2024/2659

16.10.2024

RECOMANDAREA (UE) 2024/2659 A COMISIEI

din 11 octombrie 2024

privind orientările referitoare la exportul produselor de supraveghere cibernetică în temeiul articolului 5 din Regulamentul (UE) 2021/821 al Parlamentului European și al Consiliului

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 292,

întrucât:

(1) Regulamentul (UE) 2021/821 al Parlamentului European și al Consiliului [1] instituie un regim al Uniunii pentru controlul exporturilor, serviciilor de intermediere, asistenței tehnice, tranzitului și transferului de produse cu dublă utilizare.

(2) Regulamentul (UE) 2021/821 abordează riscul ca produsele de supraveghere cibernetică să fie utilizate în legătură cu represiunea internă și/sau cu comiterea de încălcări flagrante ale drepturilor omului și ale dreptului internațional umanitar.

(3) În temeiul articolului 5 alineatul (2) și al articolului 26 alineatul (1) din Regulamentul (UE) 2021/821, Comisia și Consiliul pun la dispoziție orientări pentru exportatori cu privire la produsele de supraveghere cibernetică neincluse pe listă, având în vedere necesitatea de a asigura eficiența regimului de control al exporturilor din Uniune în ceea ce privește securitatea cibernetică și implementarea consecventă a Regulamentului (UE) 2021/821.

(4) Prezenta recomandare și orientările anexate la aceasta au ca scop să sprijine exportatorii în aplicarea controalelor privind produsele de supraveghere cibernetică neincluse pe listă, inclusiv, printre altele, măsurile de diligență necesară care evaluează riscurile legate de exportul unor astfel de produse.

(5) Orientările anexate la prezenta recomandare au făcut obiectul unor consultări ample în cadrul Grupului de experți privind tehnologia de supraveghere, în 2022 și 2023, și au luat în considerare observațiile primite în cursul unei consultări publice [2] desfășurate în al doilea trimestru al anului 2023.

(6) Ar trebui reamintit faptul că prezenta recomandare și orientările anexate nu au caracter obligatoriu. Prin urmare, exportatorilor le revine în continuare responsabilitatea de a-și respecta obligațiile în temeiul Regulamentului (UE) 2021/821, iar Comisia ar trebui să se asigure că prezenta recomandare rămâne relevantă în timp,

[1] Regulamentul (UE) 2021/821 al Parlamentului European și al Consiliului din 20 mai 2021 de instituire a unui regim al Uniunii pentru controlul exporturilor, serviciilor de intermediere, asistenței tehnice, tranzitului și transferului de produse cu dublă utilizare (JO L 206, 11.6.2021, p. 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.

ADOPTĂ PREZENTA RECOMANDARE:

Se recomandă ca autoritățile competente și exportatorii din statele membre să țină seama de orientările prevăzute în anexa la prezenta recomandare pentru a-și îndeplini obligațiile în temeiul articolului 5 alineatul (2) din Regulamentul (UE) 2021/821.

Adoptată la Bruxelles, 11 octombrie 2024.

Pentru Comisie
Valdis DOMBROVSKIS
Vicepreședinte executiv

ANEXĂ

CUPRINS

Pagina

Introducere 4

1. Dispoziții juridice, definiții și concepte-cheie relevante 4

1.1. Prezentare generală a dispozițiilor juridice relevante 4

1.2. Definiții-cheie 5

1.2.1. „Special concepute” 5

1.2.2. „Supraveghere sub acoperire” 6

1.2.3. „Persoane fizice” 6

1.2.4. „Monitorizarea, extragerea, colectarea, analizarea datelor” 6

1.2.5. „Din sistemele informatice și de telecomunicații” 7

1.2.6. „Are cunoștință” și „sunt destinate” 7

1.3. Represiunea internă, încălcări flagrante ale drepturilor omului și ale dreptului internațional umanitar 7

1.3.1. Represiunea internă 8

1.3.2. Comiterea de încălcări flagrante ale drepturilor omului 8

1.3.3. Comiterea de încălcări flagrante ale dreptului internațional umanitar 9

2. Domeniul tehnic de aplicare 9

2.1. Produse de supraveghere cibernetică incluse pe listă 9

2.2. Produse de supraveghere cibernetică potențială neincluse pe listă 9

2.2.1. Tehnologia de recunoaștere facială și emoțională 10

2.2.2. Dispozitive de localizare și urmărire 10

2.2.3. Sisteme de supraveghere video 10

3. Măsuri de diligență necesară 10

Cerințe prevăzute la articolul 5 alineatul (2) din Regulamentul (UE) 2021/821 12

4. Apendice 12

Produse de supraveghere cibernetică incluse pe listă care fac obiectul controlului în temeiul anexei I la Regulamentul (UE) 2021/821 12

Sisteme de interceptare a telecomunicațiilor (5A001.f.) 12

Sisteme de supraveghere a internetului (5A001.j.) 13

„Produse software de intruziune” (4A005, 4D004 și sisteme de control conexe în temeiul 4E001.a. și 4E001.c.) 13

Produse software de monitorizare a comunicațiilor (5D001.e.) 14

Produse utilizate pentru efectuarea criptanalizei (5A004.a.) 14

Instrumente criminalistice/de investigare (5A004.b., 5D002.a.3.b. și 5D002.c.3.b.) 14

INTRODUCERE

Cadrul Uniunii de control al exporturilor instituit prin Regulamentul (UE) 2021/821 (denumit în continuare „regulamentul") urmărește să asigure respectarea obligațiilor și angajamentelor internaționale ale Uniunii și ale statelor sale membre, inclusiv în ceea ce privește pacea, securitatea și stabilitatea regională, precum și respectarea drepturilor omului și a dreptului internațional umanitar. Prin urmare, Uniunea și statele sale membre au pus în aplicare deciziile luate în cadrul regimurilor multilaterale de control al exporturilor și au actualizat în consecință lista de control a Uniunii în anexa I la regulament ([1]). În plus, înainte de intrarea în vigoare a articolului 5 din regulament, autoritățile competente din statele membre controlaseră deja exportul anumitor produse incluse pe listă care pot avea aplicații de supraveghere ([2]), luând în considerare riscurile de utilizare abuzivă în anumite circumstanțe specifice. În cazul unor circumstanțe extrem de grave, Uniunea a impus sancțiuni care restricționează exportul anumitor echipamente de supraveghere ([3]).

Regulamentul reflectă angajamentul Uniunii de a aborda în mod eficace riscul ca produsele de supraveghere cibernetică să fie utilizate în legătură cu represiunea internă și/sau cu comiterea de încălcări flagrante ale drepturilor omului și ale dreptului internațional umanitar. În special, regulamentul introduce noi dispoziții privind controlul exportului produselor de supraveghere cibernetică neincluse pe listă, inclusiv obligația exportatorilor de a notifica autoritatea competentă atunci când au cunoștință, în conformitate cu constatările lor rezultate din îndeplinirea obligației de diligență, că produsele de supraveghere cibernetică neincluse pe listă pe care exportatorii propun să le exporte sunt destinate, integral sau parțial, utilizării în legătură cu represiunea internă și/sau comiterea unor încălcări flagrante ale drepturilor omului și ale dreptului internațional umanitar. Regulamentul invită, de asemenea, Comisia și Consiliul să pună la dispoziția exportatorilor orientări pentru a sprijini punerea în aplicare eficace a noilor controale pentru produsele de supraveghere cibernetică care nu sunt incluse pe listă.

