

Dichiarazione



Dichiarazione 2/2021 sul nuovo progetto di disposizioni del secondo protocollo addizionale alla Convenzione del Consiglio d'Europa sulla criminalità informatica (Convenzione di Budapest)

Adottata il 2 febbraio 2021

Il Comitato europeo per la protezione dei dati ha adottato la dichiarazione seguente.

Osservazioni preliminari e contesto della dichiarazione dell'EDPB

Il Comitato europeo per la protezione dei dati (EDPB) e le autorità preposte alla protezione dei dati all'interno dell'UE stanno seguendo da vicino lo sviluppo del secondo protocollo addizionale alla Convenzione di Budapest e hanno contribuito regolarmente alla consultazione tenuta dal Consiglio d'Europa, come ad esempio l'annuale "conferenza Octopus". Nel novembre 2019 l'EDPB ha anche pubblicato il suo ultimo contributo alla consultazione su un progetto di secondo protocollo addizionale¹, indicando di rimanere *disponibile per ulteriori contributi* e ha chiesto *un coinvolgimento più proattivo delle autorità preposte alla protezione dei dati fin dalle prime fasi della preparazione di queste specifiche disposizioni, al fine di garantire una comprensione e una considerazione ottimali delle garanzie per la protezione dei dati*².

In seguito alla pubblicazione di un nuovo progetto di disposizioni del secondo protocollo addizionale alla Convenzione di Budapest³, l'EDPB desidera rinnovare il proprio contributo esperto e costruttivo al fine di garantire che le riflessioni relative alla protezione dei dati siano tenute nel debito conto nel processo generale di elaborazione del protocollo addizionale, considerando che le riunioni dedicate

¹ https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf.

² L'EDPB conferma le posizioni e le raccomandazioni espresse in tale precedente contributo e ritiene pertinente ribadire i principi chiave alla luce degli ultimi sviluppi e dei nuovi progetti di disposizioni pubblicati.

³ <https://www.coe.int/en/web/cybercrime/-/towards-a-protocol-to-the-convention-on-cybercrime-additional-stakeholder-consultations>.

alla preparazione di tale protocollo si svolgono in sessioni chiuse e che nel mandato del T-CY⁴ non è stato previsto il coinvolgimento diretto delle autorità preposte alla protezione dei dati nel processo di elaborazione.

L'EDPB ritiene inoltre che le suddette disposizioni possano incidere sulle condizioni sostanziali e procedurali per l'accesso ai dati personali nell'UE, anche a seguito di richieste da parte di autorità di paesi terzi, allineandosi così ai dibattiti in corso a livello di UE e alle relative iniziative legislative attualmente all'esame dei legislatori⁵. L'EDPB chiede quindi alla Commissione europea e al Parlamento europeo, così come agli Stati membri dell'UE e ai parlamenti nazionali, di assicurare che i negoziati in corso ricevano un attento esame al fine di garantire la piena coerenza del previsto secondo protocollo addizionale con l'*acquis* dell'UE, in particolare nel campo della protezione dei dati personali.

L'accesso transfrontaliero ai dati personali è già stato affrontato in passato dalle autorità preposte alla protezione dei dati dell'UE in varie posizioni e pareri, e l'EDPB desidera ancora una volta ricordare in particolare le osservazioni del gruppo di lavoro Articolo 29 sulla questione dell'accesso diretto da parte delle autorità di polizia e giudiziarie di paesi terzi ai dati conservati in altri paesi, come proposto nel progetto di elementi per un protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica⁶, nonché la sua dichiarazione sugli aspetti relativi a protezione dei dati e privacy dell'accesso transfrontaliero alle prove elettroniche⁷. Il Garante europeo della protezione dei dati ha pubblicato il parere 3/2019 concernente il mandato per la partecipazione della Commissione ai negoziati⁸ e il parere 7/2019 sulle proposte relative agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale⁹. Questi contributi attingono anche al parere 23/2018 dell'EDPB sulle proposte della Commissione relative agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale¹⁰.

L'EDPB rimane pienamente consapevole del fatto che le circostanze per cui le autorità giudiziarie e di polizia si trovano di fronte a una "situazione transfrontaliera" rispetto all'accesso a dati personali nel contesto delle rispettive indagini possano risultare impegnative e riconosce l'obiettivo legittimo di rafforzare la cooperazione internazionale sulla criminalità informatica e l'accesso alle informazioni. Parallelamente, l'EDPB ribadisce che devono essere garantite la protezione dei dati personali e la certezza del diritto, contribuendo così all'obiettivo di stipulare accordi sostenibili per la condivisione di dati personali con paesi terzi per finalità di polizia e giudiziarie che siano pienamente compatibili con i trattati dell'UE e la Carta dei diritti fondamentali dell'Unione europea ("Carta"). L'EDPB ritiene inoltre essenziale inserire l'elaborazione del protocollo addizionale nel quadro dei valori e dei principi fondamentali del Consiglio d'Europa, con particolare riguardo ai diritti umani e allo Stato di diritto.

