2024/2659

16.10.2024

RACCOMANDAZIONE (UE) 2024/2659 DELLA COMMISSIONE

dell'11 ottobre 2024

relativa a orientamenti sull'esportazione di prodotti di sorveglianza informatica a norma dell'articolo 5 del regolamento (UE) 2021/821 del Parlamento europeo e del Consiglio

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 292,

considerando quanto segue:

(1) Il regolamento (UE) 2021/821 del Parlamento europeo e del Consiglio ([1]) istituisce un regime dell'Unione di controllo delle esportazioni, dell'intermediazione, dell'assistenza tecnica, del transito e del trasferimento di prodotti a duplice uso.

(2) Il regolamento (UE) 2021/821 affronta il rischio che prodotti di sorveglianza informatica siano usati in connessione alla repressione interna e/o all'attuazione di gravi violazioni dei diritti umani o del diritto umanitario internazionale.

(3) A norma dell'articolo 5, paragrafo 2, e dell'articolo 26, paragrafo 1, del regolamento (UE) 2021/821, la Commissione e il Consiglio mettono a disposizione degli esportatori orientamenti per quanto riguarda i prodotti di sorveglianza informatica non compresi negli elenchi, data la necessità di assicurare l'efficienza del regime di controllo delle esportazioni dell'Unione in relazione alla cibersicurezza e la coerenza dell'attuazione di tale regolamento.

(4) La presente raccomandazione e gli orientamenti ad essa allegati mirano a sostenere gli esportatori nell'applicazione dei controlli sui prodotti di sorveglianza informatica non compresi negli elenchi, tra cui le misure di dovuta diligenza per valutare i rischi connessi all'esportazione di tali prodotti.

(5) Gli orientamenti allegati alla presente raccomandazione sono stati oggetto di ampie consultazioni nell'ambito del gruppo di esperti sulle tecnologie di sorveglianza nel 2022 e nel 2023 e tengono conto delle osservazioni ricevute nel quadro di una consultazione pubblica ([2]) svoltasi nel secondo trimestre del 2023.

(6) È opportuno ricordare che la presente raccomandazione e gli orientamenti allegati non hanno carattere vincolante. Gli esportatori dovrebbero pertanto rimanere tenuti a conformarsi agli obblighi loro imposti dal regolamento (UE) 2021/821, mentre la Commissione dovrebbe garantire che la presente raccomandazione rimanga pertinente nel tempo,

([1]) Regolamento (UE) 2021/821 del Parlamento europeo e del Consiglio, del 20 maggio 2021, che istituisce un regime dell'Unione di controllo delle esportazioni, dell'intermediazione, dell'assistenza tecnica, del transito e del trasferimento di prodotti a duplice uso (GU L 206 dell'11.6.2021, pag. 1, ELI: http://data.europa.eu/eli/reg/2021/821/oj).

([2]) https://policy.trade.ec.europa.eu/consultations/guidelines-export-cyber-surveillance-items-under-article-5-regulation-eu-no-2021821_en?prefLang=it.

HA ADOTTATO LA PRESENTE RACCOMANDAZIONE:

È raccomandato alle autorità competenti e agli esportatori degli Stati membri di tenere conto degli orientamenti di cui all'allegato della presente raccomandazione al fine di adempiere gli obblighi loro imposti dall'articolo 5, paragrafo 2, del regolamento (UE) 2021/821.

Fatto a Bruxelles, l'11 ottobre 2024

Per la Commissione
Valdis DOMBROVSKIS
Vicepresidente esecutivo

ALLEGATO

INDICE

INTRODUZIONE

Il quadro di controllo delle esportazioni dell'Unione istituito dal regolamento (UE) 2021/821 («regolamento») mira ad assicurare il rispetto degli obblighi e degli impegni internazionali dell'Unione e dei suoi Stati membri, anche in materia di pace, sicurezza e stabilità regionali e rispetto dei diritti umani e del diritto umanitario internazionale. L'Unione e i suoi Stati membri hanno pertanto attuato le decisioni adottate nell'ambito dei regimi multilaterali di controllo delle esportazioni e aggiornato di conseguenza l'elenco di controllo dell'Unione di cui all'allegato I del regolamento ([1]). Già prima che l'articolo 5 del regolamento diventasse applicabile, le autorità competenti degli Stati membri avevano peraltro sottoposto a controllo l'esportazione di alcuni prodotti compresi negli elenchi che possono avere applicazioni nel campo della sorveglianza ([2]), tenendo conto dei rischi di un uso improprio in determinate circostanze specifiche. In circostanze eccezionalmente gravi l'Unione ha imposto sanzioni volte a limitare l'esportazione di determinate apparecchiature di sorveglianza ([3]).

Il regolamento riflette l'impegno dell'Unione nell'affrontare efficacemente il rischio che prodotti di sorveglianza informatica siano usati in connessione alla repressione interna e/o all'attuazione di gravi violazioni dei diritti umani o del diritto umanitario internazionale. Il regolamento introduce in particolare nuove disposizioni per il controllo delle esportazioni di prodotti di sorveglianza informatica non compresi negli elenchi, incluso l'obbligo per gli esportatori di informare l'autorità competente se sono a conoscenza, stando ai risultati della dovuta diligenza, che prodotti di sorveglianza informatica che propongono di esportare, non compresi negli elenchi, sono destinati, in tutto o in parte, a un uso connesso alla repressione interna e/o all'attuazione di gravi violazioni dei diritti umani o del diritto umanitario internazionale. Inoltre, a norma del regolamento, la Commissione e il Consiglio sono tenuti a mettere a disposizione degli esportatori orientamenti per sostenere l'attuazione efficace dei nuovi controlli sui prodotti di sorveglianza informatica non compresi negli elenchi.

I presenti orientamenti mirano pertanto a sostenere gli esportatori nell'applicazione dei controlli sui prodotti di sorveglianza informatica non compresi negli elenchi, tra cui misure di dovuta diligenza per valutare i rischi connessi all'esportazione di tali prodotti per gli utenti finali e gli usi finali ai sensi delle nuove disposizioni del regolamento.

1. DISPOSIZIONI GIURIDICHE PERTINENTI, DEFINIZIONI E CONCETTI PRINCIPALI

1.1. Panoramica delle disposizioni giuridiche pertinenti

Il regolamento introduce nuove disposizioni che prevedono specificamente controlli sulle esportazioni di prodotti di sorveglianza informatica non compresi negli elenchi di cui all'allegato I del regolamento che sono o possono essere destinati, in tutto o in parte, a un uso connesso alla repressione interna e/o all'attuazione di gravi violazioni dei diritti umani o del diritto umanitario internazionale. I considerando e gli articoli pertinenti sono:

a) il considerando 8: «Al fine di affrontare il rischio che determinati prodotti di sorveglianza informatica non compresi negli elenchi esportati dal territorio doganale dell'Unione possano essere utilizzati impropriamente da parte di persone che, in qualità di complici o responsabili, ordinano o perpetrano gravi violazioni dei diritti umani o del diritto umanitario internazionale, è opportuno sottoporre a controllo le esportazioni di detti prodotti. I rischi associati riguardano, in particolare, i casi in cui i prodotti di sorveglianza informatica sono appositamente progettati per

([1]) Cfr. in particolare i controlli relativi ai sistemi di intercettazione delle telecomunicazioni (5A001.f.), ai sistemi di sorveglianza su Internet (5A001.j.), al software di intrusione (4A005, 4D004 e controlli correlati di cui alle voci 4E001.a e 4E001.c.) e al software per il monitoraggio da parte delle autorità di contrasto (5D001.e.). Cfr. inoltre, sulla base di una valutazione caso per caso, i controlli relativi a determinati strumenti forensi/investigativi (5A004.b., 5D002.a.3.b. e 5D002.c.3.b.).