Prin urmare, prezentele orientări vizează sprijinirea exportatorilor în ceea ce privește aplicarea controalelor cu privire la produsele de supraveghere cibernetică neincluse pe listă, inclusiv, printre altele, măsurile de diligență necesară care evaluează riscurile legate de exportul unor astfel de produse către utilizatorii finali și utilizările finale în temeiul noilor dispoziții ale regulamentului.

1. DISPOZIȚII JURIDICE, DEFINIȚII ȘI CONCEPTE-CHEIE RELEVANTE

1.1. Prezentare generală a dispozițiilor juridice relevante

Regulamentul introduce noi dispoziții care prevăd în mod specific controlul exportului produselor de supraveghere cibernetică care nu sunt enumerate în anexa I la regulament și care sunt sau pot fi destinate, integral sau parțial, utilizării în legătură cu represiunea internă și/sau cu comiterea de încălcări flagrante ale drepturilor omului și ale dreptului internațional umanitar. Considerentele și articolele relevante sunt:

(a) considerentul 8: „Pentru a limita riscul ca anumite produse de supraveghere cibernetică neincluse pe listă exportate de pe teritoriul vamal al Uniunii să fie utilizate în mod abuziv de persoane complice sau responsabile de orchestrarea ori de comiterea unor încălcări grave ale drepturilor omului sau ale dreptului internațional umanitar, este oportun să se controleze exportul unor astfel de produse. Riscurile asociate se referă, în special, la cazurile în care produsele de supraveghere cibernetică sunt special concepute pentru a permite intruziunea sau inspectarea aprofundată a

([1]) A se vedea, în special, controalele referitoare la sistemele de interceptare a telecomunicațiilor (5A001.f), la sistemele de supraveghere a internetului (5A001.j.), la produsele software de intruziune (4A005, 4D004 și la controalele aferente prevăzute la 4E001.a și 4E001.c) și la produsele software de monitorizare a aplicării legii (5D001.e). A se vedea, de asemenea, pe baza unei evaluări de la caz la caz, controalele legate de anumite instrumente criminalistice/de investigare (5A004.b 5D002.a.3.b și 5D002.c.3.b).

([2]) În special sistemele de securitate a informațiilor.

([3]) A se vedea Regulamentul (CE) nr. 765/2006 al Consiliului din 18 mai 2006 privind măsuri restrictive având în vedere situația din Belarus și implicarea Belarusului în agresiunea Rusiei împotriva Ucrainei (JO L 134, 20.5.2006, p. 1, ELI: http://data.europa.eu/eli/reg/2006/765/oj); Regulamentul (UE) nr. 359/2011 al Consiliului din 12 aprilie 2011 privind măsuri restrictive împotriva anumitor persoane, entități și organisme având în vedere situația din Iran (JO L 100, 14.4.2011, p. 1, ELI: http://data.europa.eu/eli/reg/2011/359/oj); Regulamentul (UE) nr. 36/2012 al Consiliului din 18 ianuarie 2012 privind măsuri restrictive având în vedere situația din Siria și de abrogare a Regulamentului (UE) nr. 442/2011 (JO L 16, 19.1.2012, p. 1, ELI: http://data.europa.eu/eli/reg/2012/36/oj); Regulamentul (UE) nr. 401/2013 al Consiliului din 2 mai 2013 privind măsuri restrictive având în vedere situația din Myanmar/Birmania și de abrogare a Regulamentului (CE) nr. 194/2008 (JO L 121, 3.5.2013, p. 1, ELI: http://data.europa.eu/eli/reg/2013/401/oj); și Regulamentul (UE) 2017/2063 al Consiliului din 13 noiembrie 2017 privind măsuri restrictive având în vedere situația din Venezuela (JO L 295, 14.11.2017, p. 21, ELI: http://data.europa.eu/eli/reg/2017/2063/oj).

pachetelor în sistemele informatice și de telecomunicații pentru a efectua supravegherea sub acoperire a persoanelor fizice prin monitorizarea, extragerea, colectarea sau analizarea datelor, inclusiv a datelor biometrice, din respectivele sisteme. În general, se consideră că produsele utilizate exclusiv în scopuri comerciale, cum ar fi facturarea, comercializarea, serviciile de calitate, satisfacția utilizatorilor sau securitatea rețelei, nu implică astfel de riscuri.”;

(b) considerentul 9: „În vederea consolidării controlului eficace al exporturilor de produse de supraveghere cibernetică neincluse pe listă, este esențial să se armonizeze în continuare aplicarea procedurii «catch-all» în respectivul domeniu. În acest scop, statele membre se angajează să sprijine astfel de controale prin schimbul de informații între ele și cu Comisia, în special în ceea ce privește evoluțiile tehnologice ale produselor de supraveghere cibernetică și prin exercitarea vigilenței în aplicarea unor astfel de controale pentru a promova un schimb la nivelul Uniunii.”;

(c) articolul 2 punctul 20, care prevede o definiție a produselor de supraveghere cibernetică ca fiind „produse cu dublă utilizare special concepute pentru a permite supravegherea sub acoperire a persoanelor fizice prin monitorizarea, extragerea, colectarea sau analizarea datelor din sistemele informatice și de telecomunicații”;

(d) articolul 5, care introduce o cerință de autorizare pentru exportul de produse de supraveghere cibernetică care nu sunt incluse pe listă în cazul în care exportatorul a fost informat de către autoritatea competentă că produsele în cauză sunt sau pot fi destinate, integral sau parțial, unei utilizări legate de represiunea internă și/sau de comiterea unor încălcări flagrante ale drepturilor omului și ale dreptului internațional umanitar [articolul 5 alineatul (1)]. În plus, acesta impune exportatorilor obligația să notifice autoritatea competentă în cazul în care au cunoștință, conform constatărilor lor rezultate din îndeplinirea obligației de diligență, de faptul că produsele sunt destinate, integral sau parțial, utilizării în legătură cu represiunea internă și/sau cu comiterea unor încălcări flagrante ale drepturilor omului și ale dreptului internațional umanitar [articolul 5 alineatul (2)]. Autoritatea competentă respectivă decide cu privire la impunerea unei autorizații pentru exportul în cauză; și

(e) articolul 5 alineatul (2), care prevede, de asemenea, că „Comisia și Consiliul pun la dispoziție orientări pentru exportatori, astfel cum se menționează la articolul 26 alineatul (1).”

1.2. **Definiții-cheie**

Regulamentul conține considerente și dispoziții specifice care clarifică termenii specifici relevanți pentru controlul exportului produselor de supraveghere cibernetică neincluse pe listă și pe care este important ca exportatorii să le înțeleagă în mod clar pentru a efectua diligența necesară și a pune în aplicare controalele în mod eficace. O definiție de o importanță deosebită se regăsește la articolul 2 punctul 20, care include următoarea definiție precisă a „produselor de supraveghere cibernetică”: „produse cu dublă utilizare special concepute pentru a permite supravegherea sub acoperire a persoanelor fizice prin monitorizarea, extragerea, colectarea sau analizarea datelor din sistemele informatice și de telecomunicații”.

În sensul prezentelor orientări, ar trebui clarificate aspecte specifice ale definiției respective.

1.2.1. *„Special concepute”*

Un produs este conceput pentru supraveghere sub acoperire atunci când caracteristicile sale tehnice sunt adecvate pentru supravegherea sub acoperire a persoanelor fizice și o permit în mod obiectiv. Prin urmare, termenul „special concepute” înseamnă că supravegherea sub acoperire a persoanelor fizice trebuie să fi fost principalul scop al dezvoltării și conceperii produsului. Cu toate acestea, un astfel de termen nu prevede ca produsul să poată fi utilizat exclusiv pentru supravegherea sub acoperire a persoanelor fizice.