⁴ Mandato per l'elaborazione di un progetto di secondo protocollo aggiuntivo alla convenzione di Budapest sulla criminalità informatica, approvato dalla 17a sessione plenaria del Comitato della Convenzione sulla criminalità informatica (T-CY) l'8 giugno 2017, T-CY (2017)3.

⁵ In particolare, ma non solo, le discussioni sulle proposte della Commissione relative agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

⁶ Osservazioni del Gruppo di lavoro Articolo 29 sulla questione dell'accesso diretto delle autorità di contrasto di paesi terzi ai dati conservati in un'altra giurisdizione, come proposto nel progetto di elementi per un protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica, 5.12.2013.

⁷ Dichiarazione del Gruppo di lavoro Articolo 29 sugli aspetti relativi a protezione dei dati e privacy dell'accesso transfrontaliero alle prove elettroniche, 29 novembre 2017.

⁸ Parere 3/2019 del GEPD concernente la partecipazione ai negoziati in vista di un secondo protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica.

⁹ Parere 7/2019 del GEPD sulle proposte relative agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

¹⁰ Parere 23/2018 dell'EDPB, adottato il 26 settembre 2018, sulle proposte della Commissione relative agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

Per quanto riguarda "l'accesso transfrontaliero diretto a dati informatici memorizzati" di cui all'articolo 32, lettera b), della Convenzione di Budapest, l'EDPB ribadisce in particolare che, di norma, il titolare del trattamento può comunicare i dati solo sulla base di un'autorizzazione/un mandato dell'autorità giudiziaria o altro documento che giustifichi la necessità di accedere ai dati e indichi la base giuridica pertinente per tale accesso, presentati da un'autorità nazionale competente (giudiziaria o di polizia) conformemente al diritto interno, in cui sia anche specificato lo scopo per il quale i dati sono richiesti.

Poiché la Convenzione di Budapest e i suoi protocolli addizionali sono strumenti internazionali vincolanti, l'EDPB sottolinea che, in linea con la giurisprudenza della Corte di giustizia dell'Unione europea ("Corte"), "gli obblighi imposti da un accordo internazionale non possono avere l'effetto di compromettere i principi costituzionali del Trattato CE, tra i quali vi è il principio secondo cui tutti gli atti comunitari devono rispettare i diritti fondamentali, atteso che tale rispetto costituisce il presupposto della loro legittimità"¹¹. È quindi essenziale che le parti negoziali dell'UE assicurino che le disposizioni stabilite nel protocollo addizionale siano conformi all'*acquis* dell'UE nel campo della protezione dei dati, al fine di garantirne la compatibilità con il diritto primario e derivato dell'UE.

Considerando i tempi del processo di consultazione, il presente contributo dell'EDPB si concentrerà su una valutazione preliminare dei nuovi progetti di disposizioni del secondo protocollo addizionale alla Convenzione di Budapest che non sono stati oggetto di precedenti consultazioni :

- squadre investigative comuni e indagini congiunte;
- comunicazione accelerata dei dati informatici memorizzati in caso di emergenza;
- richiesta di informazioni sulla registrazione di nomi a dominio.

Ancora una volta, l'EDPB muove dall'assunto che le specifiche disposizioni sulla protezione dei dati personali siano ancora in discussione. L'EDPB resta a disposizione per ulteriori contributi e chiede un coinvolgimento più proattivo delle autorità preposte alla protezione dei dati fin dalle prime fasi della preparazione di queste specifiche disposizioni, al fine di garantire una comprensione e una considerazione ottimali delle garanzie per la protezione dei dati.

Progetto provvisorio di disposizioni sulle squadre investigative comuni e sulle indagini congiunte (JIT) (articolo 3), sulla richiesta di informazioni sulla registrazione dei nomi a dominio (articolo 6) e sulla comunicazione accelerata di dati informatici memorizzati in caso di emergenza (articolo 7)

Sulla scorta della sua valutazione preliminare, l'EDPB raccomanda di esaminare ulteriormente il progetto provvisorio di disposizioni per quanto riguarda gli elementi seguenti.

L'EDPB rileva che sia le richieste di informazioni sulla registrazione dei nomi a dominio sia quelle di comunicazione accelerata di dati informatici memorizzati, in casi di emergenza, sono richieste non vincolanti e che non sono chiaramente definiti i motivi di un eventuale rigetto; non è chiara neppure la possibilità di avvalersi della legge dello Stato parte richiesto per rifiutare tale cooperazione, compresi i motivi di rifiuto stabiliti nei MLAT (trattati di mutua assistenza giudiziaria)¹². L'EDPB ricorda a questo proposito che devono essere previste per legge le condizioni alle quali i fornitori di servizi di

¹¹ Cfr. sentenza della Corte di giustizia dell'Unione europea del 3 settembre 2008, *Kadi/Consiglio*, cause riunite C-402/05 P e C-415/05 P, ECLI:EU:C:2008:461, punto 285.

