L680/2011 Proiect de lege privind modificarea şi completarea unor acte normative în domeniul securităţii naţionale.
Proiectul propune introducerea unei noi proceduri privind autorizarea restrângerii exerciţiului unor drepturi sau libertăţi fundamentale ale persoanei, în acord cu garanţiile constituţionale şi ale Curţii Europene a Drepturilor Omului(CEDO) în materie.

Germania

Legea Serviciului Judiciar Federal prevede că, în cazul infracţiunilor care reprezintă ameninţări la adresa securităţii naţionale, a unor înalţi demnitari sau în alte situaţii enumerate în lege, cercetările intră în competenţa poliţiei judiciare. Aceasta colaborează cu poliţia, procuratura şi celelalte autorităţi competente ale Land-urilor şi ale Federaţiei pentru combaterea criminalităţii. Cu acordul instanţei de urmărire penală, poliţia judiciară are dreptul de a strânge, păstra şi utiliza informaţii referitoare la persoanele implicate, care sunt utile în desfăşurarea cercetărilor. Ministerul Federal de Interne hotărăşte, cu aprobarea Bundesrat-ului, ce fel de date pot fi colectate şi stocate. Este permisă colectarea datelor numai în cazul persoanelor bănuite că intenţionează să înfăptuiască o infracţiune gravă sau că au legături strânse cu o persoană care are asemenea intenţii. Poliţia judiciară are dreptul să legitimeze, să reţină şi să interogheze o persoană care se presupune că poate furniza informaţii necesare desfăşurării anchetei. Persoana are dreptul de a refuza să răspundă la întrebări, dar nu şi în cazul în care răspunsurile sale ar putea ajuta la prevenirea comiterii unei infracţiuni la adresa statului sau a unei persoane. În desfăşurarea cercetărilor sale, poliţia judiciară are dreptul de a utiliza mijloace şi metode speciale pentru strângerea de informaţii. Astfel, ea poate:

- pune persoana sub urmărire;
- utiliza mijloace tehnice audio sau video în afara locuinţei, de care persoana urmărită să nu aibă cunoştinţă;
- folosi alte mijloace tehnice în vederea localizării persoanei urmărite;
- apela la persoane particulare de încredere sau la un agent de poliţie care să acţioneze sub acoperire.

Infiltrarea unui poliţist sub acoperire, se poate face numai pe baza unui mandat judecătoresc obţinut pe baza cererii înaintate de conducerea instituţiei. În cazurile urgente, se poate lua această măsură şi doar pe baza aprobării conducerii instituţiei, urmând ca aceasta să continue demersurile

legale de solicitare a mandatului. Dacă mandatul nu este obținut în termen de trei zile, intervenția polițistului sub acoperire trebuie să înceteze. Pentru celelalte tipuri de măsuri speciale (utilizarea de mijloace tehnice audio-video, punerea sub urmărire a persoanei sau apelarea la persoane de încredere), conducerea Serviciului Judiciar Federal trebuie să adreseze curții judecătoreşti o cerere motivată. Mandatul acordat de curte are o valabilitate de o lună, iar pentru ultimele două măsuri de maximum două luni. Pentru prelungirea mandatului este necesară o nouă cerere. Înregistrarea de imagini fotografice sau filmate, precum şi înregistrarea de sunete din interiorul locuinței persoanei urmărite este permisă tot pe baza unui mandat judecătoresc. Pentru obținerea acestuia este necesară o cerere scrisă şi motivată din partea Preşedintelui Serviciului Judiciar Federal. Durata mandatului este de o lună, putând fi prelungită în mod repetat cu perioade de maximum o lună. Tot pe bază de mandat judecătoresc, pentru a colecta date necesare anchetei, poliția judiciară poate pătrunde în computerul sau sistemele de date informatice utilizate de persoana urmărită, îi poate intercepta şi înregistra convorbirile telefonice, poate cere localizarea urmăritului prin intermediul rețelei de telecomunicații mobile. Poliția judiciară are dreptul de a efectua percheziții şi de a confisca bunuri, de a restricționa temporar accesul unei persoane într-un anumit spațiu şi de a reține persoana aflată sub urmărire dacă aceasta nu respectă restricția impusă sau este pe cale să comită o infracțiune.