Astfel cum s-a clarificat în considerentul 8 din regulament, produsele utilizate pentru aplicații pur comerciale, cum ar fi facturarea, comercializarea, serviciile de calitate, satisfacția utilizatorilor sau securitatea rețelei, nu sunt special concepute pentru supravegherea sub acoperire a persoanelor fizice și, prin urmare, nu se încadrează în definiția produselor de supraveghere cibernetică. De exemplu, chiar dacă produsele pentru supravegherea sistemelor de operare din industrie sau pentru monitorizarea traficului utilizatorilor ar putea fi utilizate în scopuri de supraveghere, aceste produse nu sunt produse de supraveghere cibernetică conform definiției, deoarece nu sunt special concepute pentru a permite supravegherea sub acoperire a persoanelor fizice.

1.2.2. *„Supraveghere sub acoperire”*

Produsele permit supravegherea sub acoperire, în special în cazul în care supravegherea nu este în mod evident perceptibilă pentru persoana fizică afectată. Acest lucru ar fi valabil atunci când persoanele în cauză nu au cunoștință de prezența și/sau acțiunea produselor de supraveghere cibernetică și, prin urmare, nu au posibilitatea de a se sustrage de la supravegherea respectivă sau cel puțin de a-și adapta comportamentul în consecință. Chiar dacă supravegherea este efectuată prin intermediul unor produse instalate sau care funcționează în spațiul public, obținerea datelor poate fi considerată, în anumite cazuri, relevantă pentru supravegherea sub acoperire; în special, datele colectate pot fi deturnate, evaluate sau prelucrate în alte scopuri decât cele cu privire la care persoana fizică afectată este informată. Cu alte cuvinte, atunci când o persoană fizică nu se poate aștepta în mod obiectiv să se afle sub supraveghere, supravegherea poate fi considerată ca fiind sub acoperire, în conformitate cu articolul 2 punctul 20 din regulament.

1.2.3. *„Persoane fizice”*

Termenul „persoană fizică” se referă la o ființă umană vie prin opoziție față de o persoană juridică sau o entitate, care, prin urmare, nu face obiectul dispozițiilor. Termenul nu se referă la supravegherea obiectelor, a locurilor sau a mașinilor ca atare.

1.2.4. *„Monitorizarea, extragerea, colectarea, analizarea datelor”*

Potrivit Oxford English Dictionary, cuvintele „monitorizare, extragere, colectare și analiză” au următoarea semnificație lingvistică:

— „monitorizare”: observare; supraveghere, ascultare;

— „extragere”: a obține;

— „colectare”: a reuni, a strânge;

— „analiză”: a diferenția sau a determina elementele unui ansamblu (complex) pentru a determina structura sau natura acestuia și, prin urmare, pentru a explica sau a înțelege acest ansamblu; a examina îndeaproape și metodic în scopul interpretării; a supune unei analize critice sau computaționale.

Acești termeni implică faptul că elementele utilizate pentru supraveghere ar trebui să aibă capacități tehnice precise pentru prelucrarea datelor în vederea monitorizării, colectării, extragerii sau analizării datelor, cum ar fi, de exemplu, următoarele elemente:

(a) produse utilizate pentru monitorizarea datelor din sistemele informatice și de telecomunicații ([4]) (de exemplu, dimensiunea fișierelor sau traficul de pachete privind datele care sunt transmise în cadrul unui astfel de sistem);

(b) produse care extrag date din sistemele informatice și de telecomunicații prin efectuarea de intruziuni și extragere (de exemplu, software de intruziune);

(c) produse care permit o analiză a datelor extrase din sistemele informatice și de telecomunicații, inclusiv cele care pot prelucra imaginile camerei stocate în sistemele respective (de exemplu, anumite tipuri de tehnologii de analiză a datelor utilizate ca parte a sistemelor de recunoaștere facială).

Produsele utilizate pentru a monitoriza pur și simplu sistemele informatice sau pentru a urmări populația prin intermediul camerelor de supraveghere video și care permit captarea conversațiilor, a schimburilor de date, a deplasărilor și a comportamentelor individuale nu ar fi considerate produse de supraveghere cibernetică în sensul definiției din regulament, deoarece nu sunt special concepute în acest scop și trebuie să colaboreze cu alte tehnologii, cum ar fi inteligența artificială sau volumele mari de date. Cu toate acestea, întregul sistem (conlucrând cu alte tehnologii, cum ar fi inteligența artificială sau tehnologiile cu volume mari de date) ar putea fi un produs de supraveghere cibernetică în sensul definiției de la articolul 2 punctul 20 din regulament.

Este important de remarcat faptul că, deși oferă câteva exemple utile în scopuri ilustrative, definiția și domeniul de aplicare al produselor de supraveghere cibernetică nu sunt limitate de aceste exemple, deoarece obiectivul articolului 5 este de a permite un control eficace al exportului produselor care nu sunt incluse pe listă.

([4]) A se vedea punctul 1.2.5 de mai jos pentru definiție.

După cum reiese din utilizarea conjuncției „sau” în definiție, capacitățile tehnice enumerate trebuie considerate alternative și nu este necesar ca un produs să aibă toate aceste capacități tehnice pentru monitorizarea, extragerea, colectarea sau analizarea datelor. Cu alte cuvinte, este suficient ca un produs să aibă una dintre aceste capacități tehnice pentru a se încadra în definiția produsului de supraveghere cibernetică de la articolul 2 punctul 20.

1.2.5. *„Din sistemele informatice și de telecomunicații”*

Acești termeni se referă la sistemele care prelucrează electronic informații, de exemplu programare/codificare, operațiuni ale sistemelor PC (hardware) și alte servicii de administrare a informațiilor, inclusiv tehnologia software, tehnologia web, tehnologia de calcul, tehnologia de stocare etc., precum și la unele sisteme care transmit informații la distanță, de exemplu sistemele tehnice care transmit sunete, semnale, text, alte semne, imagini atât prin canale cu fir, cât și fără fir, prin fibre optice, radio și alte sisteme electromagnetice. Împreună, aceste două concepte includ o gamă largă de sisteme de transmitere sau prelucrare a informațiilor. Ar trebui remarcat faptul că sintagma se referă la sisteme și nu la echipamente.

1.2.6. *„Are cunoștință” și „sunt destinate”*

În temeiul articolului 5 alineatul (2) din regulament, un exportator informează autoritatea competentă în cazul în care acesta „are cunoștință […] de faptul că produsele de supraveghere cibernetică […] sunt destinate […] [unei utilizări legate de represiunea internă și/sau de comiterea unor încălcări flagrante ale drepturilor omului sau ale dreptului internațional umanitar]”.

Termenul „cunoștință” nu este un concept juridic nou, ci a fost utilizat în legătură cu cerințele de autorizare privind utilizarea finală (așa-numitele controale „catch-all”) în temeiul articolelor 4, 6, 7 și 8 din regulament. „A avea cunoștință” înseamnă că exportatorul are informații pozitive cu privire la utilizarea abuzivă avută în vedere. Simpla posibilitate a unui astfel de risc nu este suficientă pentru a stabili gradul de cunoștință. Cu toate acestea, termenul „cunoștință” nu poate fi asimilat pasivității: acesta presupune ca exportatorul să fi luat măsuri pentru a obține informații suficiente și adecvate pentru a evalua riscurile legate de export și pentru a asigura conformitatea cu regulamentul.

