni, le limitazioni e le procedure per tale accesso, tenendo conto anche dei requisiti di cui all'articolo 49, paragrafo 2, del regolamento generale sulla protezione dei dati, ove applicabile; e

— introdurre ulteriori chiarimenti in merito a cosa costituisca una richiesta *«legittima e debitamente giustificata»* in base alla quale è concesso l'accesso e a quali condizioni.

Per quanto riguarda la «scansione proattiva dei sistemi informatici e di rete» da parte dei CSIRT

— definire chiaramente i tipi di scansione proattiva che i CSIRT possono essere invitati a effettuare e individuare le principali categorie di dati personali interessati nel testo della proposta.

Per quanto riguarda l'esternalizzazione e la catena di approvvigionamento

— tenere conto delle caratteristiche che consentono l'efficace attuazione del principio della protezione dei dati fin dalla progettazione e per impostazione predefinita nella valutazione delle catene di approvvigionamento per la tecnologia e i sistemi di trattamento dei dati personali;

— tenere conto di requisiti specifici nel paese di origine che potrebbero rappresentare un ostacolo al rispetto della normativa dell'UE in materia di protezione della vita privata e dei dati nella valutazione dei rischi legati alla catena di approvvigionamento dei servizi, dei sistemi o dei prodotti TIC;

— includere nel testo normativo la consultazione obbligatoria del comitato europeo per la protezione dei dati al momento di definire le suddette caratteristiche e, se necessario, nella valutazione settoriale e coordinata dei rischi di cui al considerando 46;

— raccomandare di menzionare in un considerando che i prodotti open source per la cibersicurezza (software e hardware), compresa la cifratura open source, potrebbero offrire la trasparenza necessaria per attenuare i rischi specifici della catena di approvvigionamento.

Per quanto riguarda la cifratura

— chiarire nel considerando 54 che nessuna disposizione della proposta dovrebbe essere interpretata come un'approvazione dell'indebolimento della cifratura end-to-end mediante soluzioni di «backdoor» o analoghe.

Per quanto riguarda le misure di gestione dei rischi di cibersicurezza

— includere sia nei considerando sia nel dispositivo della proposta il concetto secondo cui l'integrazione della prospettiva della protezione della vita privata e dei dati nella tradizionale gestione dei rischi di cibersicurezza assicurerà un approccio olistico e consentirà sinergie alle organizzazioni pubbliche e private nella gestione della cibersicurezza e nella protezione delle informazioni che trattano senza inutili moltiplicazioni di sforzi;

— aggiungere nel testo normativo l'obbligo per l'ENISA di consultare il comitato europeo per la protezione dei dati in sede di elaborazione dei pareri pertinenti.

Per quanto riguarda le violazioni dei dati personali

— modificare il testo «entro un termine ragionevole» di cui all'articolo 32, paragrafo 1, in «senza indebito ritardo».

Per quanto riguarda il gruppo di cooperazione

— includere nel testo normativo la partecipazione del comitato europeo per la protezione dei dati al gruppo di cooperazione, tenendo conto del legame tra il compito di tale gruppo e il quadro in materia di protezione dei dati.

Per quanto riguarda la giurisdizione e la territorialità

— chiarire nel testo normativo che la proposta non incide sulle competenze delle autorità di controllo della protezione dei dati ai sensi del regolamento generale sulla protezione dei dati;

— fornire una base giuridica completa per la cooperazione e lo scambio di informazioni tra autorità competenti e autorità di controllo, ciascuna nel rispettivo ambito di competenza; e

— chiarire che le autorità competenti di cui alla proposta dovrebbero essere in grado di fornire alle autorità di controllo competenti ai sensi del regolamento (UE) 2016/679, su richiesta o di propria iniziativa, tutte le informazioni ottenute nel contesto di audit e indagini sul trattamento di dati personali e includere una base giuridica esplicita a tal fine.

Bruxelles, 11 marzo 2021.

Wojciech Rafał WIEWIÓROWSKI

(1) Proposta di direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/114, COM(2020) 823 final.
(2) La strategia dell'UE in materia di cibersicurezza per il decennio digitale, JOIN(2020) 18 final.
(3) Cfr. capitolo I. INTRODUZIONE, pag. 5 della strategia.
(4) Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016, pag. 1).