REPERE JURIDICE ÎN DEZVOLTAREA ŞI IMPLIMENTAREA SISTEMELOR INFORMAŢIONALE

LEGAL CONSIDETRATIONS IN THE DEVELOPMENT AND DEPLOYMENT OF INFORMATIONAL SYSTEMS

MOCANU Veronica,
doctor în drept, conferenţiar universitar

CZU: 349:004.4:342.733

Summary

During the last period, more and more companies as well as state institutions trend to optimize and digitalize their activities by developing and implementing new informational systems, programs, softs, etc. However, not all the time, legal aspects are well considered. Therefore, hereby article, relieve the most important legal aspects which should be considered in the context of the development and deployment of the new technologies. This paper examines steps which should be performed by interested in development bodies, as well, as presents detailed information related to the ethical aspects which should be considered in context of the development of new technologies.

Key-words: *soft, IT program, informational system, data set, innovation, technology, privacy, deployment, digitalization, personal data protection, risks, human rights, artificial-intelligence, ethics, security.*

Introducere

Trăim într-o lume dinamică, caracterizată de procesări complexe şi voluminoase de informaţii, dezvoltări şi implementări continue de resurse şi sisteme de procesare informaţională tot mai noi şi mai complexe [1]. Cantitatea de cunoştinţe acumulate de omenire pe parcursul existenţei sale a ajuns în epoca cotemporană la un volum exorbitant de mare, care pune în dificultate capacitatea umană în a le analiza şi elabora concluzii în baza unor procesări simple neautomatizate de date. Toate domeniile cercetate şi practicate de oameni sunt cuprinse în acest vîrtej al schimbărilor, este o eră a tehnologiilor avansate bazate pe date şi dezvoltare tehnologică avansată.

Ultimul deceniu s-a remarcat, astfel, prin eforturi clar definite îndreptate spre digitalizare şi optimizarea proceselor de lucru. Orientând-se spre aceste scopuri, atât oamenii de ştiinţă, cât şi businessul şi instituţiile guvernamentale sau arătat interesate în dezvoltarea şi implementarea în activitatea de business dar şi cotidiană a unor varietăţi destul de largi de sisteme informaţionale, care în lumea specialiştilor IT apar sub diferite varietăţi tehnologice şi denumiri, precum soft, aplicaţie, gadget, IoT, inteligenţă artificială, etc.

Tendinţa spre tehnologizare însă nu întotdeauna este corelată cu cadrul legal care impune rigori legate de respectul faţă de drepturile omului, egalitate, inclu-

ziune, diversitate, confidenţialitate. Lipsa corelării cu cadrul legal este cauzată pe de o parte de lipsa de comunicare între specialiştii din domeniul IT cu specialiştii din domeniul legal, iar pe de altă parte de caducitatea prevederilor legale, care de multe ori nu acoperă realităţile în dezvoltare, venite din lumea IT.

În astfel de circumstanţe, dezvoltatorii din domeniul tehnic rămân a fi pe cont propriu, având posibilitatea să ofere beneficiarilor săi sisteme informaţionale adaptate la cerinţele acestora fără ca să ţină cont în măsură suficientă de prevederi legale, ori acestea de multe ori au un caracter foarte generic. În tot cazul, însă, chiar dacă cadrul legal nu este suficient de comprehensiv în ceia ce priveşte obligaţiile dezvoltărilor şi implementatorilor de tehnologii informaţionale, prin prezentul articol se propune a se prezenta cerinţele legale minime impuse spre respectare dezvoltatorilor şi implementatorilor de tehnologii, dar şi perspectiva etică propusă drept abordarea de compromis în cazul în care lipsesc prevederi legale exhaustive.

Făcând referire la cadrul de reglementare al Republicii Moldova, stabilim totuşi că acesta oferă o orientare generală dezvoltatorilor dar şi comandatarilor de sisteme informaţionale. Astfel, orientările legale de bază sunt stabilite de prevederile Legii cu privire la informatică [2], Legii cu privire la registre [4] şi Legii cu privire la informatizare şi la resursele informaţionale de stat [3], în cazul în care se propune dezvoltarea şi implementarea unor sisteme informaţionale propuse spre utilizare instituţiilor publice. În aceiaşi ordine de idei, în cazul în care funcţionalităţile sistemulor informaţionale presupun şi activităţi de prelucrare a datelor cu caracter personal, atunci dezvoltatorii sunt obligaţi să se conformeze cu prevederile prestabilite şi de Legea privind protecţia datelor cu caracter personal [5].

