Traducere neoficială

PRINCIPIILE GLOBALE CU PRIVIRE LA SECURITATEA NAȚIONALĂ ŞI DREPTUL LA INFORMAȚIE

(“PRINCIPIILE TSHWANE”)

finalizate în Tshwane, Africa de Sud
publicate pe 12 iunie 2013

Traducerea a fost efectuată în cadrul proiectului “Promovarea şi implementarea Principiilor globale privind securitatea națională şi dreptul la informare”realizate de Institutul de politici publice cu sprijinul financiar al Fundației Soros Moldova, Programul Drept.

Instituția privată Institutul de politici publice este o organizație necomercială, neguvernamentală, non-profit, apolitică, având scopul de a contribui la dezvoltarea in Republica Moldova a unei societăți deschise, participatorii, pluraliste, bazate pe valorile democratice, prin efectuarea, sprijinirea şi sponsorizarea cercetărilor şi analizelor independente ale politicilor publice în domeniile prioritare ale existenței comunității şi funcționării societății.

Adresa IPP: str. Puşkin 16/1, Chişinău, Republica Moldova
e-mail: ipp@ipp.md; www.ipp.md

Principiile globale cu privire la securitea națională şi dreptul la informație

Aceste principii globale cu privire la securitea națională şi dreptul la informație, lansate pe 12 iunie 2013, au fost elaborate de 22 de grupuri pe parcursul unei perioade de doi ani, într-un proces care a implicat consultarea a mai mult de 500 de experți din peste 70 de țări din întreaga lume. Procesul de elaborare a culminat la o întâlnire în Tshwane, Africa de Sud, care le-a dat numele.

TABLA DE MATERII

INTRODUCERE 5
CONTEXT ŞI JUSTIFICARE 6
PREAMBUL 8
DEFINIŢII 12
PARTEA I. PRINCIPII GENERALE 15
PARTEA II. INFORMAŢII CARE POT FI NEDIVULGATE PE MOTIV DE SECURITATE NAŢIONALĂ ŞI INFORMAŢII CARE TREBUIE DIVULGATE 21
PARTEA III. A: REGULI PRIVIND SECRETIZAREA ŞI DESCRETIZAREA INFORMAŢIEI 31
PARTEA III. B: REGULI CU PRIVIRE LA ADMINISTRAREA CERERILOR DE INFORMAŢII 36
PARTEA IV. ASPECTE JUDICIARE ALE SECURITĂŢII NAŢIONALE ŞI DREPTUL LA INFORMAŢIE 40
PARTEA VI. INFORMAŢII DE INTERES PUBLIC DIVULGATE DE CĂTRE FUNCŢIONARII PUBLICI 48
PARTEA VII. LIMITE CU PRIVIRE LA MĂSURILE DE SANCŢIONARE SAU DE RESTRÂNGERE A DIVULGĂRII INFORMAŢIEI CĂTRE PUBLIC 56
PARTEA VIII. PRINCIPIUL FINAL 59
Anexă: Organizaţii partenere 60

INTRODUCERE

Aceste Principii au fost create cu scopul de a oferi repere orientative celor implicaţi în elaborarea, revizuirea sau punerea în aplicare a legilor sau a prevederilor referitoare la autoritatea statului în caz de nedivulgare a informaţiilor din motive de securitate naţională sau de pedepsire a divulgării unor astfel de informaţii.

Principiile se bazează pe acte normative internaţionale (inclusiv regionale) şi naţionale, standarde, bune practici şi opinii ale experţilor.

Ele vizează mai degrabă motivul securităţii naţionale decât toate motivele de nedivulgare a informaţiilor. Toate celelalte motive publice de restricţionare a accesului trebuie, cel puţin, să respecte aceste standarde.

Aceste Principii au fost elaborate de 22 organizaţii şi centre academice (enumerate în Anexă) prin consultarea a peste 500 de experţi din peste 70 de ţări în cadrul a 14 şedinţe organizate în întreaga lume, facilitate de Open Society Justice Initiative (Iniţiativa juridică a fundaţiilor pentru o societate deschisă) în consultanţă cu cei patru raportori speciali specializaţi pe libertatea de expresie şi/sau libertatea mass-mediei, precum şi cu raportorul special privind combaterea terorismului şi drepturile omului:

- Raportorul special al Naţiunilor Unite pentru libertatea opiniilor şi exprimării
- Raportorul Special al Naţiunilor Unite privind combaterea terorismului şi drepturile omului
- Raportorul special pentru libertatea de exprimare şi accesul la informaţie al Comisiei Africane pentru drepturile omului şi popoarelor (ACHPR)
- Raportorul special pentru libertatea de exprimare al Organizaţiei Statelor Americane (OAS)
- Reprezentantul pentru libertatea mass-mediei al Organizaţiei pentru Securitate şi Cooperare în Europa (OSCE).

CONTEXT ŞI JUSTIFICARE

Securitatea naţională şi dreptul publicului la informaţie sunt adesea percepute ca fiind antitetice. În timp ce uneori există o tensiune între dorinţa guvernului de a păstra secretul informaţiilor din motive de securitate naţională şi dreptul publicului la informaţiile deţinute de către autorităţile publice, o analiză imparţială a istoriei recente sugerează că, în practică, interesele legitime de securitate naţională sunt cel mai bine protejate atunci când publicul este bine informat despre activităţile statului, inclusiv despre cele întreprinse pentru a proteja securitatea naţională.

Permiţând controlul public asupra acţiunii statului, accesul la informaţie nu doar protejează împotriva abuzului funcţionarilor publici, dar, de asemenea, permite publicului să joace un rol în determinarea politicilor statului, astfel formând un component esenţial al adevăratei securităţi naţionale, al participării democratice şi al formulării unei politici coerente. Cu scopul de a proteja exercitarea deplină a drepturilor omului, în anumite circumstanţe păstrarea secretă a informaţiei ar putea fi necesară pentru a proteja interesele legitime ale securităţii naţionale.

Găsirea echilibrului corect devine tot mai dificilă şi fiindcă instanţele din numeroase ţări dau dovadă de mai puţină independenţă si de tot mai mult respect pentru poziţia autoritîţilor publice atunci cînd acestea invocă securitatea naţională. Această favorizare este încurajată prin prevederi legislative ale mai multor ţări în domeniul securităţii care impun excepţii de la dreptul la informaţie, de la procedura ordinară de probare, precum şi de la drepturile acuzatului la o simplă presupunere sau invocare a riscului care planează asupra securităţii naţionale. Invocarea exagerată de către autorităţile publice a temerelor legate de securitatea naţională poate submina grav principalele garanţii instituţionale de protecţie împotriva abuzului guvernului: independenţa instanţelor judecătoreşti, statul de drept, controlul legislativ, libertatea mass-mediei şi guvernare transparentă.

Aceste Principii constituie un răspuns la acele provocări continuie descrise mai sus, precum şi la faptul că, în ultimii ani, un număr semnificativ de state ale lumii s-au angajat să adopte sau să revizuiască regimurile de secretizare şi legislaţia conexă. La rândul său această tendinţă a fost înfrântă de anumite evoluţii. Probabil cea mai semnificativă a fost adoptarea rapidă, după căderea Zidului Berlinului, a legilor cu privire la accesul la informaţie. În consecinţă, la momentul publicării acestor Principii peste 5.2 miliarde de oameni din 95 de ţări din lume beneficiază de dreptul accesului la informaţie – cel puţin prin lege, dacă nu şi în practică. Oamenii din aceste ţări – adeseori pentru prima dată – îşi pun întrebarea dacă şi în ce condiţii informaţia poate fi ţinută secretă. Alte evoluţii care contribuie la sporirea numărului de acte normative care susţin secretizarea au reflectat răspunsul autorităţilor publice la acte de terorism sau la pericolul savârşirii acestora si interesul pentru reglemetarea secretizării prin lege în contextul tranziţiei spre democraţie.

PREAMBUL

Organizațiile şi persoanele fizice implicate în elaborarea acestor Principii:

Reamintind că accesul la informația deținută de către stat este un drept al fiecărei persoane şi, prin urmare, acest drept trebuie protejat de legi elaborate cu precizie şi cu excepții elaborate cu cea mai mare atenție, pentru supravegherea dreptului de către instanțe judecătoreşti independente, organe parlamentare de supraveghere şi alte instituții independente;

Recunoscând că statele pot avea un interes legitim în nedivulgarea unor anumite informații, inclusiv din motive de securitate națională şi subliniind că menținerea echilibrului adecvat dintre divulgarea şi nedivulgarea informației este vitală într-o societate democratică şi esențială pentru securitatea, progresul, dezvoltarea şi bunăstarea acesteia, precum şi pentru deplina beneficiere de drepturile omului şi de libertățile fundamentale;

Afirmând că este imperativ ca oamenii să poată monitoriza comportamentul guvernului lor şi să participe pe deplin într-o societate democratică, să beneficieze de acces la informația deținută de către autoritățile publice, inclusiv la informația referitoare la securitatea națională;

Constatând că aceste Principii sunt bazate pe acte normative internaționale şi standarde referitoare la dreptul publicului de a avea acces la informațiile deținute de către autorități şi alte drepturi ale omului, în evoluția practică a statului (după cum se reflectă, inter alia, în hotărâri ale instanțelor naționale şi internaționale, precum şi ale tribunalelor), pe principiile generale ale dreptului recunoscute de către comunitatea națiunilor şi pe scrierile experților;

Ținând cont de dispozițiile relevante conținute în Declarația Universală a Drepturilor Omului, Convenția Internațională privind Drepturile Civile şi Politice, Carta Africană a Drepturilor Omului şi Popoarelor, Convenția Americană a Drepturilor Omului, Convenția

Europeană a Drepturilor Omului şi Convenția Consiliului Europei privind Accesul la Documente Oficiale;

Ținând cont în continuare de Declarația privind Principiile Libertății de Exprimare ale Comisiei Inter-Americane pentru Drepturile Omului; Modelul Inter-American de Lege privind Accesul la Informație; Declarația privind Principiile Libertății de Exprimare din Africa şi Modelul de Lege cu privire la Accesul la Informație pentru Africa;

Reamintind Declarația Comună din 2004 a Raportorului Special al Națiunilor Unite cu privire la Libertatea de Opinie şi Exprimare, a Reprezentantului OSCE pentru Libertatea Presei şi a Raportorului Special pentru Libertatea de Exprimare al Comisiei Inter-Americane pentru Drepturile Omului; Declarațiile Comune din 2006, 2008, 2009 şi 2010 ale celor trei experți, precum şi a Raportorului Special pentru Libertatea de Exprimare şi Accesul la Informație al Comisiei Africane pentru Drepturile Omului şi Popoarelor; Declarația Comună din decembrie 2010 publicată pe Wikileaks a Raportorilor Speciali ai Comisiei Inter-Americane şi ai Națiunilor Unite; şi Raportul privind Drepturile Omului şi Combaterea Terorismului, adoptat de Comisia de la Veneția în 2010;

Reamintind în continuare Principiile de la Johannesburg privind Securitatea Națională, Libertatea de Exprimare şi Accesul la Informație adoptate de către un grup de experți convocat prin Articolul 19 în 1995, precum şi Principiile de Supraveghere şi Responsabilitate pentru Serviciile de Securitate într-o Democrație Constituțională elaborate în 1997 de către Centrul pentru Studii de Securitate Națională (CNSS) şi Fundația Poloneză Helsinki pentru Drepturile Omului;

Constatând că există principii internaționale - precum cele incluse în Legea Model privind Accesul la Informație în Africa, Principiile Călăuzitoare ale Națiunilor Unite privind Businessul şi Drepturile Omului (”Principiile Ruggie”), Tratatul privind Comerțul cu Arme, Orientările OCDE pentru întreprinderile multinaționale şi Documentul de la Montreux referitor la obligațiile juridice internaționale pertinente şi bunele practici pentru state în ceea ce priveşte operațiunile

societăților private din domeniul militar şi de securitate în timpul conflictelor armate - care recunosc importanța critică a accesului la informație din sau în raport cu întreprinderi de afacere în anumite circumstanțe; şi că unele vizează în mod express necesitatea companiilor private şi de securitate de a opera în cadrul sectorului de securitate națională pentru a face publice anumite informații;

Menționând că aceste Principii nu se referă la standarde esențiale de colectare a informației secrete, de gestionare a datelor cu caracter personal sau de schimb de informații secrete, la care se face referință în "bunele practici cu privire la cadrul legal şi instituțional pentru serviciile de informare şi supravegherea lor" publicate în 2010 de către Martin Scheinin şi, ulterior, de către Raportorul Special al ONU cu privire la promovarea şi protecția drepturilor omului şi libertăților fundamentale în lupta împotriva terorismului, la cererea Consiliului ONU pentru Drepturile Omului;