Indicația că produsele trebuie să fie „destinate” unei utilizări finale sensibile relevante presupune faptul că exportatorul ar trebui să evalueze utilizarea finală de la caz la caz, având în vedere circumstanțele specifice ale cazului respectiv. *A contrario*, un risc teoretic, și anume care nu se bazează pe o evaluare factuală a cazului, ca produsele să poată fi utilizate într-un mod care încalcă drepturile omului nu ar fi suficient pentru a presupune că acestea „sunt destinate” unei utilizări abuzive specifice în temeiul articolului 5.

1.3. **Represiunea internă, încălcări flagrante ale drepturilor omului și ale dreptului internațional umanitar**

În temeiul articolului 15 din regulament, care stabilește considerațiile pentru evaluarea unei autorizații, statele membre trebuie să ia în considerare toate considerațiile relevante, inclusiv cele care fac obiectul Poziției comune 2008/944/PESC a Consiliului ([5]).

Articolul 5 din regulament extinde controalele la exportul produselor de supraveghere cibernetică neincluse pe listă, având în vedere riscul ca acestea să fie utilizate în legătură cu represiunea internă și/sau cu comiterea unor încălcări flagrante ale drepturilor omului și ale dreptului internațional umanitar. Poziția comună 2008/944/PESC și ghidul de utilizare a acestei poziții comune ([6]) oferă orientări utile în acest sens.

([5]) Poziția comună 2008/944/PESC a Consiliului din 8 decembrie 2008 de definire a normelor comune care reglementează controlul exporturilor de tehnologie și echipament militar (JO L 335, 13.12.2008, p. 99, ELI: http://data.europa.eu/eli/compos/2008/944/oj).

([6]) A se vedea Ghidul de utilizare a Poziției comune 2008/944/PESC a Consiliului de definire a normelor comune care reglementează controlul exporturilor de tehnologie și echipament militar, https://www.consilium.europa.eu/media/40659/st12189-en19.pdf.

1.3.1. *Represiunea internă*

În temeiul articolului 2 alineatul (2) din Poziția comună 2008/944/PESC, „represiunile interne includ, printre altele, tortura și alte tratamente sau pedepse crude, inumane și degradante, execuții sumare sau arbitrare, dispariții, detenții arbitrare și alte încălcări majore ale drepturilor omului și libertăților fundamentale, astfel cum au fost stabilite de instrumentele internaționale relevante în domeniul drepturilor omului, inclusiv Declarația universală a drepturilor omului și Pactul internațional cu privire la drepturile civile și politice" (PIDCP). Ghidul de utilizare a Poziției comune 2008/944/PESC oferă orientări cu privire la elementele care trebuie luate în considerare în evaluarea exportatorului, inclusiv „antecedentele actuale și anterioare ale utilizatorului final propus în ceea ce privește respectarea drepturilor omului și ale țării beneficiare în general".

1.3.2. *Comiterea de încălcări flagrante ale drepturilor omului*

Utilizarea abuzivă a produselor de supraveghere cibernetică neincluse pe listă poate avea un impact negativ asupra unui spectru larg de drepturi ale omului și aduce atingere în mod direct dreptului la viață privată și la protecția datelor. Supravegherea arbitrară sau ilegală poate încălca, de asemenea, alte drepturi ale omului, cum ar fi dreptul la libertatea de exprimare, de asociere și de întrunire, libertatea de gândire, de conștiință și de religie, precum și dreptul la egalitate de tratament sau la interzicerea discriminării și dreptul la alegeri libere, egale și secrete. În cazuri speciale, supravegherea, inclusiv monitorizarea sau colectarea de informații ale persoanelor fizice, cum ar fi apărătorii drepturilor omului, activiștii, personalitățile politice, populațiile vulnerabile și jurnaliștii, poate duce la intimidare, reprimare, detenție arbitrară, tortură sau chiar la execuții extrajudiciare. Prin urmare, exportatorii ar trebui să includă în evaluările lor aceste aspecte legate de încălcări flagrante ale drepturilor omului.

Practica internațională arată că orice restricție privind drepturile omului trebuie să fie „adecvată" și în conformitate cu standardele internaționale privind drepturile omului. În practică, aceasta înseamnă că există garanții adecvate pentru a se asigura că restricțiile sunt prevăzute prin lege și pentru a menține esența drepturilor. Sub rezerva principiului proporționalității, pot fi impuse restricții numai dacă acestea sunt necesare și servesc efectiv unui scop legitim – de exemplu, siguranța națională sau publică, ordinea publică, protecția sănătății publice sau protecția drepturilor și libertăților celorlalți.

Produsele de supraveghere cibernetică pot include instrumente legitime și reglementate pentru aplicațiile de asigurare a aplicării legii, cum ar fi pentru prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor, inclusiv în domeniul combaterii terorismului sau al executării pedepselor în dreptul penal. În același timp, produsele de supraveghere cibernetică pot fi, de asemenea, utilizate în mod abuziv pentru a comite încălcări flagrante ale drepturilor omului și ale dreptului internațional umanitar atunci când sunt exportate către regimuri represive sau către utilizatori finali privați și/sau în zone de conflict.

Acest lucru necesită o evaluare de la caz la caz a circumstanțelor unui caz, inclusiv aplicarea reglementărilor relevante în lumina oricăror rapoarte privind încălcări flagrante ale drepturilor omului ale organismelor competente, de exemplu, Organizația Națiunilor Unite, Uniunea Europeană sau Consiliul Europei. Un indiciu privind „caracterul flagrant al" încălcărilor drepturilor omului poate fi găsit în recunoașterea acestor încălcări în informațiile publicate de organismele competente ale Organizației Națiunilor Unite, de Uniune sau de Consiliul Europei. Aceasta nu este o necesitate absolută pentru o astfel de recunoaștere explicită de către aceste organisme, ci este un factor important pentru îndeplinirea criteriilor.

În conformitate cu articolul 5, încălcarea drepturilor omului trebuie să fie „gravă". Orientări utile pentru clasificarea posibilelor încălcări ale drepturilor omului ca fiind „grave" pot fi găsite în Ghidul de utilizare a Poziției comune 2008/944/PESC. Potrivit acestui ghid, natura și consecințele încălcării sunt determinante. Încălcările sistematice și/sau larg răspândite ale drepturilor omului sunt considerate în mod regulat ca fiind grave; dar și încălcările care nu sunt sistematice sau larg răspândite pot fi considerate „grave" – de exemplu, din cauza gravității intervenției pentru persoanele afectate.

Anexa II la Ghidul de utilizare a Poziției comune 2008/944/PESC prevede o listă neexhaustivă a principalelor instrumente internaționale și regionale din domeniul drepturilor omului, inclusiv Convenția internațională cu privire la drepturile civile și politice (PIDCP), Convenția împotriva torturii și altor pedepse ori tratamente cu cruzime, inumane sau degradante, Convenția europeană a drepturilor omului (denumită în continuare „convenția") și Carta drepturilor fundamentale (Carta), care pot oferi orientări importante pentru interpretarea și aplicarea criteriilor în sprijinul unor evaluări solide ale drepturilor omului. Aceste instrumente, împreună cu protocoalele lor adiționale respective, constituie principalele norme și standarde internaționale în domeniul drepturilor omului și al libertăților fundamentale.