Ce înţelegem prin noţiunea de "sistem informaţional"?

Legea cu privire la informatică defineşte noţiunea de "sistem informaţional" drept sistem de prelucrare a informaţiei, împreună cu resursele organizaţionale asociate, cum ar fi resursele umane şi tehnice, care furnizează şi distribuie informaţia. Prin această definiţie, prezentul articolul reliefează faptul că sistemul informaţional reprezintă un fenomen complex care nu se referă doar la informaţie sau tehnică, dar implică şi resursele umane care asigură procesele de prelucrare a informaţiei [2].

Rolul sistemului informaţional este de a transmite informaţia prin utilizarea diferitor componente tehnice. De exemplu, în cadrul unei unităţi economice, rolul sistemului informaţional este de a asigura persoanele din conducere cu informaţii necesare pentru luarea diferitelor decizii economice sau de altă natură, astfel în calitate de instrumente posibile a fi utilizate în procesul de luare a deciziilor sunt elaborate softuri care prin alimentarea cu date din diferite procese operaţionale pot oferi soluţii managerilor.

Printre posibile activităţi desfăşurate prin utilizarea softului sus indicat pot fi enumerate: achiziţionarea de informaţii din sistemul de baza, completarea docu-

mentelor si transferul acestora intre diferite compartimente, centralizarea datelor, generarea deciziilor etc.

Printre exemplele de sisteme informaţionale puse în utilizare în practica Republicii Moldova pot fi menţionate: Sistemul informaţional judiciar [6], Sistemul Informaţional Integrat Vamal [7], Sistemului informaţional integrat automatizat "Migraţie şi azil" [8] Sistemului informaţional automatizat „Registrul de stat al achiziţiilor publice" (MTender) [9] etc.

Este de menţionat însă că practica utilizării sistemelor informaţionale este caracteristică nu doar instituţiilor publice dar şi celor private. Astfel, constatăm că odată cu creşterea numărului de sisteme informaţionale, cresc şi provocările legate de utilizarea acestora, precum şi eventualele riscuri, care pot afecta nu doar funcţionalitatea instituţiilor care le-au propus spre utilizare, dar şi viaţa privată sau siguranţa persoanelor fizice sau siguranţa economică a persoanelor juridice a căror date sunt propuse spre prelucrare prin utilizarea sistemelor informaţionale.

Urmare a celor menţionate, constatăm că cadrul legal se poate impune drept instrumentul care poate stabili limite dar şi instituţionaliza pârghiile de control în ceia ce priveşte dezvoltarea tehnologiilor informaţionale.

Astfel, prezentul articol, propune o detalizare a etapelor şi condiţiilor care sunt impuse spre respectare în contextul dezvoltării şi implementării sistemelor informaţionale.

Care sunt etapele de care contează pentru dezvoltarea unui sistem informaţional?

Dezvoltarea unui sistem informaţional nu trebuie abordat drept un proces spontan, sau haotic, dar din contra acest proces trebuie anticipat prin realizarea studiilor de fezabilitate, care eventual pot include atât cercetări asupra rezonabilităţii şi profitabilităţii sistemului propus spre dezvoltare, cât şi cercetarea rigorilor legale care se impun spre respectare, şi coroborarea acestora cu funcţionalităţile propuse spre dezvoltare. Din perspectiva proiectării acţiunilor de dezvoltare a sistemelor informaţionale, în Republica Moldova, se impune drept obligatorie spre consultare Reglementarea tehnică „Procesele ciclului de viaţă al software-ului" RT 38370656-002:2006, aprobată prin Ordinul ministrului dezvoltării informaţionale nr. 78/2006 [10]. Respectiva reglementare tehnică prezintă procesele ciclului de viaţă al software-ului şi este obligatorie spre respectare la crearea tuturor sistemelor informaţionale automatizate de importanţă statală. Agenţii economici, care furnizează/procură software pentru sistemele informaţionale automatizate nestatale, pot aplica prezenta reglementare tehnică în mod voluntar. Considerăm însă, că odată ce numărul de sisteme informaţionale cu caracter privat a crescut considerabil, sunt necesare completări legislative, în aşa fel încât procesul de dezvoltare a sistemelor informaţionale private la fel să corespundă principiilor generale de dezvoltare a softului.