Recunoscând importanța schimbului eficient de informații secrete între state, aşa cum se solicită în Rezoluția Consiliului de Securitate ONU din 1373;

Recunoscând în continuare că barierele în calea supravegherii publice şi independente create în numele securității naționale sporesc riscul apariției unei conduite ilegale, corupte şi frauduloase care poate rămâne nedescoperită; şi că asemenea încălcări ale dreptului la viață privată şi ale altor drepturi individuale adesea apar sub paravanul păstrării secretului securității naționale;

Preocupați de costurile pentru securitatea națională prin suprasecretizare, inclusiv împiedicarea schimbului de informații între agențiile guvernamentale şi aliați, incapacitatea de a proteja secretele legitime, incapacitatea de a găsi informații importante din mijlocul unei multitudini, colectarea repetitivă de informații de către multiple agenții şi suprasolicitarea managerilor de securitate;

Subliniind că Principiile se concentrează asupra dreptului publicului la informație şi vizează drepturile la informație ale deținuților,

victime ale încălcărilor drepturilor omului şi altele cu pretenții sporite la informație doar în măsura în care aceste drepturi sunt strâns legate de accesul public la informație;

Recunoscând că anumite informații care nu ar trebui să fie nedivulgate din motive de securitate națională, pot fi totuşi nedivulgate din diverse motive recunoscute de dreptul internațional – inclusiv, spre exemplu, relațiile internaționale, caracterul echitabil al procedurilor judiciare, drepturile părților aflate în litigiu şi dreptul la viață privată – supuse mereu principiului conform căruia informațiile pot fi nedivulgate doar atunci când interesul public în menținerea secretului informațiilor prevalează în mod clar asupra interesului public de a avea acces la informație;

Dorind să ofere orientări practice guvernelor, organelor legislative şi de reglementare, autorităților publice, autorilor de legi, instanțelor, altor organe de supraveghere, precum şi societății civile cu privire la unele dintre cele mai dificile probleme apărute la intersecția securității naționale şi a dreptului la informare, în special cele care implică respectarea drepturilor omului şi responsabilitate democratică;

Încercând să elaboreze Principii de valoare şi aplicabilitate universală;

Recunoscând că statele se confruntă cu provocări deosebit de variate în echilibrarea intereselor publice în ceea ce priveşte divulgarea şi necesitatea confidențialității în vederea protecției intereselor legitime de securitate națională şi aceasta în timp ce Principiile sunt universale, aplicarea lor practică poate răspunde realităților locale, inclusiv diverselor sisteme juridice;

Recomandă ca structurile corespunzătoare la nivel național, regional şi internațional să întreprindă acțiuni pentru a disemina şi discuta aceste Principii, precum şi pentru a le aproba, adopta şi/sau pentru a le pune în aplicare, în măsura în care este posibil, cu scopul de a ajunge progresiv la exercitarea deplină a dreptului la informație prevăzut în Principiul 1.

DEFINIȚII

În cadrul acestor principii, cu excepția cazului în care contextul cere altfel:

„Companiile private din sectorul securității naționale înseamnă**”** orice persoană juridică care îndeplineşte sau a îndeplinit orice tranzacție sau afacere în sectorul securității naționale, dar numai în acea calitate, ori ca un contractor sau furnizor de servicii, facilități, personal sau bunuri inclusiv, dar nu limitate la armament, echipament şi informații. Includ companiile private militare sau de securitate. Nu includ persoane juridice organizate non-profit sau organizații neguvernamentale”.

“Independent” înseamnă liber din punct de vedere instituțional, financiar şi operațional de influența, orientarea sau controlul executivului, inclusiv al tuturor autorităților din sectorul securității naționale.

“Informație” înseamnă orice document original sau copie a materialului documentar, indiferent de caracteristicile fizice ale acestuia, precum şi orice alt material tangibil sau intangibil, indiferent de forma şi mediul în care acesta este ținut. Aceasta include, dar nu se limitează la, înregistrări, corespondență, fapte, opinii, recomandări, memorandumuri, date, statistici, cărți, desene, planuri, hărți, diagrame, fotografii, înregistrări audio sau video, documente, e-mailuri, jurnale, mostre, modele şi date păstrate în orice format electronică.

“Informație de interes public” se referă la informația care este de interes sau beneficiu public şi nu doar de interes individual, a cărei divulgare este “în interesul public“, pentru că, spre exemplu, este utilă pentru înțelegerea publică a activităților guvernamentale.

“Interes legitim de securitate națională” se referă la un interes al cărui scop real şi impactul principal este protecția securității naționale, în conformitate cu dreptul internațional şi național. (Categoriile de informație a căror nedivulgare poate fi necesară pentru a proteja un interest legitim de securitate națională sunt stabilite în

Principiul 9). Un interes de securitate națională nu este legitim dacă scopul său real sau impactul său principal este de a proteja un interes fără legătură cu securitatea națională, cum ar fi protecția guvernului sau a oficialilor de situații jenante sau de expunere la activități ilicite; tăinuirea de informații cu privire la încălcarea drepturilor omului, orice altă încălcare a legii sau a funcționării instituțiilor publice; consolidarea sau perpetuarea unui anumit interes politic, partid sau ideologie ; sau suprimarea protestelor legale.

“Securitate națională” nu este un termen definit în aceste Principii. Principiul 2 include o recomandare conform căreia “securitatea națională“ trebuie definită cu exactitate în legislația națională, în concordanță cu necesitățile unei societăți democratice.

“Autorități publice” includ toate organele din cadrul sectoarelor executiv, legislativ şi judiciar la toate nivelurile de guvernare, autoritățile constituționale şi legale, inclusiv autorități din sectorul de securitate; şi structuri non-statale care sunt deținute sau controlate de către guvern sau care au rol de agenți guvernamentali. “Autoritățile publice“ includ, de asemenea, entități private sau alte entități care îndeplinesc funcții sau servicii publice sau operează cu fonduri publice substanțiale sau beneficii, dar numai în ceea ce priveşte îndeplinirea acestor funcții, prestarea de servicii sau utilizarea de fonduri publice sau beneficii.

“Personal public” sau **“funcționar public”** se referă la foştii sau actualii angajați publici, antreprenori şi sub-contractori ai autorităților publice, inclusiv din sectorul de securitate. “Personal public“ sau “funcționar public“ include, de asemenea, persoane angajate de structuri non-statale care sunt deținute sau controlate de guvern sau care servesc ca agenți guvernamentali; precum şi angajați ai entităților private sau de altă natură care îndeplinesc funcții sau servicii publice sau operează cu fonduri publice substanțiale sau profită de beneficii, dar numai în ceea ce priveşte îndeplinirea acestor funcții, prestarea de servicii sau utilizarea fondurilor publice sau a beneficiilor.

“Sancțiune”, utilizat ca substantiv, se referă la orice formă de pedeapsă sau de limitări, inclusiv măsuri penale, civile şi administrative. Când e utilizat ca verb, “a sancționa” înseamnă a pune în aplicare asemenea forme de pedeapsă sau limitări.

“Sectorul securității naționale” este definit ca incluzând ”i) forțele de securitate, inclusiv dar nu limitat la forțele armate, poliție şi alte entități din domeniul aplicării legii, forțele paramilitare şi serviciile de informații şi securitate (atât civile cât şi militare), precum şi ii) toate organele executive, departamentele şi ministerele responsabile de coordonarea, controlul şi supravegherea forțelor de securitate”

PARTEA I. PRINCIPII GENERALE

Principiul 1: Dreptul la informație

a) Oricine are dreptul de a solicita, primi, folosi şi divulga informații deținute de autorități publice sau în numele acestora, ori la care autoritățile publice au dreptul legal de acces;

b) Principiile internaționale recunosc, de asemenea, că şi companiile private din sectorul securității naționale, inclusiv companiile private din domeniul militar sau de securitate, au responsabilitatea de a divulga informații cu privire la situații, activități sau acțiuni care au impact asupra exercițiului drepturilor omului, potrivit unor presupuneri rezonabile;

c) Cei care au obligația de a divulga informații potrivit principiilor 1 (a) şi 1 (b) trebuie să pună la dispoziție informația la cererecu doar unele excepții limitate, prevăzute de lege şi necesare pentru a preveni un prejudiciu specific şi identificabil la adresa unor interese legitime, inclusiv la adresa securitatății naționale;

d) Numai autoritățile publice ale căror atribuții specifice includ protecția securității naționale pot invoca securitatea națională ca motiv pentru refuzul de a divulga informații;

e) Orice invocare a securității naționale pentru a refuza divulgarea unor informații de către o companie privată trebuie în mod explicit autorizată şi confirmată de o autoritate publică însărcinată cu protecția securității naționale.

Notă: Autoritățile publice şi doar autoritățile publice poartă responsabilitatea finală pentru securitatea națională şi astfel doar guvernul poate declara că informația nu trebuie eliberată, dacă aceasta poate aduce atingere securității naționale.

f) Autoritățile publice au, de asemenea, obligația pozitivă de a publica din oficiu anumite informații de interes public.

Principiul 2: Aplicarea acestor principii

a) Aceste principii se aplică exercițiului dreptului la acces la informație identificat în Principiul 1 atunci când autoritățile publice

afirmă sau confirmă că divulgarea de informații poate cauza un prejudiciu securității naționale;

b) Având în vedere că securitatea națională este unul dintre cele mai importante motive publice pentru restricționarea accesului la informații, atunci când autoritățile publice susțin alte motive publice pentru restricționarea accesului – inclusiv relațiile internaționale, ordinea publică, sănătatea publică şi siguranța publică, aplicarea legii, acordarea unor opinii viitoare libere, formularea de politici eficiente şi interesele economice ale statului – ele trebuie să respecte cel puțin standardele impuse pentru restricționarea dreptului la acces la informație stabilite prin aceste principii, după caz;

c) Este o bună practică să existe o definiție precisă a securității naționale în legislația națională, în concordanță cu necesitățile unei societăți democratice, atunci când aceasta este folosită pentru a limita accesul la informație.

Principiul 3: Condiții pentru limitarea dreptului la informație din motive de securitate națională

Nu poate fi impusă nicio restricție privind dreptul la informație din motive de securitate națională, dacă guvernul nu poate demonstra că: (1) restricția (a) este prevăzută de lege şi (b) este necesară într-o societate democratică (c) pentru a proteja un interes legitim de securitate națională; şi (2) legea prevede garanții adecvate împotriva abuzurilor, inclusiv examinare promptă, completă, accesibilă şi efectivă a valabilității restricției de către o autoritate independentă de supraveghere, precum şi examinarea completă de către instanțele de judecată.

(a) Prevăzut de lege. Legea trebuie să fie accesibilă, lipsită de ambiguitate, elaborată cu atenție şi precizie, cu scopul de a permite persoanelor fizice să înțeleagă ce informație poate fi nedivulgată şi ce informație trebuie divulgată, precum şi care acțiuni privind informațiile sunt sancționate.

(b) Necesar într-o societate democratică.

(i) Divulgarea informației trebuie să prezinte un risc real şi identificabil al unui prejudiciu semnificativ pentru un interes legitim de securitate națională.

(ii) Riscul prejudiciului din motiv de divulgare trebuie să prevaleze asupra interesului public general de divulgare.

(iii) Restricția trebuie să respecte principiul proporționalității şi trebuie să fie mijlocul minim de restricție disponibil împotriva prejudiciului.

(iv) Restricția nu trebuie să compromită însăşi esența dreptului la informație.

(c) Protecția unui interes legitim de securitate națională. Categoriile restrânse de informații care pot fi nedivulgate din motive de securitate națională trebuie clar stabilite în lege.

Note: A se vedea definiția termenului "interes legitim de securitate națională" în secțiunea Definiții de mai sus. Principiul 3(b) este cu atît mai important în cazul în care securitatea națională nu este clar definită în lege, după cum se recomandă la principiul 2.