Marea Britanie

Legea Serviciului de Securitate este în vigoare încă din anul 1989. Aceasta prevede că Serviciul are ca scop protejarea securității naționale, apărarea împotriva spionajului, terorismului şi sabotajului sau combaterea activității unor agenți străini şi a acțiunilor menite să pericliteze democrația parlamentară. Serviciul de Securitate este condus de un Director General numit de Secretarul de Stat. În ce priveşte modul de operare al Serviciilor de Securitate, legea prevede că orice intrare pe proprietatea privată a unei persoane se poate face numai pe baza unui mandat emis de Secretarul de Stat. Acesta poate emite mandatul pe baza cererii scrise a Serviciului, dacă consideră necesară acțiunea în vederea obținerii unor informații importante, care nu pot fi obținute pe o altă cale şi dacă este convins că informațiile obținute vor fi secretizate. În cazuri urgente, mandatul poate fi emis, cu acordul Secretarului de Stat, şi de către un funcționar din Departamentul său. Valabilitatea mandatului este de şase luni de la emitere, dacă a fost semnat de Secretarul de Stat şi de două zile lucrătoare în orice alt caz. Dacă este necesar, Secretarul de Stat poate prelungi mandatul pentru încă şase luni. El poate, de asemenea, să

anuleze mandatul. Orice persoană care consideră că i-au fost încălcate drepturile sau proprietatea are dreptul de a se adresa Tribunalului. Acesta este compus din trei sau mai mulți membri numiți de Majestatea Sa.

Protecția datelor cu caracter personal

Franța

În Franța, protecția datelor cu caracter personal este reglementată prin Legea Nr. 78-17 din 6 ianuarie 1978 privind Procesarea Datelor, Dosarele Informative şi Libertățile Individuale, amendată prin Legea din 6 august 2004 privind protejarea persoanei şi procesarea datelor. Conform acestui act legislativ, orice persoană care face dovada identității sale are dreptul să se intereseze la autoritatea competentă dacă aceasta deține informații cu caracter personal la adresa sa, care este scopul deținerii acestor informații, ce fel de informații sunt şi la dispoziția cui se află. Ea poate solicita să îi fie comunicate, într-o formă accesibilă, datele personale şi informațiile disponibile cu privire la proveniența acestora. La cerere, persoana poate primi o copie a datelor sale personale, contra cost. Autoritatea competentă poate refuza aceste cereri dacă au un caracter sistematic şi excesiv. Orice persoană care face dovada identității sale are dreptul de a solicita autorității competente, după caz, rectificarea, completarea, actualizarea, blocarea sau ştergerea datelor sale personale care sunt inexacte, incomplete, echivoce, expirate sau a căror colectare, utilizare, publicare sau stocare este interzisă. La cererea persoanei în cauză, autoritatea competentă trebuie să facă dovada faptului că a executat operațiunile solicitate. Dacă autoritatea competentă a transmis informațiile unei terțe părți, ea trebuie să comunice acesteia modificările survenite. În cazurile care implică probleme de securitate națională, apărare sau siguranță publică, accesul la datele personale se va face indirect, după cum urmează: comisia care primeşte cererea de acces/rectificare numeşte pe unul din membrii săi, fost membru al Consiliului de Stat, al Curții de Casație sau al Curții de Conturi, să desfăşoare investigațiile necesare şi să execute eventualele modificări. În cazurile în care se consideră că divulgarea informațiilor nu periclitează în nici un fel scopul pentru care au fost culese, autoritatea competentă poate decide ca persoana în cauză să poată solicita direct administratorului informațiilor divulgarea acestora. Atunci când datele solicitate sunt de natură medicală, solicitantul poate opta între comunicarea lor directă sau cea prin intermediul unui medic, desemnat conform Art. L111-7 al Codului de Sănătate Publică.