Revenind, la reglementarea sus indicată, reliefăm că potrivit acesteia, dezvoltarea unui sistem informaţional al unei instituţii publice, trebuie să implice parcursul a cel puţin a următoarelor etape:

a) lucrările de anteproiect;

b) elaborarea sistemului software;

c) implementarea sistemului software;

d) exploatarea sistemului software;

e) mentenanţa sistemului software;

f) utilizarea sistemului software.

Furnizorul, în comun cu beneficiarul, trebuie să creeze modelul ciclului de viaţă al sistemului software concret, utilizând etapele şi procesele indicate.

Cu fiecare etapă se atinge un scop clar şi se aduce contribuţie la ciclul de viaţă al sistemului software în întregime. Fiecare etapă se ia în consideraţie la planificarea şi îndeplinirea ciclului de viaţă al sistemului software.

Pentru realizarea fiecărei etape, organizaţia trebuie să dispună de infrastructură corespunzătoare, buget, complex tehnic de program, instrumente, proceduri aprobate şi resurse umane competente. Toate componentele indicate se planifică până la începerea realizării etapei, dar se creează şi/sau se achiziţionează pe măsura necesităţii.

Începutul şi sfîrşitul fiecărei etape şi proces, trebuie să fie perfectate documentar. Documentarea proceselor de dezvoltare trebuie abordată drept un element indispensabil al dezvoltării sistemelor informaţionale, ea urmînd să se regăsească la fiecare etapă de dezvoltare.

Documentarea proceselor de instituţionalizare şi utilizare a sistemelor informaţionale

În conformitate cu legislaţia autohtonă, pentru sistemele informaţionale care conţin seturi de date este aplicabilă Legea cu privire la registre [4]. În conformitate cu prevederile acestei legi, prin registru se va înţelege totalitatea informaţiilor documentate ţinute în sisteme informaţionale automatizate, organizată în conformitate cu cerinţele stabilite. [4]

Considerăm importantă sarcina trecerii în revistă a prevederilor acestei legi, deoarece prin conţinutul acesteia este stabilit modul de instituire, înregistrare, ţinere, reorganizare şi lichidare a registrelor, precum şi reglementată modalitatea de realizare a raporturilor juridice care apar în procesul instituirii, înregistrării, ţinerii, reorganizării şi lichidării registrelor.

Din perspectivă, practică această lege se impune a fi importantă atît pentru sectorul privat cît şi pentru cel public, ori anume prin prevederile acesteia este instituţionalizat statutul juridic al registrelor, indicându-se că acestea pot fi atât registre de stat cît şi registre private, delimitând-se cadrul obligaţional diferit pentru subiecţii implicaţi în instituţionalizarea, posesia şi beneficierea de datele din registre. Evidenţa registrelor de stat se ţine prin Registrul resurselor şi sistemelor

informaţionale de stat, aprobat de Guvern. Crearea şi ţinerea Registrului resurselor şi sistemelor informaţionale de stat se efectuează de Agenţia de Guvernare Electronică [4].

În dependenţă de statul registrului, deosebim cadru obligaţional diferit şi în ceia ce priveşte documentarea acestora. Astfel, registrele de stat de bază şi cele departamentale pot fi instituite doar de către Guvern sau de o altă autoritate publică abilitată prin lege, cu adoptarea deciziei de instituire a registrului. Registrul de stat teritorial se instituie prin hotărîre a autorităţii administraţiei publice locale. La fel, remarcăm că în conformitate cu prevederile Legii cu privire la registre înainte de punerea în exploatare a sistemului informaţional automatizat destinat ţinerii registrului de stat, autoritatea publică care a instituit registrul este obligată să aprobe regulamentul cu privire la modalitatea de ţinere a registrului.