([2]) In particolare i sistemi di sicurezza dell'informazione.

([3]) Cfr. il regolamento (CE) n. 765/2006 del Consiglio, del 18 maggio 2006, concernente misure restrittive in considerazione della situazione in Bielorussia e del coinvolgimento della Bielorussia nell'aggressione russa contro l'Ucraina (GU L 134 del 20.5.2006, pag. 1, ELI: http://data.europa.eu/eli/reg/2006/765/oj); il regolamento (UE) n. 359/2011 del Consiglio, del 12 aprile 2011, concernente misure restrittive nei confronti di determinate persone, entità e organismi in considerazione della situazione in Iran (GU L 100 del 14.4.2011, pag. 1, ELI: http://data.europa.eu/eli/reg/2011/359/oj); il regolamento (UE) n. 36/2012 del Consiglio, del 18 gennaio 2012, concernente misure restrittive in considerazione della situazione in Siria e che abroga il regolamento (UE) n. 442/2011 (GU L 16 del 19.1.2012, pag. 1, ELI: http://data.europa.eu/eli/reg/2012/36/oj); il regolamento (UE) n. 401/2013 del Consiglio, del 2 maggio 2013, concernente misure restrittive in considerazione della situazione nel Myanmar/Birmania e che abroga il regolamento (CE) n. 194/2008 (GU L 121 del 3.5.2013, pag. 1, ELI: http://data.europa.eu/eli/reg/2013/401/oj); e il regolamento (UE) 2017/2063 del Consiglio, del 13 novembre 2017, concernente misure restrittive in considerazione della situazione in Venezuela (GU L 295 del 14.11.2017, pag. 21, ELI: http://data.europa.eu/eli/reg/2017/2063/oj).

consentire l'intrusione o l'ispezione approfondita di pacchetti nei sistemi di informazione e telecomunicazioni al fine di effettuare una sorveglianza dissimulata di persone fisiche attraverso il monitoraggio, l'estrazione, la raccolta o l'analisi di dati, compresi i dati biometrici, da tali sistemi. I prodotti utilizzati per applicazioni puramente commerciali come la fatturazione, il marketing, i servizi di qualità, la soddisfazione degli utenti o la sicurezza della rete sono generalmente considerati esenti da rischi di questo tipo.»;

b) il considerando 9: «Al fine di rafforzare il controllo efficace delle esportazioni di prodotti di sorveglianza informatica non compresi negli elenchi, è necessario armonizzare ulteriormente l'applicazione di controlli onnicomprensivi in tale settore. A tal fine, gli Stati membri si impegnano a sostenere tali controlli condividendo informazioni tra loro e con la Commissione, in particolare per quanto riguarda gli sviluppi tecnologici dei prodotti di sorveglianza informatica, e vigilando nell'applicazione di tali controlli per promuovere uno scambio a livello di Unione.»;

c) l'articolo 2, punto 20), che definisce i «prodotti di sorveglianza informatica» come «prodotti a duplice uso appositamente progettati per consentire la sorveglianza dissimulata di persone fisiche mediante il monitoraggio, l'estrazione, la raccolta o l'analisi di dati provenienti da sistemi di informazione e telecomunicazione»;

d) l'articolo 5, che introduce un obbligo di autorizzazione per l'esportazione di prodotti di sorveglianza informatica non compresi negli elenchi nel caso in cui l'esportatore sia stato informato dall'autorità competente che detti prodotti sono o possono essere destinati, in tutto o in parte, a un uso connesso alla repressione interna e/o all'attuazione di gravi violazioni dei diritti umani o del diritto umanitario internazionale (articolo 5, paragrafo 1); tale articolo impone inoltre agli esportatori di informare l'autorità competente se sono a conoscenza, stando ai risultati della dovuta diligenza, che i prodotti sono destinati, in tutto o in parte, a un uso connesso alla repressione interna e/o all'attuazione di gravi violazioni dei diritti umani o del diritto umanitario internazionale (articolo 5, paragrafo 2); tale autorità competente deve decidere in merito all'opportunità di sottoporre l'esportazione interessata ad autorizzazione; e

e) l'articolo 5, paragrafo 2, che stabilisce inoltre: «La Commissione e il Consiglio mettono a disposizione degli esportatori gli orientamenti di cui all'articolo 26, paragrafo 1.».

1.2. **Definizioni principali**

Il regolamento prevede appositi considerando e disposizioni che precisano gli specifici termini pertinenti per i controlli sulle esportazioni di prodotti di sorveglianza informatica non compresi negli elenchi; è importante che gli esportatori comprendano chiaramente tali termini per poter esercitare la dovuta diligenza e attuare i controlli in modo efficace. Di particolare rilevanza è l'articolo 2, punto 20), il quale fornisce la seguente definizione precisa di «prodotti di sorveglianza informatica»: «prodotti a duplice uso appositamente progettati per consentire la sorveglianza dissimulata di persone fisiche mediante il monitoraggio, l'estrazione, la raccolta o l'analisi di dati provenienti da sistemi di informazione e telecomunicazione».

Ai fini dei presenti orientamenti è opportuno chiarire alcuni aspetti specifici di tale definizione.

1.2.1. *«Appositamente progettati»*

Un prodotto è progettato per la sorveglianza dissimulata quando le sue caratteristiche tecniche sono idonee alla sorveglianza dissimulata di persone fisiche e la consentono oggettivamente. Per «appositamente progettati» si intende pertanto che la sorveglianza dissimulata di persone fisiche deve essere stata la finalità principale dello sviluppo e della progettazione del prodotto. Tale definizione non richiede però che il prodotto possa essere usato esclusivamente per la sorveglianza dissimulata di persone fisiche.

Come chiarito nel considerando 8 del regolamento, i prodotti utilizzati per applicazioni puramente commerciali come la fatturazione, il marketing, i servizi di qualità, la soddisfazione degli utenti o la sicurezza della rete non sono appositamente progettati per la sorveglianza dissimulata di persone fisiche e pertanto non rientrano nella definizione di prodotti di sorveglianza informatica. Ad esempio, i prodotti per la sorveglianza dei sistemi operativi in ambito industriale o per il monitoraggio del traffico degli utenti potrebbero essere utilizzati a fini di sorveglianza, ma non rientrano nella definizione di prodotti di sorveglianza informatica in quanto non sono appositamente progettati per consentire la sorveglianza dissimulata di persone fisiche.