Marea Britanie

În Marea Britanie, protejarea datelor cu caracter personal se face prin Legea Protejării Datelor, aflată în vigoare din anul 1998. Partea a II-a a acestui act normativ prevede că persoanele individuale au dreptul de a fi informate de către autoritatea competentă dacă datele sale personale fac obiectul unei procesări, şi de a i se comunica despre ce fel de date este vorba, în ce scop sunt procesate acestea şi beneficiarii cărora le pot fi transmise. De asemenea, persoana vizată are dreptul de a primi, într-o formă inteligibilă, orice informaţie deţinută de autoritatea competentă care are un caracter personal, precum şi toate informaţiile cu privire la proveniența lor. Pentru a primi aceste informaţii din partea autorităţii competente, persoana trebuie să facă dovada identităţii sale, să înainteze o cerere scrisă şi să achite taxa aferentă (cu excepţia anumitor cazuri). Autoritatea competentă are obligaţia de a răspunde prompt cererii primite, înainte ca termenul legal (acesta poate varia de la un caz la altul) să expire. Persoana care face subiectul anumitor informaţii şi consideră că acestea se bazează pe date incorecte, sau care a avut de suferit sau poate avea de suferit de pe urma inexactităţii datelor, se poate adresa unei instanţe judecătoreşti. Dacă instanţa consideră că cererea este întemeiată, poate solicita autorităţii competente rectificarea, blocarea, ştergerea sau distrugerea tuturor informaţiilor bazate pe date incorecte. Dacă este cazul, instanţa poate ordona completarea datelor existente sau orice alte măsuri consideră a fi necesare pentru ca totul să corespundă prevederilor legale. Atunci când consideră necesar, instanţa judecătorească poate solicita autorităţii competente să notifice eventualele terţe părţi, care au primit datele inexacte, cu privire la modificările survenite.

Germania

Legea Federală pentru Protecţia Datelor din 15 noiembrie 2006 prevede că dreptul cetăţeanului de acces la datele sale personale, precum şi dreptul de a cere corectarea, ştergerea sau blocarea acestora, este inalienabil, el neputând fi restricţionat prin sancţiuni legale. La cererea sa, persoanei îi vor fi furnizate informaţii privind datele sale personale stocate, inclusiv cu privire la sursele din care acestea provin, la beneficiarii cărora datele le pot fi furnizate sau la scopul stocării lor. Aceste prevederi nu se aplică, însă, în cazul datelor personale stocate numai fiindcă, în baza unei prevederi legale, statutare sau contractuale, nu este permisă ştergerea lor sau dacă stocarea lor serveşte exclusiv protejării sau securizării datelor. Dacă informaţiile solicitate au legătură cu transferul de date personale către Serviciul Federal de Informaţii, Biroul de Contrainformaţii al Forţelor Armate Federale sau alte autorităţi ale Ministerului Federal al

Apărării, precum şi în cazurile în care este vizată securitatea Federaţiei, furnizarea informaţiilor către solicitant se va face numai cu acordul instituţiilor implicate. Alte motive pentru care poate fi refuzată furnizarea de informaţii sunt:
- prejudicierea bunei desfăşurări a activităţii autorităţii competente;
- periclitarea siguranţei publice;
- prejudicierea Federaţiei sau a unui Land.