După cum am menţionat supra, documentarea proceselor de dezvoltare şi utilizare a sistemelor informaţionale se impune drept o activitate imperativă. Documentele propuse spre elaborare, sunt necesare întru îndeplinirea mai multor sarcini. Pe de o parte, prin intermediul acestora proprietarul sistemului informaţional stabileşte principiile generale în contextul cărora va fi utilizat sistemul informaţional, stabilindu-se astfel părţile posibile a fi implicate în procesul de gestionare şi utilizare a sistemului, delegându-le-se astfel roluri în sistem corespunzătoare obligaţiilor funcţionale pe care le exercită. Pe de altă parte, prin aprobarea şi publicarea Regulamentelor cu privire la ţinerea registrului este asigurat realizarea în practică a principiului transparenţei, utilizatorii sistemelor informaţionale fiind astfel informaţi despre modalităţile de utilizare a datelor şi drepturilor atribuite subiecţilor implicaţi în gestionarea informaţiei prin intermediul registrelor sau a registrelor în general.

Spre deosebire de registrele de stat, pentru registrele private nu sunt stabilite rigori stricte în ceia ce priveşte documentarea acestora. Prin prezentul articol, vom pleda însă pentru modificarea legislaţiei în aşa fel încît pentru registrele şi sistemele informaţionale să fie instituţionalizate proceduri şi rigori obligatorii de documentare. Necesitatea reglementării derivă din creşterea numărului de registre puse în circulaţie de instituţiile private, dar şi de creşterea riscurilor care apar odată cu inexistenţa unui sistem clar de reglementare, penalizare sau control.

Reglementarea sistemelor informaţionale apare drept o temă destul de polemizată atât în rândul practicienilor cît şi în rândul teoreticienilor. Reprezentanţii domeniului IT, dar şi businessului tind să se opună reglementărilor, indicând că prin stabilirea regulilor businessul şi respectiv consumatorii suportă cheltuieli suplimentare, se stopează tendinţa spre inovare, tehnologizarea tinde să se birocratizeze. De cealaltă parte sunt reprezentanţii autorităţilor publice, care pledează în favoarea instituţionalizării unor mecanisme protecţioniste, transparente şi certe [11]. Se pare totuşi că bătălia este cîtigată de susţinătorii reglementărilor, ori deja avem confirmate mai multe iniţiative în acest sens atît pe continentul american cît şi cel european. La nivel european, Comisia Europeană a propus un nou cadru legislativ

pentru sistemele ce utilizează Inteligenţa Artificială, creând iniţiative de promovare a inovaţiei în domeniu. Această propunere reprezintă prima reglementare la nivel european a unei tehnologii specifice (AI). Obiectivul noului cadru legislativ este de a uniformiza activităţile de reglementare ale dezvoltării, comercializării şi utilizării inteligenţei artificiale în conformitate cu valorile Uniunii Europene. Deşi recunoaşte beneficiile aduse de AI, Comisia doreşte să se asigure de faptul că tehnologiile de acest tip care sunt utilizate în piaţa europeană respectă drepturile fundamentale ale individului. Comisia Europeană este în mod particular preocupată de protejarea împotriva riscurilor etice şi de protecţia datelor personale, inclusiv de riscul prejudecăţilor inerente din seturile de date utilizate de tehnologiile AI. La fel, reglementarea sus indicată prevede înfiinţarea unei baze de date publice care să conţină detaliile furnizorilor de sisteme AI cu risc ridicat. Drept exemplu de stat care a optat pentru instituţionalizarea reglementării poate fi menţionat şi SUA, care depune efort prin intermediul Comisiei Federale pentru Comerţ (FTC) să asigure drepturile civile şi confidenţialitatea în comerţul online prin reglementarea practicilor neloiale şi înşelătoare, prin crearea unui Oficiu pentru Drepturile Civile, sporind gradul de protecţie împotriva Big Tech [12].

În aceiaşi ordine de idei, atragem atenţia asupra faptului, că companiile care tind să dobîndească dar şi să menţină încrederea utilizatorilor, aderă la coduri de etică sectoriale, sau adoptă de sine stătător astfel de coduri, stabilind în mod voluntar obligaţia de a elabora şi aproba, dar şi a aduce la cunoştinţa utilizatorilor reglementări care definesc cadrul de utilizare a sistemelor informaţionale, registrelor, datelor cu caracter personal, etc.