"Interes public" nu este definit în aceste principii. În principiul 10 este stabilită o listă de categorii de interes public de importan*ță deosebită care trebuie publicată în mod proactiv şi nu trebuie niciodată tăinuită. În principiul 37 este stabilită o listă de categorii de activități ilicite care prezintă un interest deosebit pentru public şi pe care funcționarii publici trebuie şi pot să le divulge fără frica de represalii.*

La echilibrarea riscului de prejudiciu împotriva interesului public în ceea ce priveşte divulgarea, trebuie să se țină cont de posibilitatea atenuării oricărui prejudiciu de pe urma divulgării, inclusiv prin mijloace care necesită cheltuieli rezonabile de fonduri. În continuare urmează o listă ilustrativă de factori care trebuie luată în considerare la luarea deciziei referitoare la interesul public pentru divulgare şi dacă acesta prevalează asupra riscului prejudiciului:

• *factori care favorizează divulgarea: este rezonabilă presupunerea că divulgarea poate (a) promova discuția transparentă a afacerilor publice (b) spori responsabilitatea guvernului (c) contribui la dezbateri pozitive şi informa referitor la probleme importante sau*

chestiuni de interes major, (d) promova supravegherea efectivă a cheltuielilor fondurilor publice, (e) dezvălui motivele pentru o hotărâre de guvern, (f) contribui la protecția mediului înconjurător, (g) dezvălui amenințări în ceea ce privește sănătatea sau siguranța publică sau (h) dezvălui sau ajuta la instituirea răspunderii pentru încălcări ale drepturilor omului sau ale dreptului umanitar internațional.

• *factori care favorizează nedivulgarea: divulgarea ar reprezenta, probabil, un risc real şi identificabil de prejudiciu adus unui interes legitim de securitate națională;*

• *factori care sunt irelevanți: divulgarea ar putea în mod rezonabil (a) cauza jenă sau pierderea încrederii în guvern sau într-un funcționar public sau (b) slăbi un partid politic sau o ideologie.*

Faptul că divulgarea ar putea aduce prejudiciu economiei unei țări ar putea fi relevant pentru a stabili dacă informația trebuie nedivulgată din acest motiv, dar nu din motive de securitate națională.

Principiul 4: Sarcina autorității publice de a stabili legitimitatea oricărei restricții

a) Sarcina demonstrării legitimității oricărei restricții este a autorității publice ce urmăreşte să limiteze accesul la informații;

b) Dreptul la informații trebuie interpretat şi aplicat în sens larg şi orice restricții trebuie interpretate restrâns;

c) În exercitarea acestei sarcini, nu este suficient ca o autoritate publică să se limiteze la a afirma că există riscul unui prejudiciu; autoritatea are obligația de a oferi motive specifice, de fond pentru a-şi susține afirmațiile;

Notă: Orice persoană care solicită acces la informație trebuie să beneficieze de o oportunitate echitabilă pentru a contesta temeiul revendicat la evaluarea riscurilor în fața unei autorități administrative şi judiciare, în conformitate cu principiile 26 şi 27.

d) In nici un caz nu poate fi considerata decisivă simpla emitere a unui act de către un ministru sau alt funcționar, în care se pretinde că divulgarea informației ar prejudicia securitatea națională.

Principiul 5: Nicio excepție pentru nicio autoritate publică

a) Nicio autoritate publică – inclusiv autoritatea judecătorească, legislativul, instituțiile de supraveghere, agențiile de informații, forțele armate, poliția, alte agenții de securitate, cabinetele şefului de stat şi al guvernului, precum şi orice birouri componente ale acestora – nu poate fi exceptată de la obligația de divulgare a informațiilor;

b) Securitatea națională nu constituie temei pentru nedivulgarea informației doar din simplu motiv că aceasta a fost generată de, sau în comun cu, un stat străin sau un organ inter-guvernamental sau o anumită autoritate publică sau o unitate în cadrul unei autorități.

Notă: În ceea ce privește informațiile generate de un stat străin sau un organ inter-guvernamental, a se vedea Principiul 9 (a) (v).

Principiul 6: Accesul la informație al organelorde supraveghere

Toate instituțiile de supraveghere, de petiționare [Avocatul poporului] şi de apel, inclusiv instanțele şi tribunalele, trebuie să aibă acces la toate informațiile relevante pentru îndeplinirea atribuțiilor lor, inclusiv informațiile de securitate națională, indiferent de nivelul de secretizare.

Notă: Acest principiu este descris în detaliu în Principiul 32. El nu se referă la divulgarea publică de către organele de supraveghere. Organele de supraveghere trebuie să mențină caracterul secret al tuturor informațiilor care au fost secretizate în mod legitim în conformitate cu aceste Principii, după cum este prevăzut în Principiul 35.

Principiul 7: Resurse

Statele trebuie să aloce resurse adecvate şi să ia alte măsuri necesare, precum adoptarea de reglementări şi buna administrare a arhivelor, pentru a se asigura că aceste Principii sunt respectate în practică.

Principiul 8: Starea de urgență

În timpul stării de urgență, care amenință existența națiunii, declarată oficial şi legal conform atât legislației naționale, cât şi celei internaționale, un stat poate deroga de la obligațiile sale privind drep-

tul de a solicita, primi şi disemina informaţii, numai în măsura în care acest lucru se impune de către exigenţele situaţiei şi numai când şi pentru atât timp cât derogarea este în concordanţă cu celelalte obligaţii ale statului potrivit dreptului internaţional şi nu implică niciun fel de discriminare.

Notă: Anumite aspecte legate de dreptul de a căuta, primi şi disemina informaţii şi idei sunt atât de fundamentale pentru a beneficia de drepturile inderogabile încât acestea ar trebui să fie întotdeauna pe deplin respectate, chiar şi în situaţii de urgenţă publică. Drept exemplu non-exhaustiv este o parte sau întreaga informaţie conţinută în principiul 10, care are un astfel de caracter.

PARTEA II. INFORMAŢII CARE POT FI NEDIVULGATE PE MOTIV DE SECURITATE NAŢIONALĂ ŞI INFORMAŢII CARE TREBUIE DIVULGATE

Principiul 9: Informaţia care în mod legitim poate fi nedivulgată

a) Autorităţile publice pot restricţiona dreptul publicului de acces la informaţii pe motiv de securitate naţională, dar numai dacă aceste restricţii respectă toate celelalte prevederi ale acestor Principii, informaţia este deţinută de o autoritate publică şi se încadrează într-una din următoarele categorii:

i) Informaţii despre planurile, operaţiunile şi capacităţile curente de apărare pe durata cât informaţia este de utilitate operaţională;

Notă: Expresia "pe durata în care informaţiile sunt de utilitate operaţională" are rolul de a solicita divulgarea de informaţii de îndată ce informaţiile nu mai dezvăluie ceva care ar putea fi folosit de inamici pentru a înţelege gradul de pregătire a statului, capacitatea sau planurile sale.

ii) Informaţii despre producţia, capabilităţile ori folosirea sistemelor de armament ori a altor sisteme militare, inclusiv a sistemelor de comunicaţii;

Notă: Asemenea informaţii includ date tehnologice şi invenţii, precum şi informaţii cu privire la producere, capabilităţi sau utilizare. Informaţii despre liniile bugetare referitoare la arme şi la alte sisteme militare ar trebui să fie puse la dispoziţia publicului. A se vedea Principiile 10C (3) şi 10F. Este o bună practică pentru state să menţină şi să publice o listă de control al armelor, după cum încurajază Tratatul privind Comerţul cu Arme referitor la armele convenţionale. De asemenea, este o bună practică de a publica informaţiile despre armele, echipamentele şi numerele trupelor.

iii) Informaţii despre măsurile specifice de protejare a teritoriului statului, infrastructura critică ori instituţiile naţionale critice *(institu-*

tion essentialles) împotriva ameninţărilor sau folosirii forţei sau sabotajului, a căror eficienţă depinde de caracterul lor secret;

Notă: Termenul de "infrastructură critică" se referă la resurse strategice, active şi sisteme, fizice sau virtuale, atât de vitale pentru stat încât distrugerea sau incapacitatea unor astfel de resurse, bunuri sau sisteme ar putea avea un impact debilitant asupra securităţii naţionale.

iv) Informaţii care se referă la sau derivă din operaţiile, sursele şi metodele serviciilor de informaţii, în măsura în care privesc chestiuni de securitate naţională şi

v) Informaţii care privesc chestiuni de securitate naţională care au fost oferite de un stat străin sau o structură inter-guvernamentală cu o aşteptare expresă de confidenţialitate ori alte comunicaţii diplomatice, în măsura în care privesc chestiuni de securitate naţională.

Notă: Este o bună practică ca astfel de aşteptări să fie înregistrate în scris.

Notă: În măsura în care informaţii specifice privind terorismul, precum şi măsurile de combatere a terorismului, sunt acoperite de una dintre categoriile de mai sus, dreptul publicului de a avea acces la astfel de informaţii poate fi supus unor restricţii pe motive de securitate naţională, în conformitate cu aceste şi alte prevederi ale principiilor. În acelaşi timp, unele informaţii cu privire la terorism sau la măsurile de combatere a terorismului ar putea fi de interes public deosebit de sporit: a se vedea de exemplu, principiile 10a, 10b, şi 10h (1).

b) Este o bună practică pentru legea naţională să prevadă o listă exhaustivă de categorii de informaţii, care sunt cel puţin la fel de restrâns definite precum categoriile de mai sus;

c) Un stat poate adăuga o categorie de informaţii la lista celor de mai sus, dar numai dacă categoria este identificată în mod specific şi definită în mod restrâns iar păstrarea caracterului secret al informaţiei este necesară pentru a proteja un interes legitim de securitate naţională care este prevăzut de lege, aşa cum se stabileşte în Principiul 2 c).

Atunci când propune categoria, statul trebuie să explice cum divulgarea informaţiei din acea categorie ar prejudicia securitatea naţională.

Principiul 10: Categorii de informaţii cu o prezumţie sporită sau de interes major în favoarea divulgării

Unele categorii de informaţii, inclusiv cele enumerate mai jos, sunt de interes public deosebit de mare, având în vedere importanţa lor majoră pentru procesul de supraveghere democratică şi pentru statul de drept. În consecinţă, există o prezumţie foarte puternică şi, în unele cazuri, un imperativ major, că astfel de informaţii ar trebui să fie publice şi divulgate în mod proactiv.

Următoarele categorii de informaţii trebuie să beneficieze de cel puţin o prezumţie sporită în favoarea divulgării şi pot fi nedivulgate pe motiv de securitate naţională numai în circumstanţe excepţionale şi de o manieră compatibilă cu alte principii, doar pentru o perioadă strict limitată de timp, numai în temeiul legii şi numai în cazul în care nu există mijloace rezonabile, prin care s-ar reduce prejudiciul care ar putea fi asociat cu divulgarea. Pentru anumite subcategorii de informaţii, specificate mai jos ca fiind supuse în mod inerent unui interes public superior în ceea ce priveşte divulgarea, nedivulgarea pe motive de securitate naţională niciodată nu poate fi justificată.

A. Încălcări ale drepturilor omului şi ale dreptului umanitar internaţional

1) Există un interes public mai important în favoarea divulgării informaţiilor privind încălcări grave ale drepturilor omului ori încălcări grave ale dreptului umanitar internaţional, incluzând crime potrivit dreptului internaţional şi încălcări sistematice şi răspândite ale drepturilor la libertate şi securitate personală. Astfel de informaţii nu pot fi refuzate la divulgare în nicio circumstanţă;

2) Informaţii privind alte încălcări ale drepturilor omului sau ale dreptului umanitar se prezumă a fi subiectul unei importante prezumţii în favoarea divulgarii şi, în orice caz, nu pot fi refuzate la divul-

gare pe motive de securitate națională într-o manieră care ar preveni tragerea la răspundere a celor vinovați sau ar priva victima de accesul la un remediu eficient;

3) Când un stat trece printr-un proces de justiție de tranziție în timpul căruia statul are în special o obligație de a asigura aflarea adevărului, justiția, reparația şi garanții de ne-repetare, există un interes public mai important pentru divulgare, către societate în ansamblul ei, de informații privind încălcarea drepturilor omului de către fostul regim.Un guvern succesor ar trebui să protejeze imediat şi să păstreze integritatea, eliberând fără întârziere orice înregistrare care conține astfel de informații tăinuite de către un guvern anterior.

Notă: A se vedea principiul 21 (c) în ceea ce priveşte obligația de a căuta sau reconstitui informații despre încălcările drepturilor omului.

4) Atunci când existența încălcărilor este contestată sau suspectată, dar nu deja stabilită, acest Principiu se aplică informației care, de sine stătătoare sau împreună cu alte informații, ar aduce lumină cu privire la adevărul despre presupusele încălcări.