¹² Ad esempio, il progetto di articolo 6, paragrafo 2, si riferisce a "condizioni ragionevoli previste dal diritto nazionale".

comunicazione elettronica o l'entità che fornisce servizi di nomi a dominio sono tenuti a concedere tale accesso, in modo da garantire che il trattamento si fondi su una chiara base giuridica.

L'EDPB fa inoltre riferimento al suo precedente contributo per ribadire come l'EDPB ritenga che, eccettuati i casi di urgenza validamente accertati,¹³ e alla luce della giurisprudenza della Corte¹⁴, le autorità richiedenti dovrebbero limitarsi al pubblico ministero, a un'autorità giudiziaria o un'altra autorità indipendente. L'EDPB ritiene inoltre che il coinvolgimento sistematico delle autorità giudiziarie nelle parti richieste sia essenziale per garantire un esame efficace della conformità delle richieste alla Convenzione nonché l'applicazione del principio della doppia punibilità nel campo della cooperazione giudiziaria.

L'EDPB ricorda a questo proposito che il principio della doppia punibilità mira a fornire un'ulteriore salvaguardia per assicurare che una parte non possa avvalersi dell'assistenza di un'altra per applicare una sanzione penale inesistente nel diritto di tale altra parte. Oltre ad assicurare il rispetto dei diritti dei singoli e il giusto processo nel meccanismo previsto di cooperazione giudiziaria, tale salvaguardia prevede anche una garanzia essenziale relativa alle condizioni procedurali di accesso ai dati personali. Come già menzionato nel suo precedente contributo, in relazione alla sicurezza del trattamento dei dati, l'EDPB invita il T-CY a prendere in considerazione, come garanzia specifica per la protezione dei dati, un meccanismo finalizzato a notificare senza indugio le violazioni dei dati che potrebbero configurare gravi ingerenze nei diritti e nelle libertà degli interessati. Le violazioni dei dati personali potrebbero infatti incidere in modo significativo sui soggetti interessati.

In relazione al progetto provvisorio di disposizioni relative alla richiesta di informazioni sulla registrazione dei nomi a dominio, l'EDPB sottolinea che tali informazioni includono dati personali e che quindi qualsiasi strumento internazionale che stabilisca condizioni sostanziali e procedurali per l'accesso a tali dati deve, per le parti che sono membri dell'Unione europea, essere conforme al diritto primario e derivato dell'UE.

In relazione al progetto provvisorio di disposizioni sulla "comunicazione accelerata di dati informatici memorizzati in caso di emergenza" (articolo 7), l'EDPB rileva che, a seconda della sua applicazione ad opera di ciascuna parte, questa nuova disposizione può comportare la comunicazione diretta di dati relativi al contenuto. L'EDPB osserva altresì che lo Stato parte richiesto può richiedere, successivamente alla comunicazione dei dati, che sia presentata nelle debite forme una richiesta di mutua assistenza (articolo 7, paragrafo 5). In quest'ultimo caso, tuttavia, le parti del protocollo previsto non si impegnano a cancellare i dati o a non utilizzarli come prove se, sulla base delle informazioni supplementari ottenute attraverso la successiva richiesta di mutua assistenza, le autorità richieste concludono che non sussistono le condizioni per la comunicazione dei dati in oggetto. La disciplina giuridica applicabile ai dati comunicati una volta che questi ultimi abbiano raggiunto il paese richiedente sembra quindi dipendere totalmente dal diritto interno di tale paese. L'assenza di vincoli a livello del protocollo comporta dunque il rischio di privare questa disposizione di qualsiasi salvaguardia in termini di trattamento dei dati personali già oggetto di comunicazione.

L'EDPB sottolinea infine il requisito dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'UE¹⁵, secondo cui eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla Carta sono soggette al principio di proporzionalità e possono essere apportate solo laddove siano necessarie. Per essere legittimo ai sensi del diritto dell'UE, quindi, il progetto di disposizioni del

¹³ L'EDPB osserva che si fa riferimento alla nozione di emergenza ai sensi del paragrafo 1 del progetto di disposizione sulla mutua assistenza di emergenza e ritiene che la portata di tale nozione possa essere ulteriormente chiarita e contestualizzata.

¹⁴ Cfr. sentenza della Corte di giustizia dell'Unione europea del 21 dicembre 2016, *Tele2 Sverige AB*, cause riunite C-203/15 e C-698/15, ECLI:EU:C:2016:970, punto 120.