1.3.3. *Comiterea de încălcări flagrante ale dreptului internațional umanitar*

Dreptul internațional umanitar (denumit, de asemenea, „Convențiile de la Geneva” sau „Dreptul conflictelor armate”) a fost dezvoltat printr-o serie de tratate internaționale, în special prin Regulamentele de la Haga, Convențiile de la Geneva și cele două protocoale adiționale la acestea din 1977, și identifică norme care, în perioade de conflict armat, servesc la protejarea persoanelor care nu participă sau nu mai participă la ostilități (de exemplu, civili și combatanți răniți, bolnavi sau capturați) și impun părților beligerante limitări în ceea ce privește mijloacele și metodele de război („Convențiile de la Haga”).

Utilizarea produselor de supraveghere cibernetică neincluse pe listă ar trebui să respecte dreptul internațional umanitar atunci când acestea sunt utilizate ca mijloace și metode de război în contextul unui conflict armat. În astfel de circumstanțe, riscul unor încălcări flagrante ale dreptului internațional umanitar este luat în considerare în temeiul regulamentului și, în ceea ce privește comiterea unor încălcări flagrante ale drepturilor omului, ar trebui evaluat în funcție de destinația finală preconizată a produselor în cazul respectiv. Ghidul de utilizare a Poziției comune 2008/944/PESC oferă orientări cu privire la elementele care trebuie luate în considerare, inclusiv antecedentele trecute și actuale ale destinatarului în ceea ce privește respectarea dreptului internațional umanitar, intențiile destinatarului exprimate prin angajamente formale și capacitatea acestuia de a se asigura că echipamentele sau tehnologiile transferate sunt utilizate în conformitate cu dreptul internațional umanitar și nu sunt deturnate sau transferate către alte destinații în care ar putea fi utilizate pentru încălcări flagrante ale acestei legi.

În conformitate cu articolul 5, încălcarea dreptului internațional umanitar trebuie să fie „flagrantă”. Orientări pot fi găsite în Ghidul de utilizare a Poziției comune 2008/944/PESC, unde se recunoaște că „incidentele izolate de încălcări ale dreptului internațional umanitar nu indică neapărat atitudinea țării beneficiare față de dreptul internațional umanitar” și că „în cazul în care se poate identifica un anumit model de încălcări sau țara beneficiară nu a luat măsurile adecvate pentru a sancționa încălcările, acest lucru ar trebui să constituie un motiv serios de îngrijorare”. Comitetul Internațional al Crucii Roșii (CICR) a furnizat orientări cu privire la evaluarea încălcărilor dreptului internațional umanitar în scopul controlului exporturilor. Potrivit CICR, „încălcările dreptului internațional umanitar sunt flagrante dacă pun în pericol persoane protejate (de exemplu, civili, prizonieri de război, răniți și bolnavi) sau obiecte (de exemplu, obiecte sau infrastructuri civile) sau dacă încalcă valori universale importante”. Crimele de război, de exemplu, constituie încălcări flagrante ale dreptului internațional umanitar. CICR menționează, de asemenea, factori similari care trebuie considerați, cum ar fi Ghidul de utilizare a Poziției comune 2008/944/PESC, inclusiv angajamentele formale de a aplica normele dreptului internațional umanitar, măsurile adecvate de asigurare a tragerii la răspundere pentru încălcările dreptului internațional umanitar, formarea în domeniul dreptului internațional umanitar pentru personalul militar și interzicerea recrutării de copii pentru forțele armate.

2. **DOMENIUL TEHNIC DE APLICARE**

2.1. **Produse de supraveghere cibernetică incluse pe listă**

Apendicele la acest ghid oferă informații privind produsele de supraveghere cibernetică enumerate în anexa I la regulament, pentru a ajuta exportatorii să identifice produsele de supraveghere cibernetică potențiale care nu sunt incluse pe listă.

2.2. **Produse de supraveghere cibernetică potențială neincluse pe listă**

Deși, prin definiție, este imposibil să se furnizeze o listă exhaustivă a produselor care pot fi controlate ca „articole neincluse în listă” în temeiul articolului 5, următoarele articole ar putea avea un potențial de supraveghere și ar putea justifica o vigilență deosebită în temeiul regulamentului.

Astfel cum s-a clarificat în considerentul 8 din regulament, în general, se consideră că produsele utilizate exclusiv în scopuri comerciale, cum ar fi facturarea, comercializarea, serviciile de calitate, satisfacția utilizatorilor sau securitatea rețelei, nu implică riscuri de utilizare abuzivă, astfel cum sunt relevante în temeiul dispozițiilor privind încălcările flagrante ale drepturilor omului sau ale dreptului internațional umanitar și, prin urmare, nu fac, în general, obiectul controlului în temeiul articolului 5. Multe dintre aceste produse au funcționalități de securitate a informațiilor (criptografice sau chiar criptanalitice) care îndeplinesc parametrii de control din categoria 5 partea 2 din textul de control din anexa I la regulament. Echipamentele rețelelor de securitate – inclusiv routere, switchuri sau relee, în cazul cărora funcționalitatea de „securitate a informațiilor” se limitează la sarcinile legate de „operare, administrare sau întreținere” („OAM”) care utilizează numai standarde criptografice publicate sau comerciale – nu sunt incluse în definiția „produselor de supraveghere cibernetică”, deși exportatorii ar trebui să rămână vigilenți, având în vedere diferitele rapoarte privind utilizarea abuzivă a unor astfel de produse în contextul încălcării drepturilor omului.

2.2.1. *Tehnologia de recunoaștere facială și emoțională*

Tehnologiile de recunoaștere facială și emoțională au utilizări multiple, altele decât supravegherea cibernetică – de exemplu, pentru identificare sau autentificare – și nu s-ar încadra automat în definiție. Cu toate acestea, în anumite circumstanțe, tehnologiile de recunoaștere facială și emoțională pot intra sub incidența articolului 2 punctul 20 din regulament.

Tehnologiile de recunoaștere facială și emoțională care pot fi utilizate pentru monitorizarea sau analizarea imaginilor video stocate ar putea intra în domeniul de aplicare al definiției produsului de supraveghere cibernetică. Cu toate acestea, chiar dacă sunt îndeplinite criteriile menționate anterior, trebuie să se examineze cu atenție dacă produsul software este conceput special pentru supraveghere sub acoperire.

2.2.2. *Dispozitive de localizare și urmărire*

Dispozitivele de localizare permit urmărirea localizării fizice a unui dispozitiv de-a lungul timpului, iar unele tehnologii de localizare sunt utilizate de mai mult timp de către autoritățile de aplicare a legii și serviciile de informații. Potențialul lor de supraveghere țintită și în masă a evoluat considerabil, deoarece tehnologiile de urmărire au devenit mai avansate – inclusiv urmărirea localizării prin satelit, urmărirea localizării pe bază de antenă-releu, transceiver Wi-Fi și Bluetooth – și deoarece „dispozitivele de urmărire", cum ar fi telefoanele inteligente și alte dispozitive electronice (de exemplu, sistemele încorporate la bordul vehiculelor) au devenit larg răspândite.

Dispozitivele de localizare sunt utilizate de autoritățile de aplicare a legii și de serviciile de informații, de exemplu pentru a colecta probe în cursul unei investigații sau pentru a urmări suspecții, dar și de către societăți în scopuri comerciale, de exemplu raportarea cu privire la tiparele de mișcare agregate pe străzile comerciale, urmărirea angajaților care lucrează în afara amplasamentului sau pentru publicitatea bazată pe localizare.