5) Acest Principiu se aplică informațiilor despre încălcări care s-au petrecut sau se petrec şi se aplică indiferent dacă încălcările au fost înfăptuite de statul care deține informațiile sau de către alții;

6) Informațiile privind încălcările prevăzute de acest Principiu includ, fără limitare, următoarele:

a) O descriere completă şi orice înregistrări care demonstrează actele sau omisiunile care constituie încălcarea, precum şi datele şi circumstanțele în care s-au petrecut şi, după caz, localizarea oricărei persoane dispărute sau a rămăşițelor umane;

b) Identitatea tuturor victimelor, atât timp cât se respectă dreptul la viață privată şi alte drepturi ale victimelor, rudelor lor şi a martorilor, precum şi date agregate sau anonimizate în alt mod privind numărul şi caracteristice victimelor care pot fi relevante în apărarea drepturilor omului;

Notă: Numele şi alte date personale ale victimelor, rudelor acestora şi martorilor pot fi nedivulgate publicului larg în măsura în care este necesară prevenirea de noi prejudicii aduse acestora, dacă persoanele în cauză sau, în cazul persoanelor decedate, membrii familiilor lor, solicită în mod expres şi voluntar nedivulgarea sau nedivulgarea este, de altfel, în mod evident în concordanță cu propriile dorințe ale persoanei sau cu nevoile speciale ale grupurilor vulnerabile. În ceea ce priveşte victimele violenței sexuale, ar trebui să fie necesar acordul lor expres în divulgarea numelor lor şi a altor date personale. Victimele copii (sub 18 ani) nu ar trebui să fie identificate pentru publicul larg. Cu toate acestea, acest principiu ar trebui să fie interpretat, având în vedere realitatea că diferite guverne în diverse perioade au ecranat de ochii publicului încălcări ale drepturilor omului prin invocarea dreptului la viața privată, inclusiv a persoanelor ale căror drepturi sunt sau au fost încălcate în mod grosolan, fără a ține seama de adevăratele dorințe ale persoanelor afectate. Cu toate acestea, aceste limitări nu ar trebui să împiedice publicarea de date agregate sau anonime într-un mod diferit.

c) Numele instituțiilor şi persoanelor care au comis sau au fost în alt mod responsabile de încălcări şi, în general, a oricăror unități ale sectorului de securitate prezente la momentul încălcărilor sau implicate în orice alt mod, precum şi al superiorilor şi al comandanților şi informații privind domeniul lor de comandă şi controlul;

d) Informații privind cauzele încălcărilor şi eşecul în a le preveni.

B. Garanții pentru dreptul la libertatea şi securitatea persoanei, prevenirea torturii şi a altor rele tratamente şi ale dreptului la viață

Informațiile acoperite de acest Principiu includ:

1) Legile şi reglementările care autorizează privarea de viață a unei persoane de către stat şi legile şi reglementările privind privarea de libertate, inclusiv cele care se referă la motivele, procedurile, transferurile, tratamentul sau condițiile de detenție ale persoanelor afectate, inclusiv metodele de interogare. Există un interes public mai

important [decât protecția securității naționale] în divulgarea acestor legi şi reglementări.

Notă: Noțiunea de „legi si regulamente", așa cum este folosită în principiul 10, include toată legislația primară sau conexă, statute, regulamente, şi hotărîri, precum si decretele şi hotărîrile executive emise de un preşedinte, un prim ministru, ministru sau altă autoritate publică şi hotărîrile judecătoreşti definitive şi executorii. Noțiunea de „legi şi regulamente" include, de asemenea, orice reguli sau interpretări ale legislației considerate relevante de către autoritățile publice.

Privațiunea de libertate include orice formă de arest, detenție, închisoare sau internare.

2) Amplasarea tuturor locurile în care persoanele sunt private de libertate operate de către sau în numele statului, precum şi identitatea, şi acuzațiile aduse împotrivă sau motivele detenției tuturor persoanelor private de libertate, inclusiv în timpul unui conflict armat.3) Informații privind moartea în custodie a oricărei persoane şi informații privind orice altă privare de viață de care statul este responsabil, inclusiv identitatea persoanei sau persoanelor ucise, circumstanțele decesului lor şi localizarea rămăşițelor lor.

Notă: În niciun caz nu pot fi tăinuite informații pe motive de securitate națională care ar duce la detenția secretă a unei persoane sau la înființarea şi funcționarea de locuri secrete de detenție, sau la execuții secrete. De asemenea, nu există nicio circumstanță în care soarta sau locul în care orice persoană privată de libertate de către sau cu autorizația, sprijinul, sau consimțământul expres sau tacit, statul le poate ascunde sau refuza în alt mod, membrilor familiei persoanei sau pe alții care au un legitim interes pentru bunăstarea persoanei.

Numele şi alte date cu caracter personal ale persoanelor care au fost private de libertate, care au murit în arest sau ale căror decese au fost cauzate de agenți de stat, pot fi tăinuite publicului larg în măsura necesară pentru a proteja dreptul la viață privată, dacă

persoanele în cauză sau membrii familiilor lor, în cazul persoanelor decedate, solicită în mod expres şi voluntar nedivulgarea şi dacă nedivulgarea este în alt mod în concordanță cu drepturile omului. Identitatea copiilor privați de libertate nu ar trebui să fie pusă la dispoziția publicului larg. Cu toate acestea, aceste limitări nu ar trebui să împiedice publicarea de date agregate sau anonime într-un alt mod.

C. Structura şi atribuțiile Guvernului

Informațiile acoperite de acest Principiu includ, dar nu se limitează la, următoarele:

1) Existența tuturor autorităților militare, polițieneşti, de securitate şi de informații şi a subunităților;

2) Legile şi reglementările aplicabile acestor autorități şi organelor lor de supraveghere şi mecanismele interne de responsabilizare şi raportare, , precum şi numele oficialilor care conduc astfel de autorități;

3) Informațiile necesare pentru evaluarea şi controlul cheltuirii fondurilor publice, inclusiv bugetul total, principalele linii bugetare şi informații de bază despre cheltuieli ale acestor autorități;

4) Existența şi termenii înțelegerilor bilaterale şi multilaterale încheiate şi alte angajamente internaționale importante ale statului în chestiuni de securitate națională.

D. Deciziile de a aplica forța militară sau de a achiziționa arme de distrugere în masă

1) Informațiile prevăzute de acest Principiu includ informații relevante pentru decizia de a angaja trupe de luptă sau de a întreprinde o altă acțiune militară, inclusiv confirmarea faptului că o asemenea acțiune a fost întreprinsă, domeniul general şi extensiunea sa generală, o explicație a justificării acesteia, precum şi orice informație care demonstrează că un fapt afirmat în cadrul motivării publice a fost greşit;

Notă: Referirea la dimensiunea "generală" a acțiunii şi la domeniul de aplicare admite faptul că, în general, ar trebui să fie

posibilă satisfacerea interesului public sporit de a avea acces la informațiile relevante pentru decizia de angajare a trupelor de luptă fără a dezvălui toate detaliile cu privire la aspectele operaționale ale acțiunii militare în cauză (a se vedea Principiul 9).

2) Posesia sau achiziția de arme nucleare ori alte arme de distrugere în masă de către un stat, dar nu în mod necesar detalii despre producția lor sau capabilitățile operaționale, este o chestiune de interes public de cea mai mare importanță şi nu trebuie ținută secretă.

Notă: Acest sub-principiu nu ar trebui să fie interpretat ca susținere, în orice mod, a achiziției unor astfel de arme.

E. Supravegherea

1) Cadrul legal general privind supravegherea de orice fel, precum şi procedurile care trebuie urmate pentru autorizarea supravegherii, stabilirea țintelor supravegherii, precum şi pentru folosirea, schimbul, păstrarea şi distrugerea materialului de interceptare trebuie să fie accesibile publicului.

Notă: Aceste informații includ: (a) legislația care reglementează toate formele de supraveghere, atât cele secrete, cât şi deschise, inclusiv supravegherea indirectă, cum ar fi crearea de profiluri şi extragerea datelor, precum şi tipurile de măsuri de supraveghere care pot fi folosite; (b) obiectivele de supraveghere admise; (c) plafonul de suspiciune necesar pentru a iniția sau continua supravegherea; (d) limite privind durata măsurilor de supraveghere; (e) proceduri de autorizare şi revizuire a utilizării unor astfel de măsuri; (f) tipurile de date cu caracter personal care pot fi colectate şi/sau prelucrate în scopurile securității naționale şi (g) criteriile care se aplică la utilizarea, păstrarea, ştergerea şi transferul acestor date.

2) Publicul trebuie să aibă de asemenea acces la informațiile despre entitățile autorizare să realizeze supravegherea şi statisticile privind folosirea supravegherii.

Note: Aceste informații conțin identitatea fiecărei entități guvernamentale care a acordat autorizație specifică pentru a efectua o

anumită supraveghere în fiecare an, numărul de autorizații de supraveghere acordate în fiecare an pentru orice entitate de acest gen; cele mai bune informații disponibile cu privire la numărul de persoane şi numărul de comunicări care fac obiectul supravegherii în fiecare an; iar în cazul în care vreo supraveghere a fost efectuată fără autorizație specifică - de către ce entitate guvernamentală.

Dreptul publicului de a fi informat nu se extinde în mod necesar asupra faptului sau asupra detaliilor operaționale de supraveghere efectuată în conformitate cu legea şi cu obligațiile privind drepturile omului. Asemenea informații pot fi nedivulgate publicului, precum şi cele care fac obiectul supravegherii cel puțin până la momentul încheierii perioadei de supraveghere.

3) În plus, publicul trebuie să fie informat complet despre situația oricărei supravegheri ilegale. Informațiile despre asemenea supraveghere trebuie să fie dezvăluite la amploarea maximă fără a se încălca dreptul la viață privată al celor supuşi supravegherii;

4) Aceste principii privesc dreptul publicului de a accesa informații şi nu prejudiciază drepturile substanțiale şi procedurale suplimentare ale persoanelor care au fost sau cred că au fost supuse supravegherii;

Notă: Este o bună practică de a obliga autoritățile publice să informeze persoanele care au fost supuse unei supravegheri secrete (oferind, cel puțin, informații cu privire la tipul de măsuri care au fost utilizate, datele şi organul responsabil pentru autorizarea măsurii de supraveghere) în măsura în care acest lucru se poate face fără a pune în pericol operațiunile sau sursele şi metodele în curs de desfăşurare.

5) Prezumția importantă în favoarea divulgării recunoscută de acest Principiu nu se aplică la informații care se referă în exclusivitate la supravegherea activității guvernelor străine.

Notă: Informațiile obținute prin intermediul supravegherii secrete, inclusiv a activităților guvernelor străine, ar trebui să fie subiectul unei divulgări în circumstanțele identificate în principiul 10A.

F. Informații financiare

Informațiile prevăzute de acest Principiu includ informații suficiente pentru a permite publicului să înțeleagă finanțele sectorului de securitate, precum şi regulile care guvernează finanțele sectorului de securitate. Astfel de informații includ, fără a se limita la:

1) Bugetele departamentelor şi agențiilor cu linii bugetare;
2) Situațiile financiare anuale cu linii bugetare;
3) Regulile de management financiar şi mecanismele de control;
4) Regulile de achiziții şi
5) Rapoartele instituțiilor supreme de audit şi ale altor entități responsabile de controlul aspectelor financiare ale sectorului de securitate, inclusiv rezumate ale oricăror secțiuni ale unor astfel de rapoarte care sunt secretizate.

G. Răspunderea pentru încălcări ale Constituției şi ale legii, precum şi alte abuzuri de putere

Informația acoperită de acest principiu include informația cu privire la existența, natura şi dimensiunea încălcărilor constituționale sau ale celor prevăzute de lege, precum şi alte abuzuri de putere din partea autorităților publice sau a personalului.

H. Sănătatea publică, siguranța publică sau mediul înconjurător

Informațiile prevăzute de acest Principiu includ:

1) În cazul oricărui pericol iminent sau real la adresa sănătății publice, a siguranței publice sau a mediului, toate informațiile care pot permite publicului să înțeleagă sau să ia măsuri pentru a preveni sau reduce prejudiciul rezultat din acea amenințare, indiferent că pericolul este datorat cauzelor naturale sau activităților umane, inclusiv acțiunilor statului sau ale companiilor private;

2) Alte informații, actualizate în mod regulat, despre exploatarea resurselor naturale, poluare şi inventarele de emisii, impactul de mediu al marilor lucrări publice sau extracții de resurse existente sau propuse, precum şi evaluarea de risc şi planurile de managementpentru instalațiile în special periculoase..

PARTEA III. A: REGULI PRIVIND SECRETIZAREA ŞI DESCRETIZAREA INFORMAȚIEI

Principiul 11: Obligația de a declara motivele pentru secretizarea informației

a) Indiferent dacă un stat are un proces formal de secretizare, autoritățile publice sunt obligate să declare motivele pentru secretizarea informațiilor;

Notă: "Secretizarea" este procesul prin care sunt revizuite înregistrările care conțin informații sensibile şi este stabilit un indiciu care să precizeze cine ar putea avea acces la ele şi modul în care poate fi administrată înregistrarea. Este o bună practică de a institui un sistem formal de secretizare în scopul de a reduce arbitrarul şi nedivulgarea excesivă.

b) Motivele trebuie să indice categoria restrânsă de informații, corespunzătoare uneia dintre categoriile enumerate la Principiul 9, în care se încadrează informația, precum şi să descrie prejudiciul care ar putea rezulta din divulgare, inclusiv nivelul de gravitate şi nivelul de verosimilitate;

c) Nivelurile de secretizare, dacă sunt folosite, trebuie să corespundă nivelurilor şi verosimilității prejudiciului identificate în justificare;

d) Când informația este secretizată, i) un marcaj protector trebuie să fie adăugat înregistrării, indicând nivelul, dacă există, şi durata maximă de secretizare şi ii) trebuie inclusă o declarație care justifică necesitatea secretizării la acel nivel şi pentru acea durată.