Datele sau stocarea acestora sunt secrete, conform unei prevederi legale sau prin natura lor. Motivele refuzului nu trebuie comunicate solicitantului dacă astfel este pus în pericol însuşi scopul pentru care cererea sa a fost respinsă. În asemenea cazuri, solicitantului i se indică numai posibilitatea de a apela la Comisarul Federal pentru Protecţia Datelor şi Libertatea de Informare. Dacă persoanei solicitante nu i-au fost furnizate informaţii, aceasta poate solicita ca informaţiile să fie transmise Comisarului Federal pentru Protecţia Datelor şi Libertatea de Informare. Acest transfer are loc dacă autoritatea federală competentă supremă nu decide că, în respectivul caz, ar fi periclitată siguranţa Federaţiei sau a Land-ului. Din răspunsul transmis de Comisarul Federal către solicitant nu trebuie să transpară în nici un fel datele deţinute de autoritatea competentă, excepţie făcând cazurile în care aceasta îşi dă acordul. Furnizarea de informaţii se face gratuit (cu excepţia cazurilor în care solicitantul poate obţine un câştig comercial pe baza acestora) şi, de regulă, în scris. Dacă se constată că anumite date cu caracter personal sunt incorecte, ele trebuie corectate. Datele a căror stocare este ilegală, sau care nu mai sunt necesare, trebuie şterse. Dacă prevederi legale, statutare sau contractuale interzic ştergerea acestui tip de date, ele vor fi blocate. Blocarea datelor se face şi în cazul unor dispute legale privind corectitudinea lor.

Belgia

În data de 8 decembrie 1992, Parlamentul Belgiei a adoptat **Legea privind protecţia confidenţialităţi cu privire la procesarea datelor personale**. Legea instituie obligaţia transparenţei în utilizarea datelor personale. În termenii legii, trebuie prevenite persoanele respective când sunt procesate informaţii despre ele, trebuie anunţate cine şi de ce face acest lucru. Legea stabileşte, de asemenea, regulile privind utilizarea datelor personale precum şi drepturile de care se bucură aceste persoane ale căror fişe au fost introduse în registre sau bănci de date: dreptul de acces la datele înregistrate, de rectificare, de opoziţie ...

În data de 24 octombrie 1995, a fost adoptată o Directivă pentru a armoniza regulile de protecţie a datelor personale pe întreg teritoriul Uniunii Europene. La fel ca toate celelalte state membre, Belgia a trebuit să transpună în dreptul său intern principiile conţinute în Directivă. În consecinţă, Legea din 8 decembrie 1992 a fost modificată prin Legea din 11 decembrie 1998, şi ulterior prin legea din 28 februarie 2003**. Legea privind protecţia datelor personale din Belgia** este structurată pe nouă capitole**: *I. Definiţii, principiu şi sferă de acţiune; II. Reguli generale privind legalitatea procesării datelor personale; III. Drepturile persoanei; IV. Confidenţialitatea şi securitatea procesării; V. Notificarea anterioară şi publicitatea procesării; VI. Transferul datelor personale către ţări din afara Uniunii Europene; Comisia pentru protecţia confidenţialităţii; Comitetele sectoriale; Dispoziţii privind infracţiunile; Dispoziţii finale.***

Legea defineşte, în primul rând, datele cu caracter personal, care se pot referi la un nume al persoanei, la o fotografie, un număr de telefon, un cont de bancă, etc., iar persoana implicată poate fi oricine care completează un formular, care rezervă un bilet la tren sau împrumută o carte de la bibliotecă, etc. De asemenea, este definit „tratamentul datelor" ca fiind orice operaţie sau ansamblu de operaţii – colectarea datelor, conservarea lor, utilizarea, modificarea, comunicarea lor etc. - aplicate unor date personale. Conform dispoziţiilor legii, responsabil de acest tratament este „persoana care determină obiectivele şi mijloacele privind tratamentul datelor", care poate fi o persoană fizică sau morală, o administraţie publică, etc. Legea nu se aplică atunci când datele sunt tratate în cadrul unor activităţi exclusiv personale sau domestice. În anumite cazuri, se prevede doar o aplicare parţială a legii – de exemplu, când datele cu caracter personal sunt folosite în scopuri artistice sau literare. O serie de dispoziţii nu sunt aplicate acestor tratamente pentru a garanta un echilibru în raport cu protecţia libertăţii de exprimare. Excepţări parţiale sunt acordate şi tratamentelor efectuate în scopul securităţii publice (de către Siguranţa Statului …). Conform prevederilor legale, înainte de a pune în aplicare un tratament întreg sau parţial automatizat, responsabilul acestui tratament trebuie să-l declare la Comisia pentru protecţia vieţii private. O declaraţie nu este echivalentul unei autorizaţii ci înseamnă exclusiv declararea unui tratament. Formularul de declaraţie este accesibil pe Internet (http://www.privacycommission.be). Toate informaţiile explicative care fac parte din aceste declaraţii-cadru sunt reluate într-un registru public, care pot fi consultate de orice persoană, fie online, fie la sediul Comisiei.