¹⁵ Cfr. anche l'articolo 8, paragrafo 2, della Convenzione europea dei diritti dell'uomo.

protocollo previsto deve soddisfare tale requisito. Ciò riguarda pertanto sia i dati personali contenuti nella richiesta sia quelli contenuti nella risposta a tale richiesta. **L'EDPB è quindi particolarmente preoccupato dalla formulazione del progetto di articolo 6, paragrafo 3, lettera c) e da quella del paragrafo 13 del progetto di relazione esplicativa relativa a questa disposizione, che sembrano implicare che i paesi terzi richiedenti che sono parti del protocollo previsto possano non essere tenuti a rispettare il principio di proporzionalità nel rivolgere richieste a uno Stato membro dell'UE.** Inoltre non è del tutto chiaro se, ai sensi di queste disposizioni, sia possibile avvalersi del principio di proporzionalità come motivo di rifiuto.

Non è chiaro neanche se le parti siano vincolate dagli obblighi di assicurare, nel contesto del protocollo previsto, le condizioni e tutele di cui all'articolo 15 della Convenzione di Budapest¹⁶. **L'EDPB raccomanda di chiarire che gli obblighi di cui all'articolo 15 della Convenzione di Budapest si applicano pienamente anche nel contesto di questa cooperazione transfrontaliera.**

Disposizioni sulle garanzie per la protezione dei dati

L'EDPB ritiene essenziale che il testo provvisorio reso pubblico sia integrato da disposizioni specifiche sulle garanzie per la protezione dei dati, da valutare poi insieme ad altre disposizioni, al fine di garantire che il progetto di protocollo addizionale si traduca in un accordo sostenibile per la condivisione di dati personali con paesi terzi a fini di polizia e giudiziari, pienamente compatibile con i trattati dell'UE e con la Carta.

Il progetto provvisorio di disposizioni sulla richiesta di informazioni sulla registrazione del nome a dominio e sulla comunicazione accelerata di dati informatici memorizzati in caso di emergenza, stabilendo le condizioni procedurali per l'accesso ai dati personali, può di per sé incidere sul livello di protezione dei dati personali, e potrebbe anche necessitare di emendamenti per garantire l'applicazione operativa di adeguate garanzie per la protezione dei dati. **A questo proposito, l'EDPB desidera sottolineare nuovamente la necessità di applicare le garanzie per la protezione dei dati a qualsiasi scambio di dati personali nel contesto del protocollo previsto¹⁷, anche in relazione al trasferimento di dati personali¹⁸.**

L'EDPB ritiene che le disposizioni specifiche sulle garanzie per la protezione dei dati debbano riflettere i principi chiave e in particolare quelli di liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza. Analogamente, l'EDPB sottolinea l'importanza di garantire i diritti individuali fondamentali (accesso, rettifica, cancellazione) – limitando qualsiasi restrizione nel rispetto del principio di proporzionalità – e un efficace ricorso giudiziario per gli interessati in caso di violazione delle garanzie per la protezione dei dati. L'esercizio di tali diritti richiede anche la notifica all'interessato, almeno una volta che tale notifica non metta più a rischio l'indagine. Questi principi, diritti e obblighi sono anche in linea con la Convenzione aggiornata del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale (Convenzione 108+), alla quale hanno aderito anche molte parti della Convenzione di Budapest sulla criminalità informatica. Conformemente alla Convenzione 108+, essi dovrebbero applicarsi a tutte le autorità che trattano i dati nella parte richiedente, al fine di garantire la continuità della protezione. **Per ulteriori dettagli sulle disposizioni**

¹⁶ Cfr. in particolare l'articolo 6, paragrafo 4, tra parentesi.

¹⁷ L'articolo 6, paragrafo 4, sembra limitare l'applicazione delle garanzie e dell'articolo 15 della Convenzione alle sole informazioni comunicate e non ai dati personali inclusi nella richiesta.

¹⁸ Secondo il paragrafo 9 del progetto di relazione esplicativa, quest'ultima disposizione potrebbe/dovrebbe applicarsi esclusivamente al trasferimento di dati personali ai sensi delle disposizioni sulle squadre investigative comuni.

dell'UE a questo riguardo, l'EDPB rimanda al proprio contributo fornito nella consultazione pubblica del 2019¹⁹.

L'EDPB ribadisce l'importanza di coinvolgere le autorità preposte alla protezione dei dati nel processo di redazione del protocollo addizionale ed è pronto a contribuire e coadiuvare il T-CY nella redazione del testo provvisorio delle disposizioni sulle garanzie per la protezione dei dati.

Per il Comitato europeo per la protezione dei dati

La presidente

(Andrea Jelinek)

¹⁹ https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf.