# DIRECTIVA 2013/40/UE A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI

## din 12 august 2013

## privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 83 alineatul (1),

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European [1],

hotărând în conformitate cu procedura legislativă ordinară [2],

întrucât:

(1) Obiectivele prezentei directive constau în armonizarea sistemelor de drept penal ale statelor membre în ceea ce privește atacurile împotriva sistemelor informatice, prin instituirea unor norme minime privind definirea infracțiunilor și a sancțiunilor relevante, precum și de a îmbunătăți cooperarea dintre autoritățile competente, inclusiv poliția și alte servicii specializate de aplicare a legii din statele membre, precum și agențiile și organismele specializate competente ale Uniunii, cum ar fi Eurojust, Europol și Centrul european de combatere a criminalității informatice și Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA).

(2) Sistemele informatice reprezintă un element esențial al interacțiunii politice, sociale și economice din Uniune. Societatea este deja foarte dependentă de aceste sisteme, fenomenul fiind în creștere. Buna funcționare și securitatea acestor sisteme în Uniune sunt vitale pentru dezvoltarea pieței interne și a unei economii competitive și inovatoare. Asigurarea unui nivel adecvat de protecție a sistemelor informatice ar trebui să facă parte dintr-un cadru cuprinzător și eficace de măsuri de prevenție care să completeze măsurile prevăzute de drept penal ca răspuns la criminalitatea informatică.

(3) Atacurile împotriva sistemelor informatice, în special cele care au legătură cu criminalitatea organizată, constituie o amenințare din ce în ce mai mare, atât la nivelul Uniunii, cât și la nivel mondial, și se manifestă o îngrijorare crescândă în fața posibilității de atacuri teroriste sau motivate politic împotriva sistemelor informatice care fac parte din infrastructura critică a statelor membre și a Uniunii. Această situație reprezintă o amenințare la adresa creării unei societăți informaționale mai sigure și a unui spațiu de libertate, securitate și justiție, necesitând, prin urmare, o reacție la nivelul Uniunii, precum și o mai bună cooperare și coordonare la nivel internațional.

(4) Există un număr de infrastructuri critice în Uniune a căror perturbare sau distrugere ar avea un impact transfrontalier semnificativ. Nevoia de a spori capacitatea de protecție a infrastructurilor critice în Uniune evidențiază necesitatea de a completa măsurile de combatere a atacurilor informatice prin sancțiuni penale severe care să reflecte gravitatea unor astfel de atacuri. Prin „infrastructură critică” se poate înțelege un element, un sistem sau o componentă a acestuia aflată pe teritoriul statelor membre, care este esențială pentru menținerea funcțiilor societale vitale, a sănătății, siguranței, securității, bunăstării sociale sau economice, precum centralele electrice, rețelele de transport și rețelele guvernamentale, și a căror perturbare sau distrugere ar avea un impact semnificativ într-un stat membru ca urmare a incapacității de a menține respectivele funcții.

(5) Există dovezi în privința tendinței producerii unor atacuri la scară largă tot mai periculoase și recurente împotriva sistemelor informatice care, adesea, pot fi esențiale pentru state sau pentru funcții specifice din sectorul public sau privat. În paralel cu această tendință, se dezvoltă metode tot mai sofisticate, cum ar fi crearea și utilizarea așa-numitelor botneturi, care presupune etape succesive ale unei fapte penale, fiecare etapă prezentând un risc importante pentru interesele publice. Prezenta directivă vizează, printre altele, introducerea unor sancțiuni penale pentru etapa de creare de botneturi, și anume etapa în care se stabilește controlul la distanță asupra unui număr semnificativ de calculatoare prin instalarea unor programe malițioase, prin atacuri informatice dirijate. O dată creată, rețeaua de calculatoare infectate care alcătuiește botnetul poate fi activată fără știința utilizatorilor calculatoarelor, pentru a lansa un atac informatic la scară largă, care în mod obișnuit are capacitatea să producă prejudicii grave, astfel cum sunt menționate în prezenta directivă. Statele membre pot să determine ceea ce reprezintă pagubă gravă, conform dreptului și practicilor interne proprii, precum întreruperea serviciilor aferente unor sisteme de importanță publică semnificativă, sau care generează costuri financiare majore sau pierderea de date cu caracter personal sau de informații sensibile.

(6) Atacurile cibernetice la scară largă pot provoca daune economice importante atât prin întreruperea funcționării sistemelor informatice și a comunicațiilor, cât și prin pierderea sau modificarea unor informații confidențiale importante din punct de vedere comercial sau a altor tipuri de date. Ar trebui acordată atenție deosebită acțiunilor de sensibilizare a întreprinderilor mici și mijlocii inovatoare în privința amenințărilor în legătură cu astfel de atacuri și vulnerabilității acestora la acest tip de atacuri, având în vedere faptul că acestea sunt într-o tot mai mare măsură dependente de funcționarea corespunzătoare și de disponibilitatea sistemelor informatice, precum și faptul că resursele acestora destinate securității informatice sunt limitate.