Dispoziţiile legale sunt foarte clare în ceea ce priveşte colectarea de date, care trebuie să fie loială, corectă şi solicitate pe baza consimţământului expres obţinut; informaţii cât mai exacte şi detaliate trebuie oferite

persoanelor interesate; responsabilul cu strângerea datelor trebuie să se identifice, să explice clar scopul acestei activități, caracterul obligatoriu sau nu al răspunsului, etc. Datele colectate trebuie să fie pertinente şi necesare.
Capitolul VI se ocupă de transferul datelor personale către țări în afara Uniunii Europene. Transferul datelor personale între statele membre ale UE este de acum liber. O persoană stabilită în Belgia poate deci să transmită date personale într-un alt stat membru al UE dacă această transmisie este legitimă conform legii belgiene. În schimb, în afara UE nu pot fi transmise date personale decât dacă țara respectivă asigură o protecție a datelor corespunzătoare celei asigurate pe teritoriul UE. Orice responsabil de tratamentul datelor respective care doreşte să exporte date personale în afara UE trebuie întâi să se informeze de nivelul de protecție al țării de destinație. Chiar şi atunci când țara de destinație este considerată a avea un nivel adecvat de protecție, trebuie respectate principiile generale ale legii (în special cele referitoare la legitimitate, compatibilitatea comunicării datelor unui terț, informarea persoanelor implicate, etc.). Caracterul adecvat al nivelului de protecție al țărilor din afara UE este determinat de Comisia Europeană pe baza legislației generale şi sectoriale a statului respectiv şi a regulilor profesionale. Pentru orice informații în acest sens, trebuie consultat
site-ul Comisiei Europene (http://ec.europa.eu/justice). Pentru a facilita schimbul de date persoanele şi cu alte țări, Comisia Europeană pune la dispoziția celor interesați modele de contracte tip care în mod automat sunt considerate ca oferind garanții suficiente în ceea ce priveşte protecția datelor. În Belgia, aceste modele de contracte tip nu trebuie confirmate prin decret regal şi decizie a Comisiei belgiene pentru protecția datelor personale (în caz contrar, respectiv atunci când aceşti responsabili de tratamente elaborează ei înşişi contracte de acest gen trebuie să aibă conformările prevăzute mai sus).

Italia

Codul de protecție a datelor personale (Decretul legislativ nr.196 din 30 iunie 2003)

Procesarea datelor cu caracter personal trebuie să fie făcută şi controlată astfel încât să fie reduse riscurile de distrugere involuntară sau de folosire a datelor de către o persoană neautorizată.