2.2.3. *Sisteme de supraveghere video*

Pentru a-i ajuta pe exportatori să identifice o potențială supraveghere cibernetică, este, de asemenea, util să se clarifice ce produse nu ar fi acoperite de definiție. În acest sens, de exemplu, sistemele de supraveghere video și camerele de luat vederi – inclusiv camerele de înaltă rezoluție – utilizate pentru filmarea persoanelor în spațiile publice nu intră sub incidența definiției produselor de supraveghere cibernetică, deoarece nu monitorizează și nu colectează date din sistemele informatice și de telecomunicații.

3. MĂSURI DE DILIGENȚĂ NECESARĂ

Potrivit considerentului 7 al regulamentului, „contribuția exportatorilor […] la obiectivul general de control al comerțului este esențială. Pentru ca aceștia să poată acționa în conformitate cu prezentul regulament, evaluarea riscurilor legate de tranzacțiile vizate de prezentul regulament trebuie efectuată prin intermediul unor măsuri de examinare a tranzacțiilor, cunoscute și ca principiul obligației de diligență, ca parte a unui program intern de conformitate (PIC)".

Punctul 21 de la articolul 2 definește „programul intern de conformitate" sau „PIC" ca fiind „politici și proceduri revizuite permanent, eficace, corespunzătoare și proporționale, adoptate de exportatori pentru a facilita respectarea dispozițiilor și obiectivelor prezentului regulament și a clauzelor și condițiilor autorizațiilor prevăzute de prezentul regulament, inclusiv, printre altele, măsuri de diligență necesară care evaluează riscurile legate de exportul produselor către utilizatorii finali și utilizările finale".

Recomandarea (UE) 2019/1318 a Comisiei ([7]) oferă un cadru care să ajute exportatorii să identifice, să gestioneze și să atenueze riscurile asociate controalelor schimburilor comerciale cu produse cu dublă utilizare și să asigure conformitatea cu legile și reglementările relevante ale UE și de la nivel național.

Aceste orientări pot sprijini exportatorii atunci când efectuează măsuri de examinare a tranzacțiilor, cunoscute și sub denumirea de principiul diligenței necesare, ca parte a unui PIC.

În temeiul articolului 5 alineatul (2) din Regulamentul (UE) 2021/821, exportatorii produselor de supraveghere cibernetică neincluse pe listă au obligația de a exercita diligența necesară prin intermediul unor măsuri de examinare a tranzacțiilor, ceea ce înseamnă că iau măsuri cu privire la clasificarea produselor și la evaluarea riscurilor legate de tranzacții. Practic, exportatorii sunt încurajați să reexamineze următoarele:

([7]) Recomandarea (UE) 2019/1318 a Comisiei din 30 iulie 2019 privind programele interne de asigurare a conformității pentru controalele schimburilor comerciale cu produse cu dublă utilizare în temeiul Regulamentului (CE) nr. 428/2009 (JO L 205, 5.8.2019, p. 15, ELI: http://data.europa.eu/eli/reco/2019/1318/oj).

3.1. **Să verifice dacă produsul neinclus pe listă care urmează să fie exportat ar putea fi un „produs de supraveghere cibernetică", adică conceput special pentru a permite supravegherea sub acoperire a persoanelor fizice prin monitorizarea, extragerea, colectarea sau analizarea datelor din sistemele informatice și de telecomunicații.**

Această etapă se referă la determinarea produsului în conformitate cu dispozițiile care se aplică produselor de supraveghere cibernetică. Aceasta include o examinare a caracteristicilor tehnice ale produselor, pe baza parametrilor tehnici stabiliți în anexa I la regulament pentru produsele incluse pe listă și având în vedere termenii și conceptele specifice din definiția produselor de supraveghere cibernetică pentru produsele neincluse pe listă, precum și clasificarea ulterioară a produsului (bunuri, tehnologie sau software).

3.2. **Să examineze capacitățile produsului în cauză de a stabili potențialul de utilizare abuzivă în legătură cu represiunea internă și/sau comiterea unor încălcări flagrante ale drepturilor omului și ale dreptului internațional umanitar de către utilizatorii finali străini.**

Exportatorii ar trebui să efectueze o evaluare pentru a stabili dacă produsul ar putea fi utilizat în mod abuziv pentru a comite represiuni interne, pentru a încălca sau a abuza de drepturile omului, inclusiv dreptul la viață, dreptul de a nu fi supus torturii, tratamentelor inumane și degradante, dreptul la viață privată, dreptul la libertatea de exprimare, dreptul la asociere și întrunire, dreptul la libertatea de gândire, de conștiință și de religie, dreptul la egalitatea de tratament sau interzicerea discriminării sau dreptul la alegeri libere, egale și secrete.

Aceasta include, de asemenea, o evaluare pentru a stabili dacă produsul ar putea fi utilizat ca parte sau componentă a unui sistem care ar putea duce la aceleași încălcări și/sau utilizări necorespunzătoare.

Exportatorii ar trebui să utilizeze în evaluarea lor așa-numitele semnale de alertă care se referă la orice circumstanțe anormale într-o tranzacție care indică faptul că exportul poate fi destinat unei utilizări finale, unui utilizator final sau unei destinații inadecvate.

Semnale de alertă:

(a) produsul este comercializat cu informații referitoare la utilizarea sa potențială pentru supraveghere sub acoperire;

(b) informațiile indică faptul că un produs similar a fost utilizat în mod abuziv în legătură cu represiunea internă și/sau cu comiterea unor încălcări flagrante ale drepturilor omului și ale dreptului internațional umanitar (a se vedea secțiunea 1.3);

(c) informații care indică faptul că articolul a fost utilizat în mod ilegal în activități de supraveghere îndreptate împotriva unui stat membru sau în legătură cu supravegherea ilegală a unui cetățean al UE;

(d) informațiile indică faptul că tranzacția include produse care ar putea fi utilizate pentru instituirea, personalizarea sau configurarea unui sistem despre care se cunoaște că este utilizat în mod abuziv în legătură cu represiunea internă și/sau cu comiterea de încălcări flagrante ale drepturilor omului și ale dreptului internațional umanitar (a se vedea secțiunea 1.3);

(e) articolul sau un articol similar se găsește pe lista publicată în seria C a *Jurnalului Oficial al Uniunii Europene*, în conformitate cu articolul 5 alineatul (6) din regulament.

3.3. **Să examineze, în sprijinul autorităților competente, părțile interesate implicate în tranzacție (inclusiv utilizatorul final și destinatarii, cum ar fi distribuitorii și revânzătorii).**

În sprijinul autorităților competente și în măsura posibilului, exportatorii ar trebui:

(a) înainte și în timpul oricărei tranzacții, să verifice modul în care destinatarii și/sau utilizatorii finali intenționează să utilizeze produsul sau serviciul, pe baza declarațiilor privind utilizarea finală;

(b) să se familiarizeze cu situația de la destinația relevantă a produselor, în special cu starea generală a drepturilor omului, deoarece acest lucru oferă un indicator important al riscului de încălcări flagrante ale drepturilor omului și ale dreptului internațional umanitar legate de un export;

(c) să revizuiască riscurile ca produsul sau serviciul să fie deturnat către un alt utilizator final neautorizat, pe baza semnalelor de alertă enumerate mai jos.

Semnale de alertă:

(a) utilizatorul final are o relație evidentă cu un guvern străin care are antecedente de comitere a represiunilor interne și/sau a încălcărilor flagrante ale drepturilor omului și ale dreptului internațional umanitar;

(b) utilizatorul final face parte din punct de vedere structural din forțele armate sau din alt grup implicat într-un conflict armat care au implicat măsuri de represiune internă și/sau încălcări flagrante ale drepturilor omului și ale dreptului internațional umanitar în trecut;

(c) utilizatorul final a exportat în trecut produse de supraveghere cibernetică către țări în care utilizarea unor astfel de produse a condus la măsuri de represiune internă și/sau la încălcări flagrante ale drepturilor omului și ale dreptului internațional umanitar.