1.2.2. *«Sorveglianza dissimulata»*

I prodotti consentono una sorveglianza dissimulata in particolare quando la sorveglianza non è manifestamente percepibile dalla persona fisica interessata. Ciò avviene quando le persone interessate non sono consapevoli della presenza e/o dell'azione dei prodotti di sorveglianza informatica e non hanno pertanto la possibilità di sottrarsi a tale sorveglianza, o quantomeno di adeguare il proprio comportamento di conseguenza. Anche nel caso in cui la sorveglianza sia effettuata mediante prodotti installati o funzionanti nello spazio pubblico, in determinati casi l'acquisizione di dati può essere considerata rientrante nella definizione di sorveglianza dissimulata, in particolare laddove i dati raccolti possano essere dirottati, valutati o trattati per fini diversi da quelli resi noti alla persona fisica interessata. In altre parole, quando una persona fisica non può oggettivamente attendersi di essere sottoposta a sorveglianza, la sorveglianza può essere considerata dissimulata ai sensi dell'articolo 2, punto 20), del regolamento.

1.2.3. *«Persone fisiche»*

Per «persona fisica» si intende un essere umano vivente, in contrapposizione a una persona giuridica o a un'entità, le quali non sono pertanto soggette alle disposizioni. Il termine non comprende la sorveglianza di oggetti, siti o macchine in quanto tali.

1.2.4. *«Monitoraggio, estrazione, raccolta, analisi di dati»*

I dizionari attribuiscono il seguente significato ai lemmi «monitoraggio», «estrazione», «raccolta» e «analisi»:

— «monitoraggio»: controllo; sorveglianza, ascolto;

— «estrazione»: operazione dell'estrarre;

— «raccolta»: attività, lavoro del raccogliere;

— «analisi»: differenziare o accertare gli elementi di un tutto (complesso) al fine di determinarne la struttura o la natura e quindi spiegarlo o comprenderlo; esaminare attentamente e metodicamente a fini di interpretazione; sottoporre ad analisi critica o computazionale.

I termini in questione implicano che i prodotti usati per la sorveglianza dovrebbero disporre di capacità tecniche precise per il trattamento dei dati, al fine di monitorare, raccogliere, estrarre o analizzare dati. Ne sono esempio:

a) i prodotti usati per monitorare dati provenienti da sistemi di informazione e telecomunicazione ([4]) (ad esempio le dimensioni dei file o il traffico dei pacchetti di dati trasmessi in tale sistema);

b) i prodotti che estraggono dati provenienti da sistemi di informazione e telecomunicazione mediante intrusione ed estrazione (ad esempio software di intrusione);

c) i prodotti che consentono l'analisi dei dati estratti dai sistemi di informazione e telecomunicazione, compresi i prodotti in grado di elaborare immagini acquisite da videocamere e memorizzate in tali sistemi (ad esempio, alcuni tipi di tecnologie di analisi dei dati usate nell'ambito dei sistemi di riconoscimento facciale).

I prodotti utilizzati semplicemente per monitorare sistemi di informazione o per visualizzare la popolazione attraverso telecamere di videosorveglianza e che consentono di rilevare conversazioni, scambi di dati, movimenti e comportamenti individuali non costituirebbero prodotti di sorveglianza informatica secondo la definizione del regolamento, in quanto non sono appositamente progettati per tale finalità e devono essere utilizzati in abbinamento ad altre tecnologie quali l'intelligenza artificiale o i big data. Tuttavia, il sistema nella sua globalità (utilizzato in abbinamento ad altre tecnologie quali l'intelligenza artificiale o i big data) potrebbe costituire un prodotto di sorveglianza informatica ai sensi dell'articolo 2, punto 20), del regolamento.

È importante sottolineare, nel fornire alcuni esempi utili a scopo illustrativo, che la definizione e la portata dei prodotti di sorveglianza informatica non sono limitati da tali esempi, in quanto l'obiettivo dell'articolo 5 è consentire un controllo efficace delle esportazioni di prodotti non compresi negli elenchi.

([4]) Per la definizione cfr. il punto 1.2.5.

Come evidenziato dall'uso della congiunzione «o» nella definizione, le capacità tecniche indicate devono essere considerate alternative e non è necessario che un prodotto possieda tutte le capacità tecniche necessarie per il monitoraggio, l'estrazione, la raccolta o l'analisi di dati. In altre parole è sufficiente che un prodotto abbia una sola di dette capacità tecniche per rientrare nella definizione di prodotto di sorveglianza informatica di cui all'articolo 2, punto 20).

1.2.5. *«Provenienti da sistemi di informazione e telecomunicazione»*

Questa espressione si riferisce da un lato a sistemi che elaborano elettronicamente le informazioni, ad esempio programmazione/codifica, operazioni di sistemi PC (hardware) e altre attività di gestione dell'informazione, comprese la tecnologia software, la tecnologia web, la tecnologia informatica, la tecnologia di archiviazione ecc., e dall'altro ad alcuni sistemi che trasmettono informazioni a distanza, ad esempio sistemi tecnici che trasmettono suoni, segnali, testo, altri segni e immagini tramite canali con e senza fili, tramite fibra ottica, radio e altri sistemi elettromagnetici. Insieme, questi due concetti comprendono un'ampia gamma di sistemi di trasmissione o di trattamento delle informazioni. Va osservato che il termine si riferisce ai sistemi e non alle apparecchiature.

1.2.6. *«Conoscenza» e «sono destinati a»*

A norma dell'articolo 5, paragrafo 2, del regolamento, un esportatore è tenuto a informare l'autorità competente se è «a conoscenza […] che prodotti di sorveglianza informatica […] sono destinati» a un uso connesso alla repressione interna e/o all'attuazione di gravi violazioni dei diritti umani o del diritto umanitario internazionale.

Il termine «a conoscenza» non è un concetto giuridico nuovo, ma è stato utilizzato in relazione agli obblighi di autorizzazione collegati all'uso finale (i cosiddetti controlli «onnicomprensivi») a norma degli articoli 4, 6, 7 e 8 del regolamento. Il fatto di essere «a conoscenza» implica che l'esportatore ha una cognizione effettiva dell'uso improprio previsto. La mera eventualità che tale rischio possa sussistere non è sufficiente per stabilire che ne è a conoscenza. Il termine «conoscenza» non può tuttavia essere equiparato a un atteggiamento passivo, in quanto richiede che l'esportatore abbia adottato misure per acquisire conoscenze sufficienti e adeguate ai fini della valutazione dei rischi connessi all'esportazione, nonché per garantire il rispetto del regolamento.

L'indicazione secondo cui i prodotti devono essere «destinati a» un uso finale sensibile rilevante implica che l'esportatore dovrebbe valutare l'uso finale caso per caso, alla luce delle circostanze specifiche del caso in esame. Al contrario un rischio teorico (ossia non basato su una valutazione fattuale del caso) che i prodotti possano essere utilizzati in modo tale da violare i diritti umani non sarebbe sufficiente a permettere di dedurre che i prodotti in questione sono «destinati a» uno specifico uso improprio ai sensi dell'articolo 5.

1.3. **Repressione interna, gravi violazioni dei diritti umani o del diritto umanitario internazionale**

A norma dell'articolo 15 del regolamento, che stabilisce i fattori da considerare ai fini del rilascio di un'autorizzazione, gli Stati membri devono tenere conto di tutti i fattori pertinenti, tra cui le considerazioni cui si applica la posizione comune 2008/944/PESC del Consiglio ([5]).