[1] JO C 218, 23.7.2011, p. 130.

[2] Poziția Parlamentului European din 4 iulie 2013 (nepublicată încă în Jurnalul Oficial) și decizia Consiliului din 22 iulie 2013.

(7) Existența unor definiții comune în acest domeniu este importantă pentru a se asigura aplicarea coerentă a prezentei directive în statele membre.

(8) Se impune adoptarea unei abordări comune față de elementele constitutive ale infracțiunilor, incriminând ca infracțiuni de drept comun accesarea ilegală a unui sistem informatic, afectarea integrității unui sistem, afectarea integrității datelor și interceptarea ilegală.

(9) Interceptarea include, nelimitându-se însă în mod obligatoriu la acestea, ascultarea, monitorizarea sau supravegherea conținutului comunicațiilor și obținerea de conținut de date fie direct, prin accesul la sistemele informatice și utilizarea acestora, fie indirect, utilizând dispozitive electronice de interceptare audio sau a de ascultare a convorbirilor telefonice prin mijloace tehnice.

(10) Statele membre ar trebui să prevadă sancțiuni pentru atacurile împotriva sistemelor informatice. Sancțiunile respective ar trebui să fie eficace, proporționale și disuasive și ar trebui să includă pedeapsa cu închisoarea și/sau amendă.

(11) Prezenta directivă prevede sancțiuni penale cel puțin atunci când nu reprezintă un caz minor. Statele membre pot să determine ceea ce reprezintă un caz minor conform dreptului și practicilor interne proprii. Un caz poate fi considerat minor, de exemplu, în situațiile în care prejudiciile cauzate de infracțiune și/sau riscul la adresa intereselor publice sau private, de exemplu la adresa integrității sistemului informatic sau a datelor informatice, sau la adresa integrității, drepturilor și intereselor unei persoane, este nesemnificativ sau de așa natură încât aplicarea unei sancțiuni penale în cadrul limitelor legale sau angajarea răspunderii penale nu este necesară.

(12) Identificarea și denunțarea amenințărilor de atacuri informatice și vulnerabilității conexe ale sistemelor informatice reprezintă un element pertinent al unei prevenții și reacții eficace la atacurile informatice și al îmbunătățirii securității sistemelor informatice. Oferirea de stimulente pentru denunțarea lacunelor de securitate ar putea contribui în acest sens. Statele membre ar trebui să facă eforturi în direcția oferirii de oportunități pentru detectarea și denunțarea pe cale legală a lacunelor de securitate.

(13) Este necesar să se prevadă sancțiuni mai severe în cazul comiterii unui atac împotriva unui sistem informatic de către o organizație criminală, astfel cum este definită în Decizia-cadru 2008/841/JAI a Consiliului din 24 octombrie 2008 privind lupta împotriva crimei organizate ([1]), sau în cazul în care atacul este desfășurat la scară largă, afectând astfel un număr semnificativ de sisteme informatice, inclusiv în cazul în care atacul vizează crearea unui botnet, sau în cazul în care atacul provoacă prejudicii grave, inclusiv în cazul în care este desfășurat prin intermediul unui botnet. Este necesar să se prevadă sancțiuni mai severe în cazul în care atacul este săvârșit împotriva unei infrastructuri critice a unui stat membru sau a Uniunii.

(14) Instituirea unor măsuri eficace împotriva furtului de identitate și a altor infracțiuni legate de identitate constituie un alt element important al unei abordări integrate împotriva criminalității informatice. Necesitatea de a acționa la nivelul Uniunii pentru a combate acest tip de comportament infracțional ar putea fi, de asemenea, analizată în contextul evaluării necesității unui instrument orizontal și cuprinzător al Uniunii.

(15) În concluziile sale din 27-28 noiembrie 2008, Consiliul a invitat statele membre și Comisia să elaboreze o nouă strategie, ținând cont de conținutul Convenției Consiliului Europei privind criminalitatea informatică din 2001. Această convenție constituie cadrul juridic de referință în materie de combatere a criminalității informatice, inclusiv a atacurilor împotriva sistemelor informatice. Prezenta directivă se bazează pe convenția menționată anterior. Prin urmare, finalizarea procesului de ratificare a convenției de către toate statele membre cât mai curând posibil ar trebui să reprezinte o prioritate.

(16) Având în vedere modurile diferite în care pot fi efectuate atacurile și evoluția rapidă în materie de hardware și software, prezenta directivă face trimitere la „instrumente" care pot fi utilizate în scopul comiterii infracțiunilor prevăzute în prezenta directivă. Instrumentele respective ar putea să reprezinte, de exemplu, programe malițioase, inclusiv cele capabile să creeze botneturi, utilizate pentru a comite atacuri informatice. Chiar în cazul în care un astfel de instrument este adecvat sau deosebit de adecvat comiterii uneia dintre infracțiunile prevăzute în prezenta directivă, este posibil ca acesta să fi fost produs în scopuri legitime. Motivată de necesitatea de a evita incriminarea, în cazul în care astfel de instrumente sunt produse și introduse pe piață în scopuri legitime, cum ar fi pentru a testa fiabilitatea unor produse de tehnologia informației sau a securității sistemelor informatice, în afară de cerința privind intenția generală, trebuie să fie îndeplinită și cerința privind intenția directă de a utiliza respectivele instrumente pentru a săvârși una sau mai multe dintre infracțiunile prevăzute în prezenta directivă.

(17) Prezenta directivă nu impune răspundere penală în cazul în care criteriile obiective ale infracțiunilor prevăzute în prezenta directivă sunt îndeplinite, însă acțiunile sunt săvârșite fără intenția de a săvârși o infracțiune, cum ar fi în cazurile în care o persoană nu cunoaște faptul că accesul nu este autorizat, sau în cazul testării sau protejării autorizate a sistemelor informatice, de exemplu, atunci când o societate sau un vânzător atribuie unei persoane sarcina de a testa fiabilitatea sistemului său de securitate. În contextul prezentei directive, obligațiile contractuale sau acordurile de restricționare a accesului la sisteme informatice prin intermediul unei politici privind utilizatorii sau al unor condiții de utilizare a serviciului, precum și litigiile de muncă privind accesul la sistemele informatice și utilizarea acestora în scopuri personale de către un angajat, nu ar trebui să angajeze răspunderea penală, în cazurile în care accesul, în circumstanțe de acest tip, ar fi considerat neautorizat, acesta constituind unicul temei pentru demararea procedurilor penale. Prezenta directivă nu aduce atingere dreptului de acces la informații, astfel cum este prevăzut în legislația națională și în legislația Uniunii, însă în același timp nu servește ca o justificare pentru accesul ilegal și arbitrar la informații.

([1]) JO L 300, 11.11.2008, p. 42.

(18) Atacurile informatice ar putea fi facilitate de diverse circumstanțe, cum ar fi cea în care autorul infracțiunii are acces la sistemele de securitate ale sistemelor informatice afectate în virtutea atribuțiilor sale de serviciu. În contextul legislației naționale, astfel de circumstanțe ar trebui luate în considerare în mod corespunzător pe parcursul procedurilor penale.

(19) Statele membre ar trebui să introducă dispoziții privind circumstanțele agravante în legislația lor națională în conformitate cu normele aplicabile privind circumstanțele agravante prevăzute în sistemul lor juridic. Statele membre ar trebui să se asigure că aceste circumstanțe agravante sunt puse la dispoziția judecătorilor pentru a putea ține seama de acestea la condamnarea autorilor infracțiunilor. Rămâne la latitudinea judecătorului să evalueze aceste circumstanțe împreună cu alte elemente factuale ale cazului analizat.

(20) Prezenta directivă nu reglementează condițiile pentru exercitarea competenței în privința oricărei infracțiuni prevăzute în aceasta, cum ar fi plângerea depusă de victimă la locul în care a fost săvârșită infracțiunea, denunțarea de către statul în care se află locul săvârșirii infracțiunii sau neurmărirea penală a autorului infracțiunii la locul în care a fost săvârșită infracțiunea.

(21) În contextul prezentei directive, statele și organele publice ale acestora au în continuare obligații depline în ceea ce privește garantarea respectării drepturilor omului și a libertăților fundamentale, în conformitate cu obligațiile internaționale existente.

(22) Prezenta directivă întărește importanța rețelelor, cum ar fi rețeaua de puncte de contact, disponibile 24 de ore din 24 și șapte zile din șapte, a Consiliul Europei sau a G8. Aceste puncte de contact ar trebui să fie capabile să ofere o asistență eficace, facilitând, printre altele, schimbul de informații relevante disponibile sau oferirea de consiliere tehnică sau de informații juridice necesare cercetărilor sau procedurilor privind infracțiuni legate de sisteme informatice și datele conexe care îl privesc pe statul membru solicitant. În vederea asigurării unei bune funcționări a acestor rețele, fiecare punct de contact ar trebui să aibă capacitatea de a comunica cu punctul de contact al altui stat membru în mod rapid, cu sprijinul, printre altele, al unui personal format și dotat cu echipamentele necesare. Având în vedere viteza cu care pot fi realizate atacurile informatice la scară largă, statele membre ar trebui să fie în măsură să răspundă prompt la cererile urgente adresate de această rețea de puncte de contact. În astfel de cazuri, ar putea fi oportun ca cererea de informații să fie însoțită de un contact telefonic pentru a asigura o prelucrare rapidă a acesteia de către statul membru solicitat și trimiterea unui răspuns în termen de opt ore.

(23) Cooperarea dintre autoritățile publice, pe de o parte, și sectorul privat și societatea civilă, pe de altă parte, prezintă o mare importanță pentru prevenirea și combaterea atacurilor împotriva sistemelor informatice. Se impune să fie favorizată și îmbunătățită cooperarea dintre prestatori de servicii, producători, organe de aplicare a legii și autorități judiciare, respectând pe deplin statul de drept. Această cooperare ar putea să includă sprijinul din partea prestatorilor de servicii în efortul de a păstra eventuale probe, de a furniza elemente pentru identificarea autorilor infracțiunilor și, în ultimă instanță, de a închide, complet sau parțial, în conformitate cu dreptul și practicile naționale, sistemele informatice sau funcțiile care au fost compromise sau utilizate în scopuri ilegale. Statele membre ar trebui, de asemenea, să aibă în vedere înființarea unor rețele de cooperare și parteneriat cu prestatorii și producătorii de servicii pentru schimbul de informații în legătură cu infracțiunile care fac obiectul prezentei directive.

(24) Este necesar să se culeagă date comparabile privind infracțiunile prevăzute în prezenta directivă. Datele relevante ar trebui puse la dispoziția agențiilor și organismelor specializate competente ale Uniunii, cum ar fi Europol și ENISA, în conformitate cu atribuțiile și necesitățile informaționale ale acestora, pentru a se obține o imagine mai completă a criminalității informatice și a securității informatice și a rețelelor la nivelul Uniunii și a se contribui, astfel, la formularea unor reacții mai eficace. Statele membre ar trebui să transmită, de asemenea, Europolului și Centrului european de combatere a criminalității informatice informații privind modul de operare al autorilor, în scopul efectuării unor evaluări ale amenințărilor și a unor analize strategice ale criminalității informatice în conformitate cu Decizia 2009/371/JAI a Consiliului din 6 aprilie 2009 privind înființarea Oficiului European de Poliție (Europol) [1]. Transmiterea informațiilor poate facilita o mai bună înțelegere a amenințărilor prezente și viitoare, contribuind astfel la un proces decizional mai adecvat și mai precis în ceea ce privește prevenirea și combaterea atacurilor împotriva sistemelor informatice.

(25) Comisia ar trebui să prezinte un raport privind aplicarea prezentei directive și propunerile legislative necesare, care pot conduce la extinderea domeniului său de aplicare, ținând seama de evoluțiile din domeniul criminalității informatice. Aceste evoluții ar putea include și evoluțiile tehnologice care permit, de exemplu, o asigurare mai eficientă a respectării dispozițiilor în domeniul atacurilor împotriva sistemelor informatice, care facilitează prevenirea atacurilor sau care minimizează impactul acestora. În acest scop, Comisia ar trebui să țină seama de analizele și de rapoartele disponibile produse de factorii implicați relevanți, în special de Europol și de ENISA.

(26) Pentru a combate în mod eficient criminalitatea informatică, se impune să fie sporită rezistența sistemelor informatice prin adoptarea unor măsuri corespunzătoare pentru a asigura o protecție mai eficace a acestora împotriva atacurilor informatice. Statele membre ar trebui să ia măsurile necesare în vederea protejării sistemelor informatice care fac parte din infrastructura critică împotriva atacurilor informatice, în cadrul a ceea ce ar trebui să reprezinte protecția sistemelor lor informatice și a datelor conexe. Asigurarea unui nivel adecvat de protecție și de securitate a sistemelor informatice de către persoanele juridice, de exemplu, în legătură cu prestarea de servicii de comunicații electronice publice în conformitate cu legislația Uniunii existentă în materie

[1] JO L 121, 15.5.2009, p. 37.

de confidențialitate și de protecție ale datelor și comunicațiilor electronice, constituie o parte esențială a unei abordări cuprinzătoare pentru combaterea eficace a criminalității informatice. Ar trebui să se garanteze un nivel de protecție adecvat împotriva amenințărilor și vulnerabilităților care pot fi identificate în mod rezonabil, în conformitate cu progresele tehnologice, pentru sectoarele specifice și situațiile specifice de prelucrare a datelor. Costurile și obligațiile asumate pentru această protecție ar trebui să fie proporționale cu eventualele prejudicii provocate celor afectați de un atac informatic. Statele membre sunt încurajate să prevadă în legislația lor națională măsurile de stabilire a responsabilităților în cazurile în care o persoană juridică nu a asigurat, în mod vădit, un nivel adecvat de protecție împotriva atacurilor informatice.

(27) Lacunele și diferențele considerabile existente în legislațiile statelor membre și în procedurile penale în domeniul atacurilor împotriva sistemelor informatice pot crea obstacole în calea luptei împotriva criminalității organizate și terorismului și pot îngreuna desfășurarea unei cooperări judiciare și polițienești eficace în acest domeniu. Dat fiind caracterul transnațional, care nu ține seama de frontiere, al sistemelor informatice moderne, atacurile împotriva acestor sisteme sunt de natură transfrontalieră, subliniind nevoia urgentă de a se face în continuare demersuri pentru armonizarea legislațiilor penale în acest domeniu. De asemenea, coordonarea urmăririi penale în cazurile de atacuri împotriva sistemelor informatice ar trebui să fie facilitată de o punere în aplicare și de o aplicare propriu-zisă corespunzătoare a Deciziei-cadru 2009/948/JAI a Consiliului din 30 noiembrie 2009 privind prevenirea și soluționarea conflictelor referitoare la exercitarea competenței în cadrul procedurilor penale ([1]). Statele membre în cooperare cu Uniunea ar trebui, de asemenea, să urmărească ameliorarea cooperării la nivel internațional în domeniul securității sistemelor, rețelelor și datelor informatice. Ar trebui să se acorde atenția cuvenită securității transferului și stocării datelor în orice acord internațional care implică schimbul de date.

(28) Îmbunătățirea cooperării dintre organele competente de aplicare a legii și autoritățile judiciare din Uniune este esențială pentru combaterea eficientă a criminalității informatice. În acest context, intensificarea eforturilor în ceea ce privește formarea adecvată a autorităților competente pentru a se cunoaște mai bine criminalitatea informatică și efectele acesteia și pentru a promova cooperarea și schimbul de bune practici, de exemplu, prin intermediul agențiilor și organismelor specializate competente ale Uniunii, ar trebui încurajată. Astfel de formări ar trebui să își propună, printre altele, să sensibilizeze participanții cu privire la diferențele dintre sistemele juridice naționale, posibilele provocări de ordin juridic și tehnic întâlnite în anchetele penale și distribuția de competențe între autoritățile naționale competente.

(29) Prezenta directivă respectă drepturile omului și libertățile fundamentale și principiile recunoscute în special de Carta drepturilor fundamentale a Uniunii Europene și de Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale, inclusiv protecția datelor cu caracter personal, dreptul la confidențialitate, libertatea de exprimare și de informare, dreptul la un proces echitabil, prezumția de nevinovăție și drepturile la apărare, precum și principiile legalității și proporționalității infracțiunilor și sancțiunilor penale. În special, prezenta directivă urmărește să asigure respectarea deplină a acestor drepturi și principii și trebuie pusă în aplicare în mod corespunzător.

(30) Protecția datelor cu caracter personal constituie un drept fundamental în conformitate cu articolul 16 alineatul (1) din TFUE și cu articolul 8 din Carta drepturilor fundamentale. Prin urmare, prelucrarea de date cu caracter personal în contextul punerii în aplicare a prezentei directive ar trebui să respecte pe deplin dreptul relevant al Uniunii în domeniul protecției datelor.

(31) În conformitate cu articolul 3 din Protocolul privind poziția Regatului Unit și a Irlandei cu privire la spațiul de libertate, securitate și justiție, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, aceste state membre au notificat intenția lor de a participa la adoptarea și la aplicarea prezentei directive.

(32) În conformitate cu articolele 1 și 2 din Protocolul privind poziția Danemarcei, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, Danemarca nu participă la adoptarea prezentei directive, nu are obligații în temeiul acesteia și nu face obiectul aplicării sale.

(33) Deoarece obiectivele prezentei directive, și anume aplicarea unor sancțiuni penale eficace, proporționale și disuasive în cazul atacurilor împotriva sistemelor informatice în toate statele membre și de a îmbunătăți și încuraja cooperarea judiciară și între alte autorități competente, nu pot fi atinse la un nivel satisfăcător de statele membre și, în consecință, având în vedere amploarea sau efectele acțiunii, pot fi realizate mai bine la nivelul Uniunii, aceasta poate adopta măsuri, în conformitate cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este enunțat în articolul respectiv, prezenta directivă nu depășește ceea ce este necesar pentru atingerea acestor obiective.

(34) Prezenta directivă vizează modificarea și dezvoltarea dispozițiilor Deciziei-cadru 2005/222/JAI a Consiliului din 24 februarie 2005 privind atacurile împotriva sistemelor informatice ([2]). Întrucât modificările care urmează să fie efectuate sunt numeroase și substanțiale, Decizia-cadru 2005/222/JAI ar trebui să fie, din motive de claritate, înlocuită în totalitate în ceea ce privește statele membre care participă la adoptarea prezentei directive,

([1]) JO L 328, 15.12.2009, p. 42.

([2]) JO L 69, 16.3.2005, p. 67.

ADOPTĂ PREZENTA DIRECTIVĂ:

*Articolul 1*

**Obiect**

Prezenta directivă stabilește norme minime privind definiția infracțiunilor și a sancțiunilor penale în domeniul atacurilor împotriva sistemelor informatice. De asemenea, prezenta directivă urmărește să faciliteze prevenirea unor astfel de infracțiuni și să îmbunătățească cooperarea dintre autoritățile judiciare și alte autorități competente.

*Articolul 2*

**Definiții**

În sensul prezentei directive, se aplică următoarele definiții:

(a) „sistem informatic" înseamnă un dispozitiv sau grup de dispozitive interconectate sau omoloage, dintre care unul sau mai multe asigură, prin intermediul unui program, prelucrarea automată a datelor informatice, precum și datele informatice stocate, prelucrate, recuperate sau transmise de acest dispozitiv sau grup de dispozitive în vederea exploatării, a utilizării, a protecției și a întreținerii lor;

(b) „date informatice" înseamnă o reprezentare de fapte, informații sau concepte într-o formă adecvată pentru prelucrare într-un sistem informatic, inclusiv un program care permite unui sistem informatic să execute o funcție;

(c) „persoană juridică" înseamnă o entitate care are statutul de persoană juridică în conformitate cu legislația aplicabilă, dar nu include statele sau alte organisme publice aflate în exercițiul autorității de stat și organizațiile internaționale de drept public;

(d) „fără a avea dreptul" înseamnă un comportament menționat de prezenta directivă, inclusiv accesarea, afectarea integrității sau interceptarea fără autorizare din partea proprietarului sau a unui alt titular de drepturi, a sistemului sau a unei părți a acestuia, sau care nu este permis în temeiul legislației naționale.

*Articolul 3*

**Accesarea ilegală a sistemelor informatice**

Statele membre adoptă măsurile necesare pentru a garanta că accesarea cu intenție și fără drept a unui sistem informatic sau a unei părți a acestuia este incriminată atunci când este săvârșită prin încălcarea unei măsuri de securitate, cel puțin atunci când nu reprezintă un caz minor.

*Articolul 4*

**Afectarea ilegală a integrității sistemului**

Statele membre adoptă măsurile necesare pentru a asigura că perturbarea gravă sau întreruperea funcționării unui sistem informatic prin introducerea, transmiterea, periclitarea, ștergerea, deteriorarea, modificarea, eliminarea datelor informatice sau prin a le face inaccesibile, cu intenție și fără drept, este incriminată, cel puțin atunci când nu reprezintă un caz minor.

*Articolul 5*

**Afectarea ilegală a integrității datelor**

Statele membre adoptă măsurile necesare pentru a asigura că fapta care constă în ștergerea, periclitarea, deteriorarea, modificarea, eliminarea datelor informatice dintr-un sistem informatic sau în a le face inaccesibile, cu intenție și fără drept, este incriminată, cel puțin atunci când nu reprezintă un caz minor.

*Articolul 6*

**Interceptarea ilegală**

Statele membre adoptă măsurile necesare pentru a garanta că interceptarea, cu intenție și fără drept, prin mijloace tehnice, de transmisii private de date informatice către un sistem informatic, dinspre acesta sau în interiorul acestuia, inclusiv de emisii electromagnetice provenite de la un sistem informatic care transmite asemenea date informatice este incriminată, cel puțin atunci când nu reprezintă un caz minor.

*Articolul 7*

**Instrumentele care servesc la săvârșirea infracțiunilor**

Statele membre adoptă măsurile necesare pentru a garanta că producerea, vânzarea, procurarea în vederea utilizării, importul, distribuirea sau punerea la dispoziție în alt mod, cu intenție, a următoarelor instrumente, fără a avea dreptul și cu intenția de a servi la săvârșirea oricăreia dintre infracțiunile menționate la articolele 3-6, sunt incriminate, cel puțin atunci când nu reprezintă un caz minor:

(a) un program de calculator, conceput sau adaptat în principal în scopul săvârșirii oricăreia dintre infracțiunile menționate la articolele 3-6;

(b) o parolă de calculator, un cod de acces sau date similare, prin care un întreg sistem informatic sau orice parte a acestuia poate fi accesat(ă).

*Articolul 8*

**Instigarea, complicitatea și tentativa**

(1) Statele membre asigură că instigarea și complicitatea la săvârșirea oricăreia dintre infracțiunile menționate la articolele 3-7 sunt incriminate.

(2) Statele membre se asigură că tentativa de săvârșire a oricăreia dintre infracțiunile prevăzute la articolele 4 și 5 este incriminată.