3.4. **Să utilizeze constatările privind diligența necesară pentru a elabora planuri de prevenire și atenuare a potențialelor efecte negative viitoare.**

Exportatorii ar trebui, pe baza constatărilor lor privind diligența necesară, să întrerupă activitățile care provoacă sau contribuie la un impact negativ legat de drepturile omului, precum și să elaboreze și să pună în aplicare un plan de măsuri corective. Aceste opțiuni pot include:

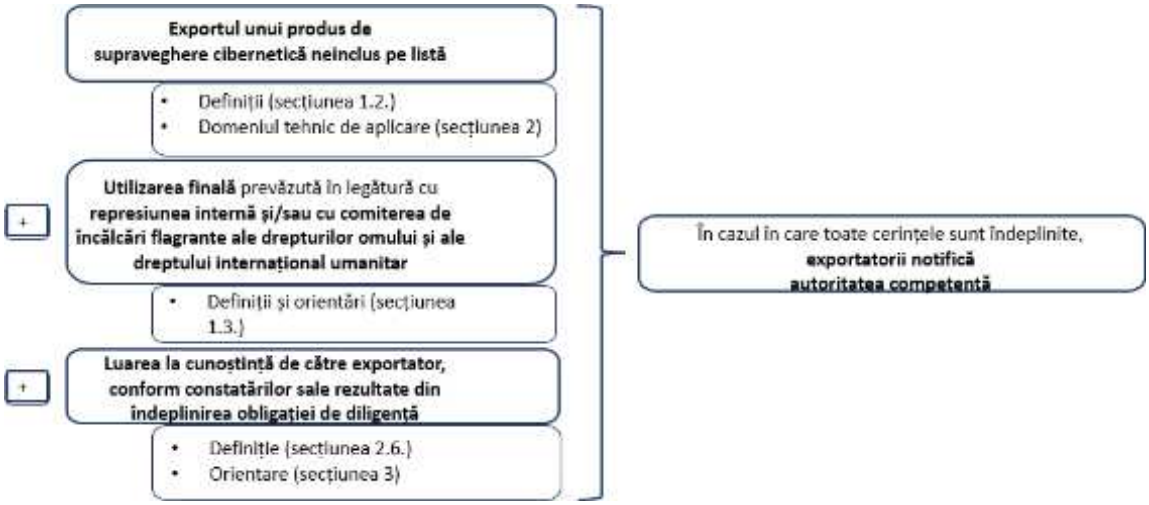
(a) actualizarea politicilor întreprinderii pentru a oferi orientări cu privire la evitarea și abordarea impactului negativ în viitor și a asigura punerea lor în aplicare;

(b) analizarea constatărilor evaluării riscurilor pentru a actualiza și a consolida sistemele de gestionare pentru a urmări mai bine informațiile și a semnala riscurile înainte de producerea efectelor negative;

(c) colectarea de informații pentru a înțelege riscurile de impact negativ la nivel înalt legate de sector;

(d) notificarea autorităților competente ale statelor membre în ceea ce privește constatările privind diligența necesară pentru a facilita fluxul de informații cu privire la anumite produse, utilizatori finali și destinații.

Cerințe prevăzute la articolul 5 alineatul (2) din Regulamentul (UE) 2021/821



4. **APENDICE**

Produse de supraveghere cibernetică incluse pe listă care fac obiectul controlului în temeiul anexei I la Regulamentul (UE) 2021/821

— **Sisteme de interceptare a telecomunicațiilor (5A001.f.)**

În majoritatea țărilor, inclusiv în statele membre, confidențialitatea comunicațiilor este protejată prin lege, dar supravegherea electronică sub acoperire a comunicațiilor de către autoritățile guvernamentale poate fi autorizată într-un cadru juridic [așa-numita interceptare legală (IL)]. Cu toate acestea, era digitală a permis utilizarea tehnologiilor de interceptare la scară largă. Utilizarea instrumentelor de interceptare de către regimul libian a evidențiat potențialul de a implementa aceste tehnologii la scară largă și a stimulat introducerea controlului exporturilor în ceea ce privește sistemele de interceptare a telecomunicațiilor în 2012.

Acest control se aplică echipamentelor concepute pentru extragerea conținutului unei comunicații (voce sau date), precum și a identificatorilor abonaților sau a altor metadate care sunt transmise prin intermediul comunicațiilor fără fir, precum și echipamentelor de monitorizare a frecvențelor radio. Acest control se aplică, de exemplu, dispozitivelor IMSI-catcher (*International Mobile Subscriber Identity* – Identitate internațională de abonat mobil) care interceptează traficul telefonului mobil și monitorizează circulația utilizatorilor de telefoane mobile sau echipamentelor care creează puncte de acces Wi-Fi false care pot extrage numere IMSI de pe un telefon, precum și anumitor tipuri de produse special concepute pentru a permite „inspectarea aprofundată a pachetelor" în sistemele de telecomunicații. Echipamentele de bruiaj al telecomunicațiilor mobile nu intră în domeniul de aplicare al produselor de supraveghere cibernetică, deoarece nu colectează date.

Deși tehnologia de uz general poate fi utilizată pentru a construi astfel de sisteme, capacitățile lor de interceptare la scară largă se vor baza pe piese și componente specifice, inclusiv, de exemplu, pe FGPA (cipuri) specifice software-ului și aplicațiilor, pentru a crește numărul de pachete sau sesiuni de comunicare care pot fi prelucrate pe secundă.

— **Sisteme de supraveghere a internetului (5A001.j.)**

Deși multe comunicații bazate pe internet sunt în prezent criptate în mod implicit, interceptarea datelor de trafic (metadate) referitoare la comunicații – cum ar fi adresele IP și frecvența și dimensiunile schimbului de date – poate fi utilizată în continuare pentru a identifica legăturile dintre persoane și numele de domeniu. Guvernele pot utiliza aceste sisteme în mod legal și sub supravegherea instanțelor judecătorești, în scopuri legitime, cum ar fi pentru identificarea persoanelor care vizitează domenii asociate cu conținut infracțional sau cu caracter terorist. Cu toate acestea, monitorizarea și analiza traficului de internet pe baza caracterizării etnice, religioase, politice sau sociale pot conduce la o cartografiere umană și socială cuprinzătoare a unei țări pentru controlul și reprimarea populației, precum și în alte scopuri, de exemplu pentru identificarea dizidenților politici. Pe lângă aspectele legate de drepturile omului și de represiunea internă, aceste produse pot contribui, de asemenea, la consolidarea capacităților militare și de securitate.

Controlul prevăzut la punctul 5A001.j se aplică sistemelor de control al internetului care operează pe o „rețea de protocol internet (IP) de nivel transport (de exemplu, rețeaua de bază IP națională)" pentru a efectua analiza, extragerea și indexarea conținutului de metadate transmise (voce, video, mesaje, fișiere atașate) pe baza unor „selectorilor stricți" și pentru a cartografia rețeaua relațională a persoanelor. Acestea sunt produse care efectuează „supraveghere sub acoperire" deoarece persoanele vizate nu au cunoștință de interceptarea comunicațiilor. În schimb, controalele nu vizează sistemele în care există o acțiune sau o interacțiune cu un utilizator sau un abonat și, de exemplu, nu se aplică rețelelor sociale sau motoarelor de căutare comerciale. În plus, controalele se aplică sistemelor care prelucrează date provenite de la o rețea centrală a unui furnizor de internet și nu se aplică rețelelor sociale sau motoarelor de căutare comerciale care prelucrează date furnizate de utilizatori.