L'articolo 5 del regolamento estende i controlli all'esportazione di prodotti di sorveglianza informatica non compresi negli elenchi in considerazione del rischio che siano usati in connessione alla repressione interna e/o all'attuazione di gravi violazioni dei diritti umani o del diritto umanitario internazionale. La posizione comune 2008/944/PESC e il manuale per l'uso della stessa ([6]) forniscono indicazioni utili al riguardo.

([5]) Posizione comune 2008/944/PESC del Consiglio, dell'8 dicembre 2008, che definisce norme comuni per il controllo delle esportazioni di tecnologia e attrezzature militari (GU L 335 del 13.12.2008, pag. 99, ELI: http://data.europa.eu/eli/compos/2008/944/oj).

([6]) Cfr. il manuale per l'uso della posizione comune 2008/944/PESC del Consiglio che definisce norme comuni per il controllo delle esportazioni di tecnologia e attrezzature militari, https://data.consilium.europa.eu/doc/document/ST-12189-2019-INIT/it/pdf.

1.3.1. *Repressione interna*

In conformità all'articolo 2, paragrafo 2, della posizione comune 2008/944/PESC, «[p]er repressione interna si intendono, fra l'altro, la tortura e altri trattamenti o punizioni crudeli, disumani e degradanti, le esecuzioni sommarie o arbitrarie, le sparizioni, le detenzioni arbitrarie e altre gravi violazioni dei diritti umani e delle libertà fondamentali definiti nei pertinenti strumenti internazionali in materia di diritti umani, compresa la Dichiarazione universale dei diritti dell'uomo e il Patto internazionale relativo ai diritti civili e politici» (ICCPR). Il manuale per l'uso della posizione comune 2008/944/PESC fornisce indicazioni sugli elementi da prendere in considerazione nella valutazione da parte dell'esportatore, quali l'esaminare, «sotto il profilo del rispetto dei diritti umani, il comportamento attuale e passato dell'utilizzatore finale previsto e quello del paese destinatario in generale».

1.3.2. *Attuazione di gravi violazioni dei diritti umani*

L'uso improprio di prodotti di sorveglianza informatica non compresi negli elenchi può incidere negativamente su un ampio ventaglio di diritti umani e interferisce direttamente con il diritto alla vita privata e alla protezione dei dati. Una sorveglianza arbitraria o illecita può violare anche altri diritti umani, quali il diritto alla libertà di espressione, di associazione e di riunione, la libertà di pensiero, di coscienza e di religione, il diritto alla parità di trattamento, o il divieto di discriminazione, e il diritto a elezioni libere, eque e a scrutinio segreto. In casi particolari la sorveglianza, compresi il monitoraggio o la raccolta di informazioni sulle persone fisiche, quali i difensori dei diritti umani, gli attivisti, le personalità politiche, le popolazioni vulnerabili e i giornalisti, può condurre a intimidazioni, repressioni, detenzioni arbitrarie, torture nonché a uccisioni extragiudiziali. Gli esportatori dovrebbero pertanto includere nelle loro valutazioni questi aspetti relativi a gravi violazioni dei diritti umani.

La prassi internazionale dimostra che eventuali restrizioni ai diritti umani devono essere «appropriate» e conformi alle norme internazionali in materia di diritti umani. In pratica ciò significa che esistono garanzie adeguate per assicurare che le restrizioni siano previste dalla legge e preservino l'essenza dei diritti. Nel rispetto del principio di proporzionalità, possono essere messe in atto restrizioni solo laddove siano necessarie e rispondano effettivamente a uno scopo legittimo, ad esempio la sicurezza nazionale o pubblica, l'ordine pubblico, la tutela della salute pubblica o la protezione dei diritti e delle libertà altrui.

I prodotti di sorveglianza informatica possono comprendere strumenti legittimi e regolamentati per applicazioni di contrasto, usati ad esempio per la prevenzione, l'indagine, l'accertamento e il perseguimento di reati – anche nel settore della lotta al terrorismo – o per l'esecuzione di sanzioni penali. Allo stesso tempo i prodotti di sorveglianza informatica possono anche essere usati impropriamente per commettere gravi violazioni dei diritti umani o del diritto internazionale umanitario quando sono esportati verso regimi repressivi o utenti finali privati e/o in zone di conflitto.

È pertanto necessaria una valutazione caso per caso delle circostanze specifiche, che comprenda l'applicazione dei regolamenti pertinenti alla luce di qualsiasi segnalazione di gravi violazioni dei diritti umani proveniente dagli organi competenti, ad esempio, delle Nazioni Unite, dell'Unione o del Consiglio d'Europa. Un indizio della «gravità» delle violazioni dei diritti umani può derivare dal fatto che tali violazioni trovino riscontro in informazioni pubblicate dagli organi competenti delle Nazioni Unite, dall'Unione o dal Consiglio d'Europa. Un simile riscontro esplicito da parte degli organismi citati non è una condizione necessaria, ma rappresenta un fattore importante nel valutare se questo criterio sia soddisfatto.

Ai sensi dell'articolo 5, la violazione dei diritti umani deve essere «grave». Il manuale per l'uso della posizione comune 2008/944/PESC fornisce indicazioni utili per valutare se le violazioni dei diritti umani siano qualificabili come «gravi». Secondo tale manuale sono determinanti la natura e le conseguenze della violazione. Le violazioni sistematiche e/o diffuse dei diritti umani sono regolarmente considerate gravi, ma possono essere considerate «gravi» anche violazioni che non sono né sistematiche né diffuse, ad esempio a causa della gravità dell'azione per le persone colpite.

L'allegato II del manuale per l'uso della posizione comune 2008/944/PESC contiene un elenco non esaustivo dei principali strumenti internazionali e regionali in materia di diritti umani, tra cui il Patto internazionale relativo ai diritti civili e politici (ICCPR), la Convenzione contro la tortura ed altre pene o trattamenti crudeli, disumani o degradanti, la Convenzione europea dei diritti dell'uomo («Convenzione») e la Carta dei diritti fondamentali («Carta»), che possono fornire indicazioni importanti per l'interpretazione e l'applicazione dei criteri a sostegno di valutazioni solide in materia di diritti umani. Tali strumenti e i relativi protocolli aggiuntivi costituiscono le norme e gli standard internazionali principali nei settori dei diritti umani e delle libertà fondamentali.

1.3.3. *Attuazione di gravi violazioni del diritto umanitario internazionale*

Il diritto umanitario internazionale (noto anche come «diritto di Ginevra» o «diritto dei conflitti armati») è stato elaborato attraverso una serie di trattati internazionali, i più importanti dei quali sono i regolamenti dell'Aia, le convenzioni di Ginevra e i relativi due protocolli aggiuntivi del 1977, e individua norme che, nel corso di un conflitto armato, mirano a proteggere le persone che non partecipano, o non partecipano più, alle ostilità (come i civili e i combattenti feriti, malati o prigionieri) e impongono alle parti belligeranti restrizioni quanto ai mezzi e ai metodi di guerra (diritto dell'Aia).