Notă: Este încurajată oferirea unei declarații care să justifice fiecare decizie de secretizare, deoarece aceasta determină funcționarii de stat să acorde atenție prejudiciului specific care ar rezulta din divulgare şi facilitează procesul de desecretizare şi divulgare. Marcarea alineat-cu-alineat asigură ulterior coerență procesului de divulgarea a porțiunilor nesecretizate de documente.

Principiul 12: Accesul public la regulile de secretizare

a) Publicul trebuie să aibă posibilitatea de a comenta procedurile şi standardele care guvernează secretizarea înainte ca ele să devină aplicabile;

b) Publicul trebuie să aibă acces la procedurile şi standardele scrise care guvernează secretizarea.

Principiul 13: Autoritatea de a secretiza

a) Numai oficialii special autorizaţi sau desemnaţi în conformitate cu legea pot secretiza informaţiile. Dacă un oficial nedesemnat crede că informaţia trebuie secretizată, informaţia poate fi considerată secretizată pentru o perioadă de timp scurtă şi expres definită până un oficial desemnat a analizat recomandarea de secretizare;

Notă: În lipsa unor prevederi legale care să controleze autoritatea de a secretiza, este o practică bună de a specifica, cel puţin, întrun regulament o astfel de autoritate delegată.

b) Identitatea persoanei responsabile de decizia de secretizare trebuie să fie indicată sau identificabilă pe document, pentru a asigura responsabilitatea, cu excepţia cazului când există motive convingătoare pentru a ascunde identitatea;

c) Oficialii desemnaţi prin lege trebuie să atribuie autoritatea originală de secretizare unui număr cât mai mic, eficient din punct de vedere administrativ, de subordonaţi de rang înalt.

Notă: Este o bună practică de a publica informaţiile despre numărul de persoane care au autoritatea de a secretiza, precum şi numărul de persoane care au acces la informaţiile secretizate.

Principiul 14: Facilitarea contestărilor interne la secretizare

Personalul public, inclusiv cei afiliaţi sectorului de securitate, care crede că informaţia a fost impropriu secretizată, poate contesta secretizarea informaţiei.

Notă: Personalul angajat în sectorul de securitate este primul care trebuie încurajat să conteste secretizarea, având în vedere creşterea sporită de secretizare în agenţiile de securitate, faptul că cele mai multe ţări nu au stabilit sau desemnat o structură independentă care să primească plângeri din partea personalului angajat în sectorul de securitate, precum şi faptul că divulgarea de informaţii referitor la securitate de multe ori duce la sancţiuni mai mari decât divulgarea altor informaţii.

Principiul 15: Obligaţia de a păstra, administra şi conserva informaţii de securitate naţională

a) Autorităţile publice au obligaţia de a păstra, administra şi conserva informaţiile conform standardelor internaţionale[1]. Informaţia poate fi exceptată de la păstrare, administrare şi conservare numai în conformitate cu legea.

b) Informaţia trebuie administrată corespunzător. Sistemele de îndosariere trebuie să fie consecvente, transparente (fără a dezvălui informaţii secretizate legitim) şi complete, astfel încât cererile specifice de acces să ducă la identificarea tuturor informaţiilor relevante chiar dacă informaţia nu este divulgată;

c) Fiecare entitate publică trebuie să creeze şi să facă publică, precum şi să revizuiască şi să actualizeze periodic, o listă detaliată şi corectă a documentelor secretizate pe care le deţine, mai puţin a acelor documente cu caracter excepţional a căror simplă existenţă nu poate fi dezvăluită legitim conform Principiului 19, dacă acestea există.

Notă: Este o practică bună de a actualiza anual aceste liste.

---

1. Acestea includ: Consiliul Internaţional al Arhivelor (CAI), *Principii de acces la arhive: (2012*); CAI,
Declaraţia Universală privind Arhivele (2010; aprobată de UNESCO); Consiliul Europei, *Recomandarea nr*
R (2000) 13 privind o politică europeană privind accesul la arhive (2000); Antonio González Quintana, CAI, *Politici privind arhivele în protecţia drepturilor omului*: o versiune actualizată şi mai completă a raportului întocmit de către UNESCO şi Consiliul Internaţional al Arhivelor (1995), privind gestionarea Arhivelor serviciilor de securitate de stat ale fosteilor regimuri represive (2009).

Principiul 16: Limite de timp pentru perioada de secretizare

a) Informația poate fi refuzată de la divulgare pe motive de securitate națională numai atât timp cât este necesar pentru a proteja interesul legitim de securitate națională. Deciziile de a refuza divulgarea trebuie să fie revizuite periodic pentru a asigura respectarea acestui Principiu;

Notă: Este o practică bună ca revizuirea să fie solicitată prin statut cel puțin o dată la cinci ani. Mai multe țări solicită revizuirea în perioade mai scurte de timp.

b) Cel care secretizează trebuie să specifice data, condițiile sau evenimentul când secretizarea se încheie;

Notă: Este o practică bună ca această limită de timp sau specificarea unor condiții, sau evenimentul când expiră secretizarea să fie supuse unor revizuiri periodice.

c) Nicio informație nu poate rămâne secretizată pe durată nedeterminată. Perioada prezumtivă maximă de secretizare pe motive de securitate națională trebuie stabilită prin lege;

d) Informația poate fi restricționată dincolo de prezumtivul termen limită numai în circumstanțe excepționale, potrivit unei noi decizii de a restricționa accesul, luată de altă factor de decizie, care să stabilească un nou termen.

Principiul 17: Proceduri de desecretizare

a) Legislația națională trebuie să stabilească responsabilitatea Guvernului de a coordona, superviza şi implementa activitățile guvernamentale de desecretizare, inclusiv îmbunătățirea şi actualizarea regulată a instrucțiunilor de desecretizare.

b) Trebuie stabilite proceduri pentru identificarea informațiilor de interes public secretizate pentru desecretizare prioritară. Dacă informațiile de interes public, inclusiv informațiile care se încadrează într-una din categoriile enumerate în Principiul 10, sunt secretizate datorită unor sensibilități excepționale, ele trebuie desecretizate cât de repede posibil;

c) Legislația națională trebuie să stabilească proceduri pentru desecretizarea în bloc;

d) Legislația națională trebuie să stabilească perioade fixe pentru desecretizarea automată pentru diferite categorii de informații secretizate. Pentru a scădea povara desecretizării, informațiile trebuie desecretizate automat, fără examinare, oricând este posibil;

e) Legislația națională trebuie să stabilească o procedură accesibilă şi publică pentru cererile de desecretizare a documentelor;

f) Documentele desecretizate, inclusiv cele desecretizate de către instanțe de judecată, tribunale sau alte organe de supraveghere, avocați parlamentari sau instanțe de apel ar trebui să fie dezvăluite în mod proactiv sau puse la dispoziția publicului într-un alt mod (de exemplu, prin armonizarea legislației în domeniul arhivelor naționale sau privind accesul la informații, sau ambelor).

Notă: Acest principiu nu aduce atingere prevederii cu privire la alte motive de nedivulgare prevăzute în preambulul paragrafului 15.

Notă: Bune practici adiționale includ următoarele:

• examinarea periodică a utilizării noilor tehnologii în procesele de desecretizare; şi

• consultări regulate cu persoane cu experiență profesională în ceea ce priveşte procesul de stabilire a priorităților de desecretizare, inclusiv atât desecretizarea automate, cât şi în bloc.

PARTEA III. B: REGULI CU PRIVIRE LA ADMINISTRAREA CERERILOR DE INFORMAȚII

Principiul 18: Obligația de a lua în considerare cererea, chiar dacă informația a fost secretizată

Faptul că informația a fost secretizată nu este decisiv în determinarea modului de a răspunde la o cerere pentru acea informație. Autoritatea publică ce deține informația trebuie să ia în considerare cererea potrivit acestor Principii.

Principiul 19: Obligația de a confirma sau infirma

a) La primirea unei cereri de informații, autoritatea publică trebuie să confirme sau să nege dacă deține informația solicitată.

b) Dacă într-un sistem de drept există posibilitatea ca, în circumstanțe extraordinare, să se secretizeze însăşi existența sau inexistența unei anumite informații conform Principiului 3, atunci refuzul de a confirma sau nega existența informației ca răspuns la o anumită cerere trebuie să se bazeze pe arătarea motivelor pentru care simpla confirmare sau negare a existenței informației ar pune în pericol o categorie distinctă de informații care este stabilită că necesită un asemenea tratament excepțional în legislația națională.

Principiul 20: Obligația de expunere în scris a motivelor refuzului

a) Dacă o autoritate publică refuză o solicitare de informații , în întregime sau în parte, ea ar trebui să precizeze în scris motivele specifice pentru aceasta, în conformitate cu Principiile 3 şi 9, în termenul specificat de lege pentru a răspunde la solicitarea de informații;

Notă: A se vedea Principiul 25 în care perioada de timp în care trebuie să fie dat răspunsul trebuie să fie prevăzută prin lege.

b) Autoritatea trebuie de asemenea să ofere solicitantului suficiente informații privind funcționarul/funcționarii care au autorizat refuzul şi procesul prin care care s-a ajuns la refuz, doar dacă aceasta prin sine însăşi nu ar dezvălui informații secretizate, precum şi căile de atac, pentru a permite examinarea respectării legii de către autoritate.

Principiul 21: Obligația de a recupera sau de a reconstitui informația lipsă

a) Când o autoritate publică nu poate localiza informația care ar răspunde unei cereri iar înregistrările conținând informația ar fi trebuit sa fie conservate, colectate sau produse, autoritatea trebuie să facă eforturi rezonabile pentru a recupera sau reconstitui informația în scopul unei potențiale divulgări către solicitant;

Notă: Acest principiu se aplică pentru informații care nu pot fi localizate dintr-un anumit motiv, de exemplu, pentru că niciodată nu au fost colectate, au fost distruse sau sunt nedetectabile.

b) Un reprezentant al autorității publice poate fi solicitat ca sub jurământ şi într-un timp rezonabil şi prevăzut legal să indice toate procedurile îndeplinite pentru a încerca să recupereze sau să reconstituie informația într-un mod în care să permită ca acele proceduri să fie supuse controlului judecătoresc;

Notă: Atunci când nu pot fi găsite informațiile care trebuie să fie menținute prin lege, problema ar trebui să fie adresată poliției sau autorităților administrative pentru investigație. Rezultatul investigației trebuie să fie făcut public.

c) Obligația de a recupera sau reconstitui informația este în mod special importantă i) când informația se referă la presupuse grave şi sistematice încălcări ale drepturilor omului şi/sau ii) în timpul tranziției către o formă democratică de guvernământ de la o guvernare caracterizată de largi încălcări ale drepturilor omului.

Principiul 22: Obligația de a divulga parți ale documentelor

Excepții de la divulgare se aplică numai informațiilor specifice şi nu documentelor întregi sau altor înregistrări. Pot fi nedivulgate numai informații specifice a căror validitate de restricție a fost demonstrată („informații excepții"). În cazul în care o înregistrare conține atât informații excepții, cât şi informații care nu constituie excepții, autoritățile publice au obligația de a extrage şi divulga informațiile care nu constituie excepții.

Principiul 23: Obligația de a identifica informația nedivulgată

O autoritate publică care deține informații pe care refuză să le divulge trebuie să identifice acele informații pe cât de specific posibil. Cel puțin autoritatea trebuie să dezvăluie cantitatea de informație pe care refuză să o dezvăluie, de exemplu prin estimarea numărului de pagini.

Principiul 24: Obligația de a furniza informația în formatul disponibil

Autoritățile publice trebuie să furnizeze informațiile în formatul preferat de solicitant în măsura în care aceasta este posibil.

Notă: Aceasta include, de exemplu, obligația autorităților publice de a lua măsuri corespunzătoare pentru a furniza informații persoanelor cu dizabilități, în format şi tehnologii accesibile, în timp util şi fără costuri suplimentare, în conformitate cu Convenția ONU privind drepturile persoanelor cu dizabilități.