În cazul în care procesarea datelor se încheie, indiferent de motiv, acestea trebuie:
- să fie distruse;
- să fie transmise unui alt operator, în vederea prelucrării;
- să fie păstrate pentru scopuri strict personale, fără a fi distribuite sistemelor de comunicație;
- să fie trimise unui alt operator de date în scopul realizării unor arhive istorice, ştiinţifice sau statistice, conform legii, regulamentelor în vigoare şi legislației comunitare.
Furnizorul unui serviciu de comunicații electronice accesibile publicului împreună cu furnizorul sistemului public de comunicații au obligația de a lua măsuri în vederea protejării datelor personale. În lipsa existenței unui acord între părți, conflictele vor fi soluționate de către Autoritatea privind siguranța Comunicațiilor, conform dispozițiilor legale în vigoare.
Procesarea datelor cu caracter personal se face ținând cont de următoarele specificații tehnice:
- autentificare computerizată;
- utilizarea unui sistem informatic autorizat;
- actualizarea periodică a specificațiilor efectuate de entitățile responsabile cu gestionarea sistemelor electronice;
- protejarea datelor şi a mijloacelor electronice împotriva tuturor operațiunilor ilegale de prelucrare precum şi a accesului neautorizat;
- punerea în aplicare a codurilor de protecție sau a celor de identificare asupra datelor referitoare la sănătate şi viața sexuală.

Notificarea privind adunarea datelor cu caracter personal trebuie să conțină:
- date de natură genetică;
- date biometrice sau alte date ce fac referire la localizarea geografică a persoanelor fizice sau obiectelor, prin intermediul unei rețele de comunicații electronice;
- date referitoare la sănătate şi viața sexuală, atunci când scopul prelucrării este reproducerea asistată, prelevarea de organe sau alte scopuri medicale.

Datele cu caracter personal ce fac obiectul prelucrării pot fi transferate pe teritoriul altui stat din Uniunea Europeană, temporar sau nu, în orice formă şi prin orice mijloace, în următoarele situații:
- în cazul în care persoana în cauza şi-a dat acordul;
- în cazul în care transferul este necesar pentru îndeplinirea obligațiilor ce revin dintr-un contract la care persoana în cauză este parte;
- în cazul în care transferul datelor este necesar pentru protejarea unui interes public important; datele pot fi de natură personală sau judiciară;

- atunci când transferul se face cu scopul de a proteja viața unei persoane sau integritatea sa corporală;
- în cazul în care datele sunt necesare pentru efectuarea investigațiilor de către avocatul apărării;
- în scopuri ştiințifice sau statistice.

Datele personale supuse procesării vor fi păstrate şi verificate ținând cont şi de inovațiile tehnologice, de natura lor şi de caracteristicile procesării, astfel încât să se minimalizeze, prin măsurile preventive de securitate potrivite, riscul distrugerii sau pierderii acestor date, accidental sau nu, riscul accesului neautorizat la aceste date sau al procesării ilegale sau în neconcordanță cu scopul în care au fost strânse datele respective.

Furnizorul de servicii de comunicații electronice care sunt disponibile public va lua măsurile tehnice şi organizaționale conform Secțiunii 31, adecvate riscului existent, pentru a asigura securitatea serviciilor sale şi integritatea traficului de date, locației datelor şi a comunicațiilor electronice, împotriva utilizării sau accesului neautorizat.

Dacă securitatea serviciilor sau a datelor o cere, se vor lua măsuri aplicabile rețelei iar furnizorul unui serviciu de comunicații electronic disponibil publicului va lua aceste măsuri împreună cu furnizorul de rețea de comunicații publică. Dacă nu se ajunge la un acord între cei doi furnizori, conflictul va fi rezolvat în instanța oricăruia dintre furnizori, de către Autoritatea pentru Asigurarea Securității Comunicațiilor conform reglementărilor legislației în vigoare.

În cazul riscului de spargere a securității rețelei, furnizorul de servicii de comunicații electronice disponibile public îşi va informa abonații şi, dacă este posibil, îşi va informa utilizatorii despre respectivul risc iar atunci când riscul este în afara domeniului acoperit de măsurile care trebuie luate, îi va informa şi despre posibilele remedii, inclusiv despre posibilele costuri implicate. Aceste informații vor fi de asemenea furnizate Garantului şi Autorității pentru Protecția Comunicațiilor.

În cadrul cerințelor de securitate generale sau al celor stipulate în regulamentele specifice, controlorii de date vor fi obligați în orice caz să adopte măsurile de securitate minime conform legii pentru a se asigura un nivel minim de protecție a datelor personale.