L'uso di prodotti di sorveglianza informatica non compresi negli elenchi deve conformarsi al diritto umanitario internazionale laddove tali prodotti siano impiegati come mezzi e metodi di guerra nel contesto di un conflitto armato. In simili circostanze il rischio di gravi violazioni del diritto umanitario internazionale è un fattore da prendere in considerazione ai sensi del regolamento e, come per l'attuazione di gravi violazioni dei diritti umani, tale rischio dovrebbe essere valutato alla luce dell'uso finale cui sono destinati i prodotti nel caso specifico. Il manuale per l'uso della posizione comune 2008/944/PESC fornisce indicazioni sugli elementi da prendere in considerazione, tra cui i comportamenti presenti e passati del destinatario in materia di rispetto del diritto internazionale umanitario, le intenzioni del destinatario espresse attraverso impegni formali e la capacità del destinatario di assicurare che la tecnologia o le attrezzature trasferite siano usate in modo conforme al diritto internazionale umanitario e non siano sviate o trasferite verso altre destinazioni in cui potrebbero essere usate per violazioni gravi di tale diritto.

Ai sensi dell'articolo 5, la violazione del diritto umanitario internazionale deve essere «grave». Indicazioni in merito si trovano nel manuale per l'uso della posizione comune 2008/944/PESC, in cui si riconosce che «[c]asi isolati di violazioni del diritto internazionale umanitario non sono necessariamente indicativi di un atteggiamento del paese destinatario nei confronti del diritto internazionale umanitario», mentre «[d]ovrebbe destare serie preoccupazioni il fatto che si possa distinguere un certo schema di violazioni o che il paese destinatario non abbia preso misure appropriate per punire le violazioni». Il Comitato internazionale della Croce Rossa (CICR) ha fornito orientamenti per la valutazione delle violazioni del diritto umanitario internazionale ai fini del controllo delle esportazioni. Secondo il CICR le violazioni del diritto umanitario internazionale sono gravi se mettono in pericolo persone protette (ad esempio civili, prigionieri di guerra, feriti e malati) o oggetti protetti (ad esempio beni o infrastrutture civili) o se ledono importanti valori universali. I crimini di guerra, ad esempio, costituiscono gravi violazioni del diritto umanitario internazionale. Il CICR menziona inoltre che sono da tenere in considerazione fattori analoghi a quelli indicati dal manuale per l'uso della posizione comune 2008/944/PESC, tra cui gli impegni formali ad applicare le norme del diritto umanitario internazionale, misure adeguate che garantiscano l'assunzione di responsabilità per le violazioni del diritto umanitario internazionale, una formazione in ambito di diritto umanitario internazionale per i militari e il divieto di reclutare bambini nelle forze armate.

2. **AMBITO DI APPLICAZIONE TECNICO**

2.1. **Prodotti di sorveglianza informatica compresi negli elenchi**

L'appendice dei presenti orientamenti contiene informazioni sui prodotti di sorveglianza informatica compresi negli elenchi di cui all'allegato I del regolamento volte ad aiutare gli esportatori nell'identificazione di potenziali prodotti di sorveglianza informatica non compresi negli elenchi.

2.2. **Potenziali prodotti di sorveglianza informatica non compresi negli elenchi**

Sebbene sia per definizione impossibile fornire un elenco esaustivo dei prodotti che possono essere sottoposti a controllo in quanto «prodotti non compresi negli elenchi» ai sensi dell'articolo 5, i prodotti descritti di seguito potrebbero essere oggetto di sorveglianza e giustificare una particolare vigilanza ai sensi del regolamento.

Come chiarito al considerando 8 del regolamento, i prodotti utilizzati per applicazioni puramente commerciali come la fatturazione, il marketing, i servizi di qualità, la soddisfazione degli utenti o la sicurezza della rete sono generalmente considerati esenti da rischi di uso improprio rilevanti in relazione a gravi violazioni dei diritti umani o del diritto umanitario internazionale, per cui non sono generalmente soggetti al controllo di cui all'articolo 5. Molti di questi prodotti hanno funzionalità di sicurezza dell'informazione (crittografiche o anche crittoanalitiche) che rientrano nei parametri relativi ai controlli di cui alla categoria 5, parte 2, del testo descrittivo dei controlli all'allegato I del regolamento. Non rientrano nella definizione di «prodotti di sorveglianza informatica» neppure le apparecchiature di rete per la sicurezza, compresi router, interruttori, gateway o relè, se le funzioni di «sicurezza dell'informazione» sono limitate ai compiti «OAM» («operazioni, amministrazione o manutenzione») che applicano solamente standard crittografici pubblicati o commerciali, anche se gli esportatori dovrebbero rimanere vigili in considerazione di varie segnalazioni di un uso improprio di tali prodotti per violazioni dei diritti umani.

2.2.1. *Tecnologia di riconoscimento facciale e delle emozioni*

Le tecnologie di riconoscimento facciale e delle emozioni hanno molteplici usi al di là della sorveglianza informatica – ad esempio sono utilizzate a fini di identificazione o autenticazione – e non rientrerebbero automaticamente nella definizione. In determinate circostanze, tuttavia, tali tecnologie possono essere comprese nell'ambito di applicazione dell'articolo 2, punto 20), del regolamento.

Potrebbero rientrare nella definizione di prodotto di sorveglianza informatica le tecnologie di riconoscimento facciale e delle emozioni che possono essere usate per monitorare o analizzare immagini video memorizzate. Anche qualora siano soddisfatti i criteri di cui sopra, è comunque necessario valutare attentamente se il software sia stato appositamente progettato per la sorveglianza dissimulata.

2.2.2. *Dispositivi di localizzazione*

I dispositivi di localizzazione consentono di tracciare l'ubicazione fisica di un dispositivo nel tempo; le autorità di contrasto e le agenzie di intelligence utilizzano alcune tecnologie di localizzazione già da tempo. Il loro potenziale a fini di sorveglianza mirata e di massa si è notevolmente evoluto con l'ulteriore sviluppo delle tecnologie di tracciamento – tra cui il tracciamento della localizzazione tramite satellite o tramite torri cellulari, i ricetrasmettitori Wi-Fi e Bluetooth – e con l'ampia diffusione dei «dispositivi di tracciamento» quali gli smartphone e altri dispositivi elettronici (come i sistemi di bordo delle automobili).

Le autorità di contrasto e le agenzie di intelligence utilizzano i dispositivi di localizzazione ad esempio per raccogliere prove nel corso di un'indagine o per rintracciare gli indagati; anche le imprese li utilizzano, a fini commerciali, ad esempio per ottenere dati sui modelli di spostamento aggregati nelle strade commerciali, seguire i dipendenti che lavorano fuori sede o per la pubblicità geolocalizzata.

2.2.3. *Sistemi di videosorveglianza*

Al fine di aiutare gli esportatori a individuare potenziali casi di sorveglianza informatica, è utile chiarire anche quali prodotti non rientrerebbero nella definizione. In questo senso, ad esempio, i sistemi e le telecamere di videosorveglianza, comprese le videocamere ad alta risoluzione, utilizzati per la ripresa di persone negli spazi pubblici non rientrano nella definizione di prodotti di sorveglianza informatica, in quanto non monitorano né raccolgono dati provenienti da sistemi di informazione e telecomunicazione.

3. **MISURE DI DOVUTA DILIGENZA**

Ai sensi del considerando 7 del regolamento, «[i]l contributo degli esportatori […] all'obiettivo generale dei controlli sugli scambi è fondamentale. Affinché essi possano agire in conformità del presente regolamento, la valutazione dei rischi connessi alle operazioni oggetto del presente regolamento deve essere eseguita mediante misure di controllo delle operazioni, note anche come principio della dovuta diligenza, nell'ambito di un programma interno di conformità (Internal Compliance Programme — ICP)».