Principiul 25: Termene limită pentru a răspunde la solicitările de informații

a) Termenele pentru răspunsul la solicitări, inclusiv pe fond, pentru controlul intern, pentru decizia organului independent, dacă acesta există, şi pentru controlul judiciar trebuie stabilite de lege şi trebuie să fie, pe cât este practic posibil, cât mai scurte;

Notă: În conformitate cu cerințele stabilite în cele mai multe legi privind accesul la informații, cea mai bună practică este considerată de a prevedea douăzeci de zile lucrătoare sau mai puțin drept perioadă de timp în care trebuie acordat un răspuns de fond. În cazul în care termenele limită pentru a răspunde solicitărilor nu sunt prevăzute în lege, termenul limită ar trebui să fie de cel mult 30 de zile pentru o cerere standard. Legile pot să prevadă termene limite diferite, luând în considerare diferite volume şi niveluri de complexitate şi sensibilitate ale documentelor.

b) Termene scurte trebuie să se aplice atunci când există o necesitate demonstrată pentru informație în regim de urgență, cum ar fi

atunci când informația este necesară pentru apărarea vieții sau libertății unei persoane.

Principiul 26: Dreptul la revizuirea deciziei de nedivulgare a informației

a) Un solicitant are dreptul la o revizuire rapidă şi ieftină a refuzului de divulgare a informației sau a chestiunilor legate de cerere de către o autoritate independentă;

Notă: Un refuz poate presupune un refuz implicit sau tăcut. Taxele, termenele limite şi formatul constituie aspecte care fac obiectul unei revizuiri de către o autoritate independentă.

b) Autoritatea independentă trebuie să aibă competența şi resursele necesare pentru a asigura revizuirea eficientă, inclusiv acces complet la informațiile relevante, chiar dacă acestea sunt secretizate;

c) O persoană trebuie să aibă dreptul de a obține revizuirea independentă şi efectivă a tuturor aspectelor relevante de către o instanță competentă sau de către tribunal.

d) În cazul în care o instanță pronunță o hotărâre conform căreia nedivulgarea informațiilor este justificată, aceasta ar trebui să facă publice în scris motivele factual-specifice şi analiza sa juridică, cu excepția unor circumstanțe extraordinare şi în conformitate cu Principiul 3.

PARTEA IV. ASPECTE JUDICIARE ALE SECURITĂȚII NAȚIONALE ŞI DREPTUL LA INFORMAȚIE

Principiul 27: Principiul de supraveghere judiciară generală

a) Invocarea securității naționale nu poate fi folosită pentru a submina dreptul fundamental la un proces echitabil din partea unui tribunal competent, independent şi imparțial, stabilit de lege;

b) Atunci când o autoritate publică urmăreşte să refuze divulgarea de informații pe motivul securității naționale în cadrul oricăror proceduri legale, o instanță trebuie să aibă competența de a examina informația pentru a determina dacă informația poate rămâne nedivulgată. Instanța nu trebuie să respingă contestația fără să examineze informația;

Notă: În conformitate cu Principiul 4 (d), instanța nu trebuie să se bazeze pe rezumate sau declarații care doar afirmă necesitatea de a păstra secretul, fără a oferi o bază probatorie pentru afirmație.

c) Instanța trebuie să se asigure că persoana solicitantă poate, pe cât mai mult posibil, să ştie şi să combată susținerile guvernului pentru a nu divulga informația;

d) Instanța trebuie să se pronunțe asupra legalității şi temeiniciei susținerilor guvernului şi poate ordona divulgarea sau măsurile compensatorii potrivite în cazul unei nedivulgări parțiale sau totale, inclusiv respingerea acuzațiilor în proceduri penale.

e) Instanța trebuie să evalueze independent dacă autoritatea a invocat temeinic orice motiv de nedivulgare; faptul secretizării nu trebuie să fie decisiv pentru nedivulgarea informației. În mod similar, instanța trebuie să evalueze natura oricărui prejudiciu invocat de autoritatea publică, şansele ca acesta să se petreacă şi interesul public pentru divulgare, în conformitate cu standardele prevăzute de Principiul 3.

Principiul 28: Accesul public la procesele judiciare

a) Invocarea securității naționale nu poate fi motiv de subminare a dreptului fundamental al publicului de a avea acces la procesele judiciare;

b) Hotărârile judecătoreşti – cuprinzând toate dispozițiile instanței, inclusiv principalele concluzii, probe şi motivări legale – trebuie făcute publice, mai puțin atunci când interesele copiilor sub 18 ani o impun;

Note: Dreptul internațional nu permite nicio derogare, pe motive de securitate națională, de la obligația de a pronunța hotărâri în mod public.

Nu trebuie să fie făcute publice înregistrări ale procedurilor judiciare cu minori. Înregistrări ale altor proceduri judiciare care implică copiii în mod normal trebuie să stilizeze numele şi alte informații de identificare a copiilor sub vârsta de optsprezece ani.

c) Dreptul publicului de acces la justiție trebuie să includă accesul public prompt la: a) motivarea judecătorească; ii) informații despre existența şi progresul cauzelor; iii) argumentele aduse în fața instanței; iv) şedințele de judecată şi procesele; v) dovezile din cadrul procedurilor în instanță care stau la baza unei condamnări, cu excepția când o derogare de la aceasta este justificată în conformitate cu prezentele Principii;

Notă: Într-o societate democratică dreptul internațional privind cerințele unui proces echitabil permite instanțelor să excludă de la şedință publicul, în totalitate sau parțial, din motive de securitate națională, precum şi de moralitate, de ordine publică, în interesul vieții private a părților sau pentru a evita să aducă atingere intereselor justiției, cu condiția că aceste restricții sunt în toate cazurile necesare şi proporționale.

d) Publicul trebuie să aibă oportunitatea de a contesta orice susținere a autorității publice că o restricție a accesului public la procesele judiciare este strict necesară pe motive de securitate națională;

e) Atunci când o instanță dispune o restricționare a accesului la procesele judiciare, trebuie să facă disponibile public în scris motivele de fapt şi de drept ale deciziei, cu excepția circumstanțelor extraordinare, conforme cu Principiul 3.

Note: Acest principiu nu urmăreşte să modifice legea existentă a

unui stat în ceea ce priveşte procedurile preliminare la care publicul, de obicei, nu are acces. El se aplică doar atunci când procesul de judecată ar permite în alt mod accesul publicului şi încercarea de a îngrădi accesul se bazează pe o invocare a securităţii naţionale.

Dreptul publicului de a avea acces la procedurile judiciare şi la materiale derivă din importanţa accesului în promovarea (i) caracterului echitabil real şi perceput şi imparţialitatea procedurilor judiciare; (ii) comportamentului corespunzător şi mai onest al părţilor, precum şi (iii) corectitudinea consolidată a comentariilor publice.

Principiul 29: Accesul părţii la informaţie în cadrul procedurilor penale

a) Instanţa nu poate interzice unui inculpat să participe la propriul proces pe motive de siguranţă naţională;

b) În nicio situaţie o condamnare sau privare de libertate nu poate fi bazată pe probe pe care inculpatul nu a avut posibilitatea de a le cunoaşte şi contesta;

c) În interesul justiţiei, autorităţile publice trebuie să pună la dispoziţia inculpatului şi ale apărătorilor lui acuzaţiile împotriva unei persoane şi orice informaţie necesară pentru a asigura dreptul la un proces echitabil, indiferent dacă informaţiile sunt secretizate, în conformitate cu Principiile 3-6, 10, 27 şi 28, inclusiv prin considerarea interesului public.

d) Atunci când o autoritate publică refuză să divulge informaţiile necesare asigurării unui proces echitabil, instanţa trebuie să suspende sau să respingă acuzaţiile.

Notă: Autorităţile publice nu trebuie să se bazeze pe informaţii în beneficiul lor atunci când pretind păstrarea secretului, deşi ele pot decide asupra păstrării secretului informaţiilor şi a suportării consecinţelor.

Notă: Principiile 29 şi 30 sunt incluse în aceste principii în ceea ce priveşte accesul publicului la informaţii având în vedere faptul că

revizuirea judiciară, precum şi divulgările conexe în contextul supravegherii judiciare de multe ori constituie mijloace importante pentru divulgarea publică a informaţiilor.

Principiul 30: Accesul părţii la informaţie în cauzele civile

a) Toate susţinerile privind refuzul unei autorităţi publice de a divulga informaţii într-o cauză civilă trebuie să fie supusă controlului într-o manieră conformă cu Principiile 3-6, 10, 27 şi 28, inclusiv prin considerarea interesului public.

b) Victimele încălcărilor drepturilor omului au dreptul la remedii şi reparaţii efective, inclusiv la divulgarea publică a abuzurilor suferite. Autorităţile publice nu pot refuza informaţii relevante pentru cauza lor într-un mod contrar acestui drept;

c) Publicul are de asemenea dreptul la informaţii privind încălcări grave ale drepturilor omului şi ale dreptului internaţional umanitar.

PARTEA V. ORGANE DE SUPRAVEGHERE A SECTORULUI DE SECURITATE

Principiul 31: Instituirea unor organe independente de supraveghere

Statele trebuie să înființeze, dacă nu au facut-o deja, organisme independente de supraveghere a entităților sectorului de securitate, inclusiv ale operațiunilor, reglementărilor, politicilor, finanțelor şi administrării acestora. Astfel de organisme de supraveghere trebuie să fie independente instituțional, operațional şi financiar de instituțiile pe care sunt mandatate să le supravegheze.

Principiul 32: Acces nerestricționat la informații necesare pentru îndeplinirea mandatului

a) Organismele independente de supraveghere trebuie să aibă legal garantat dreptul de acces la toate informațiile necesare pentru îndeplinirea mandatului. Nu ar trebui să existe nicio restricție privind accesul, indiferent de nivelul de secretizare sau de confidențialitate a informației, după îndeplinirea unor condiții rezonabile pentru accesul securizat;

b) Informațiile la care organismele de supraveghere trebuie să aibă acces includ, dar nu se limitează la:

i) Toate înregistrările, tehnologiile şi sistemele în posesia autorităților sistemului de securitate, indiferent de formă sau mediu de stocare sau dacă au fost sau nu create de acea autoritate;

ii) Localizări fizice, obiecte şi facilități, şi

iii) Informații deținute de persoanele pe care organismele de supraveghere le consideră relevante pentru funcțiile lor de supraveghere.

c) Orice obligație a personalului public de a păstra secretul sau confidențialitatea nu trebuie să îi împiedice să ofere informații organismelor de supraveghere. Divulgarea de asemenea informații nu trebuie să fie considerată încălcare a legii sau a obligațiilor contractuale care impun păstrarea confidențialității.

Principiul 33: Competențele, resursele şi procedurile necesare pentru a asigura accesul la informație

a) Organismele independente de supraveghere trebuie să aibă atribuții legale adecvate pentru a fi în măsură să acceseze şi să interpreteze orice informație relevantă pe care o consideră necesară pentru îndeplinirea mandatului;

i) Aceste atribuții trebuie să includă cel puțin dreptul de a chestiona membrii puterii executive, actuali şi foşti, şi angajați şi contractori ai autorităților publice, să solicite şi să inspecteze înregistrări relevante şi să inspecteze locații şi facilități fizice;

ii) Organismele independente de supraveghere trebuie, de asemenea, să aibă autoritatea de a audia astfel de persoane şi înregistrări şi să ia mărturii sub jurământ sau declarații de la persoanele presupuse a deține informații care sunt relevante pentru îndeplinirea mandatului lor, cu întreaga cooperare a agențiilor de aplicare a legii, atunci când este necesar.

b) Organismele independente de supraveghere, atunci când procesează informații sau mărturii, trebuie să ia în considerare, inter alia, prevederile relevante ale dreptului la viață privată, precum şi protecția împotriva auto-incriminării şi alte cerințe ale procesului echitabil;

c) Organismele independente de supraveghere trebuie să aibă acces la resursele financiare, tehnologice şi umane necesare pentru a le permite să identifice, acceseze şi analizeze informații care sunt relevante pentru îndeplinirea efectivă a funcțiilor lor;

d) Legea trebuie să oblige instituțiile sectorului de securitate să acorde organismelor independente de supraveghere cooperarea de care au nevoie pentru a accesa şi interpreta informația necesară pentru îndeplinirea funcțiilor lor;

e) Legea trebuie să oblige instituțiile sectorului de securitate să divulge organismelor independente de supraveghere, din proprie inițiativă şi la timp, categorii de informații pe care organismele independente de supraveghere le-au stabilit ca fiind necesare pentru

îndeplinirea mandatului lor. Aceste informații trebuie să includă, dar să nu se limiteze la posibile încălcări ale legii şi ale standardelor drepturilor omului.