*Articolul 9*

**Sancțiuni**

(1) Statele membre iau măsurile necesare pentru a garanta că infracțiunile menționate la articolele 3-8 sunt sancționate de sancțiuni penale eficace, proporționale și disuasive.

(2) Statele membre iau măsurile necesare pentru a garanta că infracțiunile menționate la articolele 3-7 sunt sancționate cu o pedeapsă maximă cu închisoarea de cel puțin doi ani, cel puțin atunci când nu reprezintă un caz minor.

(3) Statele membre iau măsurile necesare pentru a garanta că infracțiunile menționate la articolele 4 și 5 sunt sancționate cu o pedeapsă maximă cu închisoarea de cel puțin trei ani în cazul în

care sunt săvârșite cu intenție și un număr semnificativ de sisteme informatice a fost afectat prin utilizarea unui instrument menționat la articolul 7, conceput sau adaptat în principal în acest scop.

(4) Statele membre iau măsurile necesare pentru a garanta că infracțiunile menționate la articolele 4 și 5 sunt sancționate cu o pedeapsă maximă cu închisoarea de cel puțin cinci ani în cazul în care:

(a) sunt săvârșite în cadrul unei organizații criminale, astfel cum este definită în Decizia-cadru 2008/841/JAI, independent de sancțiunea prevăzută de aceasta;

(b) provoacă prejudicii grave; sau

(c) sunt săvârșite împotriva unui sistem informatic din infrastructura critică.

(5) Statele membre iau măsurile necesare pentru a garanta că infracțiunile menționate la articolele 4 și 5, în cazurile în care sunt săvârșite prin abuzul de date cu caracter personal ale unei alte persoane, în scopul de a obține încrederea unei terțe părți, cauzând prejudicii prin aceasta deținătorului de drept al identității, acestea, în conformitate cu legislația națională, pot fi considerate circumstanțe agravante, cu excepția cazurilor în care respectivele circumstanțe sunt încadrate la altă infracțiune sancționată de legislația națională.

*Articolul 10*

**Răspunderea persoanelor juridice**

(1) Statele membre iau măsurile necesare pentru a garanta angajarea răspunderii persoanelor juridice pentru oricare dintre infracțiunile prevăzute la articolele 3-8, săvârșite în beneficiul lor de către orice persoană, acționând fie în nume propriu, fie ca parte a unui organism al persoanei juridice și având o funcție de conducere în cadrul persoanei juridice, în temeiul:

(a) unei împuterniciri din partea persoanei juridice;

(b) unei prerogative de a lua decizii în numele persoanei juridice;

(c) unei prerogative de a exercita controlul în cadrul persoanei juridice.

(2) Statele membre adoptă măsurile necesare pentru a garanta angajarea răspunderii persoanelor juridice în cazul în care nesupravegherea sau neexercitarea controlului, imputabile unei persoane menționate la alineatul (1), a permis săvârșirea, de către o persoană aflată în subordine, a oricăreia dintre infracțiunile menționate la articolele 3-8, în beneficiul acelei persoane juridice.

(3) Răspunderea persoanelor juridice în temeiul alineatelor (1) și (2) nu exclude procedurile penale îndreptate împotriva persoanelor fizice care sunt autori, instigatori sau complici la oricare dintre infracțiunile prevăzute la articolele 3-8.

*Articolul 11*

**Sancțiuni aplicabile persoanelor juridice**

(1) Statele membre iau măsurile necesare pentru a garanta că oricărei persoane juridice a cărei răspundere este angajată în temeiul articolului 10 alineatul (1) i se aplică sancțiuni eficace, proporționale și disuasive, care includ amenzi penale sau administrative și care pot să includă alte sancțiuni, ca de exemplu:

(a) decăderea din dreptul de a primi beneficii publice sau ajutor public;

(b) interdicția temporară sau permanentă de a desfășura activități comerciale;

(c) punerea sub supraveghere judiciară;

(d) lichidarea judiciară;

(e) închiderea temporară sau permanentă a unităților care au servit la comiterea infracțiunii.

(2) Statele membre iau măsurile necesare pentru a garanta că oricărei persoane juridice a cărei răspundere este angajată în temeiul articolului 10 alineatul (2) i se aplică sancțiuni sau măsuri eficace, proporționale și disuasive.

*Articolul 12*

**Competență**

(1) Statele membre își determină competența cu privire la infracțiunile menționate la articolele 3-8 în cazul în care infracțiunea a fost săvârșită:

(a) integral sau parțial pe teritoriul lor; sau

(b) de către unul dintre resortisanții lor, cel puțin în cazurile în care acțiunea constituie o infracțiune acolo unde a fost săvârșită.