L'articolo 2, punto 21), definisce un «programma interno di conformità» o «ICP» come «politiche e procedure efficaci, adeguate e proporzionate in corso adottate dagli esportatori al fine di facilitare la conformità alle disposizioni e agli obiettivi del presente regolamento nonché ai termini e alle condizioni delle autorizzazioni attuate a norma del presente regolamento, comprese, tra l'altro, misure di dovuta diligenza per valutare i rischi connessi all'esportazione dei prodotti per gli utenti finali e gli usi finali».

La raccomandazione (UE) 2019/1318 della Commissione ([7]) fornisce un quadro di riferimento per aiutare gli esportatori a individuare, gestire e attenuare i rischi associati al controllo del commercio dei prodotti a duplice uso nonché garantire il rispetto delle pertinenti disposizioni legislative e regolamentari dell'Unione e nazionali.

I presenti orientamenti possono sostenere gli esportatori nell'attuazione di misure di controllo delle operazioni, note anche come principio della dovuta diligenza, nell'ambito di un ICP.

A norma dell'articolo 5, paragrafo 2, del regolamento (UE) 2021/821, gli esportatori di prodotti di sorveglianza informatica non compresi negli elenchi sono tenuti ad esercitare la dovuta diligenza mediante misure di controllo delle operazioni, ossia adottando misure per la classificazione dei prodotti e la valutazione del rischio dell'operazione. Nella pratica, gli esportatori sono incoraggiati a esaminare i punti descritti di seguito.

([7]) Raccomandazione (UE) 2019/1318 della Commissione, del 30 luglio 2019, sui programmi interni di conformità relativi ai controlli del commercio dei prodotti a duplice uso ai sensi del regolamento (CE) n. 428/2009 (GU L 205 del 5.8.2019, pag. 15, ELI: http://data.europa.eu/eli/reco/2019/1318/oj).

3.1. **Valutare se il prodotto da esportare non compreso negli elenchi possa costituire un «prodotto di sorveglianza informatica», ossia un prodotto appositamente progettato per consentire la sorveglianza dissimulata di persone fisiche mediante il monitoraggio, l'estrazione, la raccolta o l'analisi di dati provenienti da sistemi di informazione e telecomunicazione.**

Questa fase consiste nel determinare la natura del prodotto in base alle disposizioni applicabili ai prodotti di sorveglianza informatica. Prevede un esame delle caratteristiche tecniche dei prodotti basata, da una parte, sui parametri tecnici di cui all'allegato I del regolamento per i prodotti compresi negli elenchi e, dall'altra, sui termini e sui concetti specifici della definizione di prodotti di sorveglianza informatica per i prodotti non compresi negli elenchi, alla luce della conseguente classificazione del prodotto (beni, tecnologia o software).

3.2. **Esaminare le capacità del prodotto in questione per determinare il potenziale uso improprio connesso alla repressione interna e/o all'attuazione di gravi violazioni dei diritti umani o del diritto umanitario internazionale da parte di utenti finali stranieri.**

Gli esportatori dovrebbero effettuare una valutazione volta a stabilire se il prodotto possa essere utilizzato impropriamente per attuare una repressione interna o violazioni o abusi dei diritti umani, compresi il diritto alla vita, la libertà dalla tortura, da trattamenti inumani e degradanti, il diritto alla vita privata, il diritto alla libertà di espressione, il diritto di associazione e di riunione, il diritto alla libertà di pensiero, di coscienza e di religione, il diritto alla parità di trattamento, o il divieto di discriminazione, o il diritto a elezioni libere, eque e a scrutinio segreto.

Questa fase comprende inoltre una valutazione volta a determinare se il prodotto possa essere utilizzato come parte o componente di un sistema in grado di dare luogo a dette violazioni e/o detto uso improprio.

Nella loro valutazione gli esportatori dovrebbero utilizzare indicatori di rischio («red flags») che segnalano eventuali circostanze anomale di un'operazione e indicano che l'esportazione può essere destinata a un uso finale, a un utente finale o a una destinazione inadeguati.

Indicatori di rischio:

a) il prodotto è commercializzato con informazioni relative a un suo potenziale uso a fini di sorveglianza dissimulata;

b) informazioni da cui risulti che un prodotto simile è stato utilizzato impropriamente in connessione alla repressione interna e/o all'attuazione di gravi violazioni dei diritti umani o del diritto umanitario internazionale (cfr. sezione 1.3);

c) informazioni da cui risulti che il prodotto è stato utilizzato illecitamente nel quadro di attività di sorveglianza dirette contro uno Stato membro, o in relazione alla sorveglianza illecita di un cittadino dell'UE;

d) informazioni da cui risulti che l'operazione comprende prodotti che potrebbero essere utilizzati per realizzare, personalizzare o configurare un sistema notoriamente utilizzato in modo improprio in connessione alla repressione interna e/o all'attuazione di gravi violazioni dei diritti umani o del diritto umanitario internazionale (cfr. sezione 1.3);

e) il prodotto, o un prodotto analogo, figura nell'elenco pubblicato nella serie C della *Gazzetta ufficiale dell'Unione europea* a norma dell'articolo 5, paragrafo 6, del regolamento.

3.3. **Esaminare, a sostegno delle autorità competenti, i portatori di interessi coinvolti nell'operazione (compresi gli utenti finali e i destinatari quali i distributori e i rivenditori).**

Nella misura del possibile, a sostegno delle autorità competenti, gli esportatori dovrebbero:

a) prima e nel corso di qualsiasi operazione, esaminare in che modo i destinatari e/o gli utenti finali intendano usare il prodotto o il servizio, sulla base delle dichiarazioni relative all'uso finale;

b) familiarizzarsi con il contesto della destinazione dei prodotti, in particolare per quanto riguarda la condizione generale dei diritti umani, in quanto si tratta di un importante indicatore del rischio di gravi violazioni dei diritti umani o del diritto umanitario internazionale connesse all'esportazione;

c) valutare, sulla base degli indicatori di rischio elencati di seguito, il rischio che il prodotto o il servizio sia dirottato verso un utente finale diverso non autorizzato.

Indicatori di rischio:

a) l'utente finale intrattiene una relazione palese con un governo straniero che ha antecedenti di atti di repressione interna e/o gravi violazioni dei diritti umani o del diritto umanitario internazionale;

b) l'utente finale è strutturalmente inquadrato nelle forze armate o in un altro gruppo coinvolto in un conflitto armato che in passato ha registrato misure di repressione interna e/o gravi violazioni dei diritti umani o del diritto umanitario internazionale;

c) in passato l'utente finale ha esportato prodotti di sorveglianza informatica in paesi in cui l'uso di tali prodotti ha dato luogo a misure di repressione interna e/o a gravi violazioni dei diritti umani o del diritto umanitario internazionale.