Principiul 34: Transparența organelor independente de supraveghere

A. Aplicabilitatea legislației privind accesul la informații

Legislația privind exercitarea dreptului publicului de a accesa informații deținute de autoritățile publice trebuie să se aplice organismele independente de supraveghere.

B. Raportarea

(1) Organismele independente de supraveghere trebuie să fie obligate legal să realizeze rapoarte periodice şi să facă aceste rapoarte disponibile public. Aceste rapoarte trebuie să includă, cel puțin, informații privind organismele independente de supraveghere în sine, inclusiv despre mandatul, compunerea, bugetul, performanța şi activitățile lor.

Notă: Aceste rapoarte trebuie să conțină, de asemenea, informații despre mandatul, structura, bugetul şi activitățile generale ale oricărei instituții din domeniul securității, informație care nu este de la sine pusă la dispoziția publicului.

(2) Organismele independente de supraveghere trebuie să ofere versiuni publice ale rapoartelor care se referă la studii şi investigații tematice şi de caz şi trebuie şi ofere pe cât de multe informații posibil privind chestiunile de interes public, inclusiv cu privire la acele domenii enumerate la Principiul 10;

(3) În raportarea publică, organismele independente de supraveghere trebuie să respecte drepturile tuturor persoanelor interesate, inclusiv dreptul lor la viață privată;

(4) Organismele independente de supraveghere trebuie să ofere instituțiilor care fac obiectul supravegherii oportunitatea de a analiza, în timp util, orice raport ce urmează a fi făcut public pentru a le

permite să ridice obiecții cu privire la includerea de material ce poate fi secretizat. Decizia finală cu privire la ce trebuie publicat trebuie să rămână la însuşi organismul de supraveghere.

C. Disponibilitate şi accesibilitate

(1) Baza legală a organismelor de supraveghere, inclusiv mandatul şi atribuțiile, trebuie să fie disponibile public şi uşor accesibile.

(2) Organismele independente de supraveghere trebuie să creeze mecanisme şi facilități pentru persoane analfabete, care vorbesc în limbi ale minorităților sau care au probleme de văz sau de auz să acceseze informații despre activitatea lor;

(3) Organismele independente de supraveghere trebuie să ofere o paletă de mecanisme liber accesibile prin care publicul, inclusiv persoanele din zone geografic îndepărtate, să fie ajutate să ia contact cu ele şi, în cazul organismelor în care procesează plângeri, să depună plângeri sau să exprime temeri.

(4) Organismele independente de supraveghere trebuie să aibă mecanisme care să permită păstrarea efectivă a confidențialități plângerilor şi anonimitatea celui care se plânge.

Principiul 35. Măsuri pentru protecția informației administrate de către organele de supraveghere din sectorul de securitate

a) Legea trebuie să impună organismelor independente de supraveghere să implementeze toate măsurile necesare să protejeze informația din posesia lor.

b) Legislativele trebuie să aibă puterea să decidă dacă i) membrii comitetelor legislative de supraveghere şi ii) conducătorii şi membrii organismelor independente nelegislative ar trebui să fie subiecți ai controlului de securitate înainte de numire.

c) Când controlul de securitate este cerut, trebuie să fie întreprins i) în timp util, ii) conform unor principii stabilite, iii) fără partizanat sau motivație politică şi iv) pe cât posibil de o instituție care nu e supravegheată de entitatea ai cărei membrii/personal sunt controlați.

d) Potrivit principiilor din Partea a VI-a şi a VII-a, membrii sau personalul organismelor independente de supraveghere care dezvăluie chestiuni secretizate sau confidențiale în orice alt mod în afara mecanismelor normale de raportare ale organismului trebuie să fie supuşi procedurilor administrative, civile sau penale potrivite.

Principiul 36: Atribuția legislativului de a face publice informațiile

Legislativul ar trebui să aibă puterea de a dezvălui orice informații publicului, inclusiv informații față de care puterea executivă pretinde dreptul de a refuza divulgarea pe motive de securitate națională, in cazul in carecosideră necesar să facă acest lucru în conformitate cu procedurile pe care el ar trebui să le instituie.

PARTEA VI. INFORMAȚII DE INTERES PUBLIC DIVULGATE DE CĂTRE FUNCȚIONARII PUBLICI

Principiul 37: Categorii de activități ilicite

Divulgarea, de către funcționarii publici, de informații, chiar secretizate, care arată activități ilicite care intră în una din următoarele categorii trebuie considerată ”divulgare protejată”, dacă respectă condițiile stabilite de Principiile 38-40. O divulgare protejată se poate referi la o activitate ilicită care s-a petrecut, se petrece sau se va petrece.

a) Infracțiuni;
b) Încălcări ale drepturilor omului;
c) Încălcări ale dreptului internațional umanitar;
d) Corupție;
e) Pericole pentru sănătatea şi siguranța publică;
f) Pericole pentru mediu;
g) Abuzul de funcție publică;
h) Erori judiciare;
i) Proasta administrare sau risipirea resurselor;
j) Pedepsirea pentru divulgarea oricăror abuzuri din categoriile de mai sus; şi
k) Ascunderea deliberată a oricărei chestiuni care se încadrează la categoriile de mai sus.

Principiul 38: Temeiurile, motivarea şi dovada pentru divulgarea informaţtiei ce denotă activități ilicite divulgar

a) Legea trebuie să protejeze de represalii, definite potrivit Principiului 41, funcționarii publici care divulgă informații ce demonstrează activități ilicite, indiferent dacă informația este secretizată sau facută confidențială în orice alt mod, atât timp cât, la momentul divulgării:

(i) persoana care face divulgarea a avut motive rezonabile să creadă că informația divulgată tinde să demonstreze activități ilicite

care se încadrează într-una dintre categoriile prevăzute de Principiul 37, şi

(ii) divulgarea respectă condiţiile prevăzute de Principiile 38-40

b) Motivaţia pentru o divulgare protejată este irelevantă cu excepţia situaţiei când este demonstrat faptul că se ştia ca informaţia este neadevărată;

c) Unei persoane ce face o divulgare protejată nu trebuie să i se ceară să aducă dovezi în susţinere or să suporte sarcina probei în privinţa divulgarii.

Principiul 39: Proceduri pentru divulgări protejate şi reacţionare la aceste divulgări

A. Divulgări interne

Legea trebuie să stabilească în sarcina autorităţilor publice obligaţia de a reglementa proceduri interne şi a desemna persoanele cărora să li se adreseze divulgarile protejate.

B. Divulgări facute către organele independente de supraveghere

(1) Statele trebuie de asemenea să stabilească sau să identifice organisme independente care să primească şi să investigheze divulgari protejate. Astfel de organisme trebuie să fie instituţional şi operaţional independente de sectorul de securitate şi de alte autorităţi de la care se fac divulgările, inclusiv independente de executiv.

(2) Funcţionarii publici trebuie autorizaţi să realizeze divulgari protejate către organisme independente de supraveghere ori către orice alt organism competent să investigheze chestiunea fără ca să fie obligaţşi ca mai întâi să facă divulgarea internă.

(3) Legea trebuie să garanteze că organismele independente de supraveghere au acces la toate informaţiile relevante şi să acorde acestora atribuţiile necesare de investigare care să asigure accesul. Astfel de atribuţii trebuie să includă pe cele de audiere si atribuţia de a solicita ca o mărturie să fie făcută sub jurământ sau afirmare.

C. Obligaţiile organelor interne şi ale organelor independente de supraveghere care recepţionează divulgări

Dacă o persoană face o divulgare protejată, aşa cum este definită de Principiul 37, intern sau către un organism independent de supraveghere, organismul căruia i se adresează divulgarea trebuie să fie obligat să:

1. Investigheze încălcarea legii reclamate şi să ia măsuri prompte în scopul de a rezolva chestiunea într-un termen prevăzut de lege sau, după ce s-a consultat cu persoana care a făcut divulgarea, să o direcţioneze către un organism care este autorizat şi competent să o investigheze;

2. Protejeze identitatea funcţionarului public care urmăreşte să facă divulgări confidenţiale; divulgările anonime trebuie analizate pe fond;

3. Protejeze informaţia dezvăluită şi faptul că divulgarea a fost făcută cu excepţia şi în limita situaţiei în care divulgări suplimentare de informaţii sunt necesare pentru remedierea încălcării legii; şi

4. Notifice persoana care face divulgarea despre evoluţia şi finalizarea unei investigaţii şi, pe cât posibil, despre măsurile luate sau recomandările făcute.

Principiul 40: Protecţia divulgărilor publice

Legea trebuie să protejeze de represalii (aşa cum este definit în Principiul 41) divulgările către public a informaţiilor privind activităţi ilicite,aşa cum sunt definite de Principiul 37 , dacă divulgarea îndeplineşte următoarele criterii:

a) 1. Persoana a făcut o divulgare internă şi/sau către un organism independent de supraveghere a aceleiaşi sau a unei foarte asemănătoare informaţii şi:

i) Organismul către care s-a făcut divulgarea a refuzat sau a eşuat să investigheze divulgarea în mod eficient , în conformitate cu standardele internaţionale aplicabile; sau

ii) Persoana nu a primit o soluţionare rezonabilă şi potrivită, într-un termen rezonabil şi stabilit de lege.

SAU

2. Persoana a crezut în mod rezonabil că exista un risc semnificativ ca, în cazul unei divulgări interne şi/sau către un organism independent de supraveghere, să se fi distrus sau ascuns probe, să fi fost influențat un martor sau să fi fost supusă represaliilor ea însăşi sau un terț;

SAU

3. Nu exista nici niciun organism intern sau independent de supraveghere către care să fie făcută divulgarea:

SAU

4 Divulgarea se refera la un act sau o omisiune care constituia un risc grav şi iminent pentru primejduirea vieții, sănătății sau siguranței unei persoane sau a mediului înconjurător.

ŞI

b) Persoana care a făcut divulgarea a dezvăluit atâta informație cât era rezonabil necesar pentru a arăta activitatea ilicită

Notă: Dacă în procesul de divulgare a informațiilor care denotă activități ilicite o persoană divulgă, de asemenea, documente care nu sunt relevante pentru a demonstra activitățile ilicite, persoana ar trebui totuşi să fie protejată împotriva represaliilor, cu excepția cazului în care prejudiciul divulgării prevalează asupra oricărui interes public în divulgare.

ŞI

c) Persoana care a făcut divulgarea a crezut în mod rezonabil că interesul public în divulgarea informației depăşea orice prejudiciu adus interesului public prin divulgare.

Notă: Testul "crezut în mod rezonabil" este un test mixt obiectiv-subiectiv. Persoana, de fapt, trebuie să fi crezut (subiectiv) şi credința trebuie să fi fost rezonabilă pentru ca el sau ea să fi procedat astfel (obiectiv). Dacă este contestat, persoana ar putea avea nevoie să apere caracterul rezonabil al credinței sale şi în cele din urmă să rămână la latitudinea unei instanțe independente sau a tribunalului de a stabili dacă acest test a fost îndeplinit, astfel încât divulgarea să devină protejabilă.

Principiul 41: Protecția împotriva represaliilor pentru divulgări de informații care demonstrează activități ilicite

A. Imunitatea față de răspunderea civilă şi penală pentru divulgări protejate

O persoană care a făcut o divulgare, în conformitate cu Principiile 37-40, nu trebuie să fie subiectul :

(1) Procedurilor penale, inclusiv, dar nu limitate la, urmărirea penală pentru divulgarea de informații secretizate sau confidențiale; sau

(2) Procedurilor civile legate de divulgarea de informații secretizate sau confidențiale, inclusiv dar nu limitate la, încercărilor de a obține despăgubiri sau procedurilor de defăimare;

B. Interzicea altor forme de represalii

1. Legea trebuie să interzică represalii împotriva oricărei persoane care a făcut, este suspectată că a făcut sau ar putea face divulgări în conformitate cu Principiile 37-40.

2. Formele interzise de represalii includ, dar nu se limitează la:

a) Măsuri sau sancțiuni administrative, inclusiv dar nu limitate la: scrisori de avertizare, cercetări cu caracter sancționator, retrogradare, transfer, schimbare de atribuții, nepromovare, concediere, acțiuni care pot aduce sau intenționează să aducă prejudicii reputației unei persoane, sau suspendare sau revocarea unui certificat de securitate:

b) Vătămări sau hărțuire fizică sau emoțională; sau

c) Amenințări cu oricare dintre cele de mai sus.

3. Acțiunile luate împotriva altor persoane decât cea care fac divulgarea pot, în anumite circumstanțe, să constituie represalii interzise.