(2) Atunci când își determină competența în conformitate cu alineatul (1) litera (a), un stat membru se asigură că are competență atunci când:

(a) autorul săvârșește infracțiunea atunci când este prezent fizic pe teritoriul său, indiferent dacă infracțiunea vizează un sistem informatic situat pe teritoriul său; sau

(b) infracțiunea vizează un sistem informatic situat pe teritoriul său, indiferent dacă autorul era sau nu era prezent fizic pe teritoriul său.

(3) Un stat membru informează Comisia atunci când decide să își determine competența în ceea ce privește o infracțiune dintre cele menționate la articolele 3-8, care a fost săvârșită în afara teritoriului său, inclusiv în cazul în care:

(a) autorul infracțiunii își are reședința obișnuită pe teritoriul său; sau

(b) infracțiunea a fost săvârșită în beneficiul unei persoane juridice având sediul pe teritoriul său.

*Articolul 13*

**Schimbul de informații**

(1) În scopul efectuării schimbului de informații referitoare la infracțiunile menționate la articolele 3-8, statele membre se asigură că dispun de un punct de contact național operațional și că utilizează rețeaua existentă de puncte de contact operaționale disponibile 24 de ore din 24 și șapte zile pe săptămână. Statele membre se asigură, de asemenea, că dispun de procedurile necesare astfel încât, pentru cereri urgente de asistență, autoritatea competentă poate indica, în termen de cel mult opt ore de la primire, cel puțin dacă cererea va primi un răspuns, precum și forma și ora estimată ale acestui răspuns.

(2) Statele membre informează Comisia cu privire la punctul lor de contact desemnat menționat la alineatul (1). Comisia comunică aceste informații celorlalte state membre, precum și agențiilor și organelor specializate competente ale Uniunii.

(3) Statele membre iau toate măsurile necesare pentru a se asigura că sunt puse la dispoziție canale adecvate pentru a facilita aducerea, fără întârziere, la cunoștința autorităților naționale competente a infracțiunilor menționate la articolele 3-6.

*Articolul 14*

**Monitorizare și statistici**

(1) Statele membre se asigură că dispun de un sistem adecvat pentru înregistrarea, producerea și furnizarea de date statistice cu privire la infracțiunile menționate la articolele 3-7.

(2) Datele statistice menționate la alineatul (1) acoperă, cel puțin, datele disponibile cu privire la numărul de infracțiuni menționate la articolele 3-7 înregistrate de statele membre și numărul de persoane urmărite penal și condamnate pentru infracțiunile prevăzute la articolele 3-7.

(3) Statele membre transmit Comisiei datele culese în conformitate cu prezentul articol. Comisia asigură publicarea unei revizuiri consolidate a acestor rapoarte statistice și transmiterea acesteia către agențiile și organele specializate competente ale Uniunii.

*Articolul 15*

**Înlocuirea Deciziei-cadru 2005/222/JAI**

Decizia-cadru 2005/222/JAI este înlocuită în ceea ce privește statele membre care participă la adoptarea prezentei directive, fără a aduce atingere obligațiilor statelor membre în ceea ce privește termenul pentru transpunerea deciziei-cadru în legislația națională.

În ceea ce privește statele membre care participă la adoptarea prezentei directive, trimiterile la Decizia-cadru 2005/222/JAI se interpretează ca trimiteri la prezenta directivă.

*Articolul 16*

**Transpunere**

(1) Statele membre pun în aplicare actele cu putere de lege și actele administrative necesare pentru a se conforma prezentei directive până la 4 septembrie 2015.

(2) Statele membre transmit Comisiei textul dispozițiilor care transpun în legislația națională obligațiile care le revin în temeiul prezentei directive.

(3) Atunci când statele membre adoptă respectivele măsuri, acestea conțin o trimitere la prezenta directivă sau sunt însoțite de o asemenea trimitere la data publicării lor oficiale. Statele membre stabilesc modalitatea de efectuare a acestei trimiteri.

*Articolul 17*

**Raportare**

Până la 4 septembrie 2017, Comisia prezintă Parlamentului European și Consiliului un raport de evaluare a gradului în care statele membre au adoptat măsurile necesare pentru a se conforma prezentei directive, însoțit, dacă este necesar, de propuneri legislative. Comisia ține seama, de asemenea, de evoluțiile tehnice și juridice în domeniul criminalității informatice, în special cu privire la domeniul de aplicare al prezentei directive.

*Articolul 18*

**Intrarea în vigoare**

Prezenta directivă intră în vigoare în a douăzecea zi de la data publicării sale în *Jurnalul Oficial al Uniunii Europene*.

*Articolul 19*

**Destinatarii**

Prezenta directivă se adresează statelor membre, în conformitate cu tratatele.

Adoptată la Bruxelles, 12 august 2013.

| *Pentru Parlamentul European* | *Pentru Consiliu* |
|---|---|
| *Președintele* | *Președintele* |
| M. SCHULZ | L. LINKEVIČIUS |