3.4. **Usare i risultati della dovuta diligenza per elaborare piani volti a prevenire e attenuare potenziali impatti negativi futuri.**

Gli esportatori dovrebbero, sulla base dei risultati della dovuta diligenza, porre termine ad attività che causano, o contribuiscono a causare, impatti negativi in relazione ai diritti umani, ed elaborare e attuare un piano di azioni correttive. Tali azioni possono comprendere quanto segue:

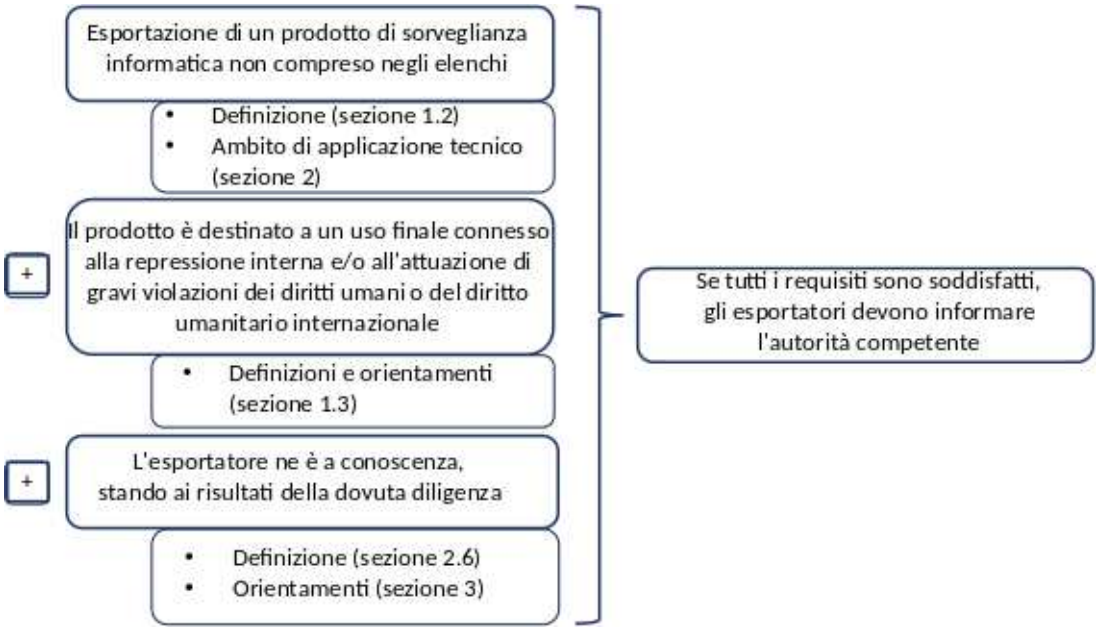
a) aggiornare le politiche dell'impresa al fine di includervi orientamenti su come evitare e affrontare gli impatti negativi in futuro, e far sì che tali orientamenti siano applicati;

b) attingere ai risultati della valutazione del rischio per aggiornare e rafforzare i sistemi di gestione, al fine di monitorare meglio le informazioni e individuare i rischi prima del verificarsi di impatti negativi;

c) raccogliere informazioni che permettano di comprendere i rischi elevati di impatti negativi connessi al settore;

d) informare le autorità competenti degli Stati membri dei risultati della dovuta diligenza per agevolare il flusso delle informazioni relative a determinati prodotti, utenti finali e destinazioni.

Requisiti di cui all'articolo 5, paragrafo 2, del regolamento (UE) 2021/821



4. **APPENDICE**

Prodotti di sorveglianza informatica compresi negli elenchi in quanto sottoposti a controllo a norma dell'allegato I del regolamento (UE) 2021/821

— **Sistemi di intercettazione delle telecomunicazioni (5A001.f.)**

Nella maggior parte dei paesi, compresi gli Stati membri, la riservatezza delle comunicazioni è tutelata dalla legge, ma la sorveglianza elettronica dissimulata delle comunicazioni da parte delle autorità governative (la cosiddetta «intercettazione legale») può essere autorizzata nell'ambito di un quadro giuridico. L'era digitale ha però introdotto la possibilità di utilizzare tecnologie di intercettazione su larga scala. L'uso di strumenti di intercettazione da parte del regime libico ha messo in luce le potenzialità di un utilizzo di queste tecnologie su larga scala e incoraggiato l'introduzione di controlli sulle esportazioni di sistemi di intercettazione delle telecomunicazioni nel 2012.

Questo controllo si applica alle apparecchiature progettate per l'estrazione del contenuto di una comunicazione (voce o dati), degli identificativi degli abbonati o di altri metadati trasmessi via interfaccia aerea mediante comunicazione senza fili, così come alle apparecchiature di monitoraggio a radiofrequenza. Si applica, ad esempio, agli IMSI catcher (*International Mobile Subscriber Identity*, identità utente mobile internazionale) che intercettano il traffico dei telefoni cellulari e tracciano lo spostamento dei relativi utenti, o alle apparecchiature che creano falsi hotspot Wi-Fi in grado di estrarre numeri IMSI da un telefono, come pure a determinati tipi di prodotti appositamente progettati per consentire l'«ispezione approfondita di pacchetti» nei sistemi di telecomunicazioni. Le apparecchiature di disturbo delle telecomunicazioni mobili non rientrano nell'ambito di applicazione dei prodotti di sorveglianza informatica in quanto non raccolgono dati.

Benché per costruire sistemi di questo tipo possa essere utilizzata tecnologia di uso generale, le capacità di intercettazione su larga scala di tali sistemi si baseranno su parti e componenti specifici, tra cui software specifico, circuiti integrati avanzati o per un'applicazione specifica (FPGA, ASIC ecc.) per aumentare il numero di pacchetti o di sessioni di comunicazione che possono essere elaborati al secondo.

— **Sistemi di sorveglianza su Internet (5A001.j.)**

Sebbene molte delle comunicazioni basate su Internet siano oggi generalmente criptate per impostazione predefinita, l'intercettazione dei dati sul traffico (metadati) relativi alle comunicazioni – come gli indirizzi IP e la frequenza e le dimensioni dello scambio di dati – può ancora essere utilizzata per individuare collegamenti tra persone e nomi di dominio. I governi possono sfruttare questi sistemi in modo lecito e sotto controllo giudiziario per finalità legittime, quali l'identificazione di soggetti che visitano domini associati a contenuti criminali o terroristici. Il monitoraggio e l'analisi del traffico Internet sulla base della caratterizzazione etnica, religiosa, politica o sociale possono invece portare a una mappatura umana e sociale completa di un paese a scopo di controllo e di repressione della popolazione e per altri fini, come l'individuazione di dissidenti politici. Oltre che alle questioni relative ai diritti umani e alla repressione interna, questi prodotti possono contribuire anche al rafforzamento delle capacità di sicurezza e militari.

Il controllo di cui alla voce 5A001.j. si applica ai sistemi di controllo su Internet che operano su una «rete IP carrier class (ad esempio dorsale IP di livello nazionale)» per eseguire analisi, estrazioni e l'indicizzazione di contenuti di metadati trasmessi (voce, video, messaggi, allegati) sulla base di «criteri restrittivi» e mappare la rete di rapporti delle persone. Questi sono prodotti che effettuano una «sorveglianza dissimulata» perché le persone che ne sono oggetto non sono consapevoli dell'intercettazione delle comunicazioni. Per contro, i controlli non concernono i sistemi in cui esiste un'azione o un'interazione con un utente o un abbonato, e non si applicano ad esempio ai social network o ai motori di ricerca commerciali. Inoltre, i controlli si applicano ai sistemi che trattano dati provenienti da una rete centrale di un fornitore di Internet, ma non ai social network o ai motori di ricerca commerciali che trattano dati forniti dagli utenti.