C. Investigarea represaliilor de către un organism independent de supraveghere şi de către autoritățile judiciare

1. Orice persoană trebuie să aibă dreptul de a raporta către un organism independent de supraveghere şi/sau către o autoritate judiciară orice măsură de represalii ori amenințare cu represalii, în legătură cu divulgări protejate.

2. Organismele independente de supraveghere trebuie să investigheze o sesizare privind represaliile sau amenințarea cu represalii. Astfel de organisme trebuie să aibă posibilitatea de a începe o investigație în absența unei sesizări privind represalii.

3. Organismele independente de supraveghere trebuie să aibă atribuțiile şi resursele să investigheze efectiv orice represalii pretinse, inclusiv atribuția de a audia persoane şi a de obține documente şi de a audia martori sub jurământ sau afirmație.

4. Organismele independente de supraveghere trebuie să depună toate eforturile pentru a se asigura că procedurile privind represaliile pretinse sunt echitabile şi în concordanță cu standardele procesului echitabil.

5. Organismele independente de supraveghere trebuie să aibă autoritatea de a cere autorităților publice în chestiune să adopte măsuri de remediere sau restorative, inclusiv dar nu limitate la reangajare; renumire; şi/sau plata de taxe legale şi alte costuri rezonabile, plata retroactivă a salariului şi a altor beneficii, costuri de călătorie şi/sau daune compensatorii.

6. Organismele independente de supraveghere trebuie să aibă autoritatea de a ordona autorității publice să se abțină de la sancțiuni punitive.

7. Astfel de organisme trebuie să finalizeze investigația într-un termen rezonabil şi stabilit de lege.

8. Astfel de organisme trebuie să notifice persoanele relevante cel puțin cu privire la finalizarea investigației şi, pe cât posibil, cu privire la măsurile luate şi recomandările făcute;

9. Persoanele pot contesta în instanța judecătorească decizia organului independent de supraveghere, conform căreia acțiunile în rezultatul divulgării nu constituie represalii sau măsuri de reparare sau de restabilire.

D. Sarcina probei

Dacă o autoritate publică ia o măsură împotriva oricărei persoane, autoritatea are sarcina de a demonstra că măsura nu a avut legătură cu divulgarea.

E. Nerenunțarea la drepturi şi remedii

Nu se poate renunța sau nu pot fi limitate drepturile şi remediile prevăzute de Principiile 37-40 prin nicio formă de înțelegere, politică publică, formă sau condiție de angajare, inclusiv prin nicio înțelegere de arbitraj pre-dispută. Orice încercare de renunțare sau limitare a drepturilor şi remediilor trebuie considerată nulă.

Principiul 42: Încurajarea şi facilitarea divulgărilor protejate

Statele trebuie să încurajeze funcționarii publici să facă divulgari protejate. Pentru a facilita astfel de divulgări, statele trebuie să ceară tuturor autorităților publice să emită reglementări care să pună în practică Principiile 37-42.

Notă: Aceste reglementări ar trebui să ofere, cel puțin: (1) sfaturi cu privire la drepturile şi/sau responsabilitățile de a divulga activități ilicite, (2) tipurile de informații care trebuie sau pot fi divulgate, (3) procedurile necesare pentru a face astfel de divulgări; şi (4) protecții prevăzute de lege.

Principiul 43: Apărarea interesului public pentru funcționarii publici

a) Ori de câte ori funcționarul public poate fi supus unor proceduri penale sau civile sau unor sancțiuni administrative, în legătură cu divulgarea unor informații, care nu este astfel protejată de aceste Principii, legea trebuie să prevadă posibilitatea acestuia de a se apăra invocând interesul public, dacă interesul public pentru divulgarea informației în chestiune depăşeşte interesul public pentru ne-divulgare.

Notă: Acest principiu se aplică tuturor divulgărilor de informații care nu sunt încă protejate, fie pentru că informațiile nu se încadrează într-una dintre categoriile menționate în Principiul 37, fie că divulgarea conține informații care se încadrează în una dintre categoriile menționate în Principiul 37, dar nu a fost făcută în conformitate cu procedurile descrise în Principiile 38-40.

b) Pentru a decide dacă interesul public pentru divulgare depăşeşte interesul public pentru ne-divulgare, autoritățile de cercetare penală şi judiciare trebuie să ia în considerare:

i) Dacă amploarea divulgării a fost rezonabil necesară pentru divulgarea informației de interes public;

ii) Amploarea şi riscul de prejudiciere a interesului public cauzat de divulgare;

iii) Dacă persoana a avut motive rezonabile să creadă că divulgarea ar fi fost în interes public;

iv) Dacă persoana a încercat să facă o divulgare protejată prin procedurile interne şi/sau către un organ independent de supraveghere, şi/sau către public, în conformitate cu procedurile descrise în Principiile 38-40; şi

v) Existența unor circumstanțe urgente care justifică divulgarea.

Notă: Orice lege care prevede pedepse penale pentru o divulgare neautorizată de informații ar trebui să fie în concordanță cu Principiul 46 (b). Acest principiu nu urmăreşte să limiteze vreun drept la libera exprimare deja disponibil pentru funcționarii publici sau oricare dintre protecțiile garantate în conformitate cu principiile 37 - 42 sau 46.

PARTEA VII. LIMITE CU PRIVIRE LA MĂSURILE DE SANCȚIONARE SAU DE RESTRÂNGERE A DIVULGĂRII INFORMAȚIEI CĂTRE PUBLIC

Principiul 44: Protecție împotriva sancțiunilor pentru divulgarea rezonabilă, făcută cu bună-credință de către ofițerii de comunicare

Persoanele cu atribuții de a răspunde cererilor de informații din partea publicului nu trebuie sancționate pentru divulgarea informației despre care în mod rezonabil şi cu buna-credință au crezut că poate fi divulgată potrivit legii.

Principiul 45: Sancțiuni pentru distrugerea sau refuzul de a divulga informații

a) Personalul public trebuie să fie supus sancțiunilor pentru distrugerea sau modificarea cu intenție a informațiilor, în scopul de a nega accesul la ele.

b) Dacă o instanță sau un organ independent a ordonat divulgarea informației şi informația nu este divulgată în timp rezonabil, oficialul şi/sau autoritatea publică responsabilă pentru ne-divulgare trebuie să fie supusă unor sancțiuni potrivite, cu excepția situației în care s-a declarat apel potrivit procedurilor legale.

Principiul 46: Limitări cu privire la pedepsele penale pentru divulgarea de informații de către funcționarii publici

a) Divulgarea publică de informații, din partea funcționarului public, chiar dacă neprotejată de Partea a IV-a, nu trebuie să fie subiectul sancțiunilor penale, deşi poate fi subiectul sancțiunilor administrative, precum ar fi pierderea certificatelor de securitate sau chiar concedierea.

b) Dacă totuşi legea impune sancțiuni penale pentru divulgarea neautorizată a informației către public ori către persoane cu scopul ca informația să fie făcută publică, următoarele condiții trebuie să se aplice:

i) Sancțiunile penale trebuie să se aplice divulgării unor categorii restrânse de informații care sunt clar stabilite de lege;

Notă: Dacă legislația națională prevede categoriile de informații a căror divulgare ar putea face obiectul unor sancțiuni penale, acestea trebuie să fie similare cu următoarele în ceea ce priveşte specificitatea şi impactul asupra securității naționale: date tehnologice despre armele nucleare, surse, coduri şi metode de colectare a informației secrete,; coduri diplomatice, identități ale agenților sub acoperire; şi proprietate intelectuală, în care statul are interes de proprietate, precum şi cunoştințe care ar putea prejudicia securitatea națională.

ii) Divulgarea trebuie să producă un risc real şi identificabil de a cauza un prejudiciu important;

iii) Orice sancțiune penală, aşa cum este prevăzută de lege şi aplicată, trebuie să fie proporțională cu prejudiciul creat; şi

iv) Persoana trebuie să poată să invoca în apărarea sa interesul public, aşa cum este prevăzut de Principiul 43.

Principiul 47: Protecția împotriva sancțiunilor pentru posesia şi diseminarea informațiilor secretizate de către persoane care nu sunt funcționari publici

a) O persoană care nu este funcționar public nu poate fi sancționată pentru primirea, posesia sau divulgarea către public a informațiilor secretizate.

b) O persoană care nu este funcționar public nu poate fi subiectul unor acuzații de complot sau de alte infracțiuni în baza faptului că a căutat şi a obținut informația.

Notă: Acest principiu îşi propune să împiedice urmărirea penală pentru achiziționarea sau reproducerea de informații. Cu toate acestea, acest principiu nu are drept scop împiedicarea urmăririi penale a unei persoane pentru comiterea altor infracțiuni, cum ar fi furt sau şantaj, comise în cursul căutării, sau pentru obținerea informațiilor.

Notă: Divulgările către terți funcționează ca o corecție importantă pentru supra-secretizarea generalizată.

Principiul 48: Protecția surselor

Nicio persoană care nu este funcționar public nu trebuie obligată să dezvăluie o sursă confidențială sau materiale nepublicate într-o investigație privind divulgarea neautorizată de informații către presă sau public.

Notă: Acest principiu se referă doar la investigațiile privind divulgarea neautorizată a informațiilor, nu şi la alte infracțiuni.

Principiul 49: Împiedicarea prealabilă

a) Împiedicarea prealabilă a publicării în interesul protejării securității naționale trebuie interzisă.

Notă: Împiedicările prealabile sunt ordine ale organelor judiciare sau ale altor organe de stat care interzic publicarea de materiale specifice aflate deja în posesia unei persoane care nu este funcționar public.

b) Dacă informația a fost pusă la dispoziția publicului, prin orice mijloace, legale sau nu, orice încercare de a opri publicarea subsecventă a informației în forma în care este deja în domeniul public este prezumtiv invalidă.

Notă: Prin termenul "disponibile în mod general" se subînțelege că informațiile au fost diseminate pe scară destul de largă, astfel încât nu există măsuri concrete care ar putea fi întreprinse şi care ar păstra informațiile secrete.

PARTEA VIII. PRINCIPIUL FINAL

Principiul 50: Relația dintre aceste principii şi alte standarde

Nicio prevedere a acestor principii nu trebuie interpretată ca restrângând sau limitând orice drept la informație recunoscut potrivit reglementărilor şi standardelor internaționale, regionale sau naționale sau orice normă a dreptului intern sau internațional care ar prevedea o mai mare protecție pentru divulgările făcute de personalul public sau de alte persoane.

Anexă: Organizații partenere

Următoarele 22 de organizații au contribuit în mod substanțial la elaborarea principiilor şi s-au angajat în diseminareea, publicarea şi în punerea lor în aplicare[2]. După denumirea fiecărei organizații este indicat oraşul, dacă este cazul, în care este situată organizația, precum şi țara sau regiunea în care activează. Organizațiile care întreprind activități substanțiale în trei sau mai multe regiuni sunt menționate ca fiind ”globale”, adică organizații care activează la nivel global.

- Africa Freedom of Information Centre (Kampala/Africa);
- African Policing Civilian Oversight Forum (APCOF) (Cape Town/Africa)
- Alianza Regional por la Libre Expresión e Información (Americas)
- Amnesty International (London/global);
- Articolul 19, the Global Campaign for Free Expression (London/global);
- Asian Forum for Human Rights and Development (Forum Asia) (Bangkok/Asia);
- Center for National Security Studies (Washington DC/United States);
- Central European University (Budapest/ Europe);
- Centre for Applied Legal Studies (CALS), Wits University (Johannesburg/South Africa);
- Centre for European Constitutionalization and Security (CECS), University of Copenhagen (Copenhagen/Europe);
- Centre for Human Rights, University of Pretoria (Pretoria/ Africa);

[2] În plus, Aidan Wills şi Benjamin Buckland, de la Geneva Centre for Democratic Control of the Armed Forces (DCAF), dar care nu este afiliat niciuneia dintre organizațiile partenere au adus, de asemenea, contribuții semnificative în special la partea V cu privire la organele de supraveghere şi la partrea VI – cu privire la divulgările de interes public, precum şi la principii în ansamblu.

• Centre for Law and Democracy (Halifax/global);

• Centre for Peace and Development Initiatives (Islamabad/Pakistan);

• Centre for Studies on Freedom of Expression and Access to Information (CELE), Palermo University School of Law (Buenos Aires/Argentina);

• Commonwealth Human Rights Initiative (New Delhi/Commonwealth);

• Egyptian Initiative for Personal Rights (Cairo/Egypt);

• Institute for Defence, Security and Peace Studies (Jakarta/Indonesia);

• Institute for Security Studies (Pretoria/Africa);

• International Commission of Jurists (Geneva/global);

• National Security Archive (Washington DC/global);

• Open Democracy Advice Centre (Cape Town/Southern Africa); şi

• Open Society Justice Initiative (New York/global).

NOTE