— **„Produse software de intruziune" (4A005, 4D004 și controalele aferente menționate la 4E001.a. și 4E001.c.)**

Produsele software de intruziune permit operatorului său să obțină în mod disimulat acces de la distanță la un dispozitiv electronic, cum ar fi un telefon inteligent, un laptop, un server sau un dispozitiv al internetului obiectelor, să obțină date stocate pe dispozitiv, să intercepteze prin intermediul unei camere video sau al unui microfon din dispozitiv sau conectat la dispozitiv și să utilizeze dispozitivul ca bază pentru a efectua atacuri asupra echipamentelor la care se conectează dispozitivul sau împotriva contactelor utilizatorului („piraterie informatică prin intermediul dispozitivelor terților"). Deși există utilizări legitime ([8]) ale produselor software de intruziune, de exemplu, „software de acces de la distanță" utilizat pentru asistența de la distanță acordată de departamentele TI, natura disimulată a supravegherii și amploarea informațiilor care ar putea fi colectate prezintă un risc ridicat de încălcare a dreptului la viață privată și la protecția datelor cu caracter personal și pot submina în mod grav dreptul la libertatea de exprimare.

([8]) Din motive de claritate, produsele de supraveghere cibernetică enumerate în anexa I la Regulamentul privind produsele cu dublă utilizare ar necesita o autorizație pentru a fi exportate către țări terțe, indiferent dacă utilizarea produsului este legitimă sau nu.

Controlul prevăzut la punctul 4A005 și următoarele include produse software, precum și sisteme, echipamente, componente și tehnologii conexe, special concepute sau modificate pentru generarea, comanda și controla sau furniza „produse software de intruziune”, dar nu se aplică „produselor software de intruziune” efective, astfel cum sunt definite în anexa I la regulament. Aceste instrumente cibernetice sunt controlate având în vedere perturbările și daunele potențiale pe care le pot cauza dacă sunt utilizate și executate cu succes, dar controalele nu au ca scop să afecteze activitatea cercetătorilor în domeniul securității cibernetice și a industriei, de exemplu, deoarece aceștia din urmă trebuie să facă schimb de informații referitoare la produsele software de intruziune pentru a putea dezvolta soluții pentru produsele lor și pentru a le pune în aplicare înainte de lansarea publică a unei vulnerabilități.

— **Produse software de monitorizare a comunicațiilor (5D001.e.)**

Aceste produse software sunt concepute pentru monitorizarea și analizarea de către autoritățile de aplicare a legii autorizate a datelor colectate prin intermediul măsurilor de interceptare specifice solicitate de la un furnizor de servicii de comunicații. Aceste produse software permit efectuarea de căutări pe baza „selectorilor stricți” în ceea ce privește conținutul comunicațiilor sau metadatele, prin utilizarea unei interfețe pentru interceptarea legală și cartografierea rețelei relaționale sau urmărirea deplasării persoanelor vizate pe baza rezultatelor căutărilor. Aceste produse software sunt destinate „supravegherii sub acoperire”, deoarece utilizează date colectate din interceptarea comunicațiilor fără ca persoanele să aibă cunoștință de acestea. În plus, „analizează” datele colectate prin intermediul „sistemelor de telecomunicații”. Produsul software este instalat în infrastructura autorității guvernamentale [de exemplu, instalația de monitorizare a aplicării legii (IMAL)], iar controlul nu se aplică sistemelor de conformitate a interceptării legale (IL) (de exemplu, sisteme de gestionare a IL și dispozitive de mediere) care sunt dezvoltate comercial și instalate în spațiul furnizorului de servicii de comunicații (de exemplu, integrate în rețeaua de comunicații) și pe care furnizorul de servicii le exploatează și le întreține. Astfel cum se clarifică în textul de control, controalele nu se aplică „produselor software” special concepute sau modificate în scopuri pur comerciale, cum ar fi facturarea, calitatea serviciului (QoS), calitatea experienței (QoE), dispozitivele de mediere sau plățile mobile sau utilizarea serviciilor bancare.

— **Produse utilizate pentru efectuarea criptanalizei (5A004.a.)**

Acest control se aplică produselor concepute să dejoace mecanisme criptografice pentru a obține variabile confidențiale sau informații importante, inclusiv text în clar, parole sau chei criptografice. Criptografia este utilizată pentru a proteja confidențialitatea informațiilor aflate în tranzit și în repaus. Criptanaliza este utilizată pentru a anula această confidențialitate și, prin urmare, această tehnologie „permite” supravegherea sub acoperire prin monitorizarea, extragerea, colectarea sau analizarea datelor din sistemele informatice și de telecomunicații.

— **Instrumente criminalistice/de investigare (5A004.b., 5D002.a.3.b. și 5D002.c.3.b.)**

Instrumentele criminalistice/de investigare sunt concepute pentru a extrage date brute dintr-un dispozitiv (de exemplu, dispozitive de calcul sau comunicare), astfel încât datele să nu fie modificate sau corupte și să poată fi utilizate în scopuri judiciare, și anume în cadrul unei anchete penale sau al unei proceduri în fața unei instanțe judecătorești. Aceste produse eludează controalele de „autentificare” sau de autorizare a unui dispozitiv, astfel încât datele brute să poată fi extrase din dispozitiv. Aceste produse sunt utilizate de guvern și de autoritățile de aplicare a legii, dar și de forțele militare pentru a extrage și analiza date din dispozitivele confiscate. Deși au utilizări legitime, ele pot fi totuși utilizate în mod abuziv și, prin urmare, pot prezenta un risc pentru datele sensibile sau comerciale.

Cu toate acestea, instrumentele criminalistice/de investigare care nu sunt „special concepute” pentru supravegherea sub acoperire nu se încadrează în definiția produselor de supraveghere cibernetică de la articolul 2 punctul 20. De asemenea, instrumentele criminalistice/de investigare care extrag numai date ale utilizatorilor sau în cazul în cărora datele nu sunt protejate pe dispozitiv nu sunt incluse în textul de control de la 5A004.b. și urm. În același timp, controalele nu se aplică echipamentelor de producție sau de testare ale producătorului, instrumentelor de administrare a sistemului sau produselor destinate exclusiv sectorului comerțului cu amănuntul, de exemplu produselor de deblocare a telefoanelor mobile. Prin urmare, având în vedere varietatea acestor tipuri de tehnologii, aplicarea controalelor depinde de o evaluare de la caz la caz a fiecărui produs.

În cele din urmă, se subliniază că există alte produse legate de supraveghere enumerate în anexa I la regulament care nu ar trebui considerate ca făcând obiectul definiției produselor de supraveghere cibernetică, cum ar fi echipamentele de bruiaj a telecomunicațiilor mobile (5A001.f.) concepute pentru deteriorarea sau perturbarea comunicațiilor sau a sistemelor, produsele software de intruziune care modifică un sistem (4D004) și echipamentele de detecție acustică cu laser (6A005.g.) care colectează date audio cu un laser sau care permit ascultarea conversațiilor la distanță (denumit uneori „microfon «laser»”). În mod similar, utilizarea vehiculelor aeriene fără pilot incluse în listă în scopuri de supraveghere nu ar presupune includerea acestor produse în definiția produselor de supraveghere cibernetică.