— **«Software di intrusione» (4A005, 4D004 e controlli correlati di cui alle voci 4E001.a. e 4E001.c.)**

Il software di intrusione consente all'operatore di ottenere in modo dissimulato un accesso remoto a un dispositivo elettronico, come uno smartphone, un computer portatile, un server o un dispositivo dell'Internet delle cose, ottenere dati memorizzati sul dispositivo, spiare attraverso una videocamera o un microfono integrati nel dispositivo o ad esso collegati e utilizzare il dispositivo come punto di partenza per effettuare attacchi su apparecchiature cui il dispositivo si collega o contro i contatti dell'utente («pirateria informatica tramite dispositivi di terzi»). Benché i software di intrusione possano essere utilizzati anche per scopi legittimi ([8]), ad esempio il «software per l'accesso remoto» che i servizi informatici utilizzano per il supporto a distanza, il carattere dissimulato della sorveglianza e la portata delle informazioni che questa può permettere di raccogliere presentano un elevato rischio di violazione del diritto alla vita privata e alla protezione dei dati personali e possono compromettere gravemente il diritto alla libertà di espressione.

([8]) Va chiarito che i prodotti di sorveglianza informatica compresi negli elenchi di cui all'allegato I del regolamento sui prodotti a duplice uso in quanto sottoposti a controllo necessiterebbero di un'autorizzazione per essere esportati in paesi terzi indipendentemente dal fatto che siano utilizzati a fini legittimi o no.

Il controllo di cui alla voce 4A005 e altre si applica a software, sistemi, apparecchiature, componenti e relative tecnologie, appositamente progettati o modificati per la generazione, il comando e il controllo, o la consegna di «software di intrusione», ma non al «software di intrusione» in sé, quale definito nell'allegato I del regolamento. Questi strumenti informatici sono sottoposti a controllo per via delle perturbazioni e dei danni potenziali che possono causare se utilizzati ed eseguiti con successo, ma i controlli non sono destinati a incidere sull'attività, ad esempio, dei ricercatori e dell'industria del settore della cibersicurezza, che hanno bisogno di condividere informazioni relative al software di intrusione per poter elaborare soluzioni per i loro prodotti e renderle disponibili prima che sia divulgata pubblicamente una vulnerabilità.

— **Software per il monitoraggio delle comunicazioni (5D001.e.)**

Questo software è progettato per il monitoraggio e l'analisi, da parte delle autorità di contrasto autorizzate, di dati raccolti attraverso misure di intercettazione mirate richieste a un fornitore di servizi di comunicazione. Il software in questione consente di condurre ricerche sulla base di «criteri restrittivi» dei contenuti delle comunicazioni o dei metadati attraverso un'interfaccia di intercettazione legale ed effettuare la mappatura della rete di rapporti o il tracciamento dei movimenti di specifici individui in base ai risultati delle ricerche. Si tratta di un software destinato alla «sorveglianza dissimulata» in quanto utilizza i dati raccolti dall'intercettazione delle comunicazioni senza che gli interessati ne siano consapevoli. Il software «analizza» inoltre i dati raccolti attraverso «sistemi di telecomunicazione». Il software è installato presso l'autorità governativa (ad esempio la sezione di monitoraggio delle autorità di contrasto, *Law enforcement monitoring facility* - «LEMF») e il controllo non si applica ai sistemi di controllo della conformità dell'intercettazione legale (ad esempio i sistemi di gestione dell'intercettazione legale e i dispositivi di mediazione) che sono sviluppati commercialmente e installati nello spazio del fornitore di servizi di comunicazione (ad esempio integrati nella rete di comunicazione) e che il fornitore di servizi gestisce e mantiene. Come chiarito nel testo descrittivo del controllo, non è sottoposto a controllo il «software» appositamente progettato o modificato per fini puramente commerciali quali la fatturazione, la rete di qualità del servizio (QoS), la qualità dell'esperienza (QoE), i dispositivi di mediazione o il pagamento mobile o l'uso bancario.

— **Prodotti utilizzati per effettuare la crittoanalisi (5A004.a.)**

Questo controllo si applica ai prodotti progettati al fine di neutralizzare i meccanismi crittografici per ricavarne le variabili confidenziali o i dati riservati, compresi il testo in chiaro, le parole d'ordine o le chiavi crittografiche. La crittografia serve a salvaguardare la riservatezza delle informazioni in transito e a riposo. La crittoanalisi viene usata per neutralizzare tale riservatezza, e di conseguenza questa tecnologia «consente» la sorveglianza dissimulata mediante il monitoraggio, l'estrazione, la raccolta o l'analisi di dati provenienti da sistemi di informazione e telecomunicazione.

— **Strumenti forensi/investigativi (5A004.b., 5D002.a.3.b. e 5D002.c.3.b.)**

Gli strumenti forensi/investigativi sono progettati per estrarre dati grezzi da un dispositivo (ad esempio informatico o di comunicazione) per evitare che siano manomessi o corrotti e fare in modo che possano essere utilizzati a fini giudiziari, ossia nel quadro di un'indagine penale o dinanzi a un organo giurisdizionale. Questi prodotti eludono l'«autenticazione» o i controlli di autorizzazione di un dispositivo al fine di poter estrarne i dati grezzi. Si tratta di prodotti utilizzati dal governo e dalle autorità di contrasto, ma anche dalle forze militari per estrarre e analizzare dati provenienti da dispositivi sequestrati. Pur avendo un uso legittimo, possono però essere utilizzati impropriamente e comportare quindi un rischio per i dati sensibili o commerciali.

Gli strumenti forensi/investigativi che non sono «appositamente progettati» per la sorveglianza dissimulata non rientrano invece nella definizione di prodotti di sorveglianza informatica di cui all'articolo 2, punto 20). Nemmeno gli strumenti forensi/investigativi che estraggono solo i dati dell'utente o i dati che non sono protetti sul dispositivo rientrano nel testo descrittivo del controllo di cui alla voce 5A004.b. e altre. I controlli non si applicano neppure alle apparecchiature di produzione o di prova dei fabbricanti, agli strumenti per amministratori di sistema o ai prodotti destinati esclusivamente al settore della vendita al dettaglio, ad esempio i prodotti per sbloccare i telefoni cellulari. Pertanto, considerata la varietà di questi tipi di tecnologia, l'applicazione dei controlli dipende da una valutazione caso per caso di ciascun prodotto.

Si noti infine che negli elenchi di cui all'allegato I del regolamento sono compresi altri prodotti collegati alla sorveglianza che non dovrebbero considerarsi ricompresi nella definizione di prodotti di sorveglianza informatica, quali le apparecchiature di disturbo delle telecomunicazioni mobili (5A001.f.) progettate per danneggiare o perturbare le comunicazioni o i sistemi, il software di intrusione che apporta modifiche a un sistema (4D004) e le apparecchiature laser per la rilevazione acustica (6A005.g.) che raccolgono dati audio con un laser o che consentono di ascoltare conversazioni a distanza (talvolta conosciute come «microfono laser»). Analogamente, l'uso degli UAV compresi negli elenchi a fini di sorveglianza non farebbe rientrare tali prodotti nella definizione di prodotti di sorveglianza informatica.