Condiţii legale impuse spre respectare în contextul dezvoltării şi implementării sistemelor informaţionale

Securitatea sistemelor informaţionale

Reţelele împreună cu sistemele şi serviciile informatice îndeplinesc un rol vital în societate, iar odată cu creşterea numărului de sisteme informaţionale propuse spre utilizare, cresc proporţional şi riscurile de securitate. Amploarea, frecvenţa şi impactul incidentelor de securitate sunt în creştere şi reprezintă o ameninţare gravă pentru funcţionarea reţelelor şi a sistemelor informatice. Sistemele respective pot să devină, de asemenea, o ţintă pentru acţiunile dăunătoare deliberate menite să afecteze sau să întrerupă funcţionarea sistemelor. Astfel de incidente pot să împiedice desfăşurarea activităţilor economice, să genereze pierderi financiare substanţiale, să submineze încrederea utilizatorilor în sistemele informaţionale propuse spre utilizare.

Astfel, constatăm că asigurarea securităţii sistemelor informaţionale, confidenţialitatea datelor prelucrate prin intermediul acestora, dar şi protecţia datelor cu caracter personal se impun drept sarcini prioritare pentru dezvoltatori atunci când aceştia concep un sistem informaţional, ori în cazul în care acest principiu nu este gândit de la început, implementarea ulterioară a principiilor de se-

curitate se poate impune drept una deficitară. Poate fi abordată drept exemplu în acest sens, cauza C- 131/ 12 Google Spain şi Google potrivit căreia principiul asigurării dreptului la protecţia datelor cu caracter personal trebuie considerat pornind chiar de la etapa de dezvoltare, iar implementarea sau punerea în uz a unui sistem care nu corespunde principiilor de protecţie a datelor poate fi considerată drept încălcare.

Obligaţia dezvoltării şi implementării sistemelor informaţionale securizate este stabilită atât la nivel internaţional cât şi la nivel naţional. Pentru ţările membre UE spre exemplu, responsabilitatea asigurării securităţii reţelelor şi a sistemelor informaţionale revine în mare măsură operatorilor de servicii esenţiale şi furnizorilor de servicii digitale. Astfel, prin Directiva 2016/1148 din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a reţelelor şi a sistemelor informatice [14] în Uniune se promoveze să se dezvolte prin cerinţe adecvate de reglementare şi practici voluntare sectoriale o cultură a gestionării riscurilor, care să implice evaluarea riscurilor şi aplicarea unor măsuri de securitate adecvate riscurilor întâmpinate. Stabilirea unor condiţii de concurenţă al căror caracter echitabil să prezinte încredere este şi ea esenţială pentru funcţionarea eficace a grupului de cooperare şi a reţelei CSIRT în scopul asigurării unei cooperări efective din partea tuturor statelor membre. La fel, potrivit reglementării sus indicate statele membre a comunităţii UE se asigură că operatorii de servicii esenţiale notifică autorităţii competente sau echipelor CSIRT, fără întârzieri nejustificate, incidentele care au un impact semnificativ asupra continuităţii serviciilor esenţiale pe care le furnizează. Notificările includ informaţii care să permită autorităţii competente sau echipelor CSIRT să stabilească orice impact transfrontalier al incidentului. Notificarea nu expune partea care notifică unei răspunderi sporite [14].

Pentru a determina importanţa impactului unui incident, se ţine cont în mod special de următorii parametri:

- numărul de utilizatori afectaţi de perturbarea serviciului esenţial;
- durata incidentului;
- distribuţia geografică în ceea ce priveşte zona afectată de incident [15].

La nivel naţional, obligativitatea asigurării securităţii informaţionale se materializează prin obligaţii diferenţiate pentru instituţiile private, instituţiile publice care utilizează TIC (cerinţe minime de nivel 1) în activitatea sa şi pentru instituţiile publice care utilizează TIC în activitatea instituţiei şi prestează servicii bazate pe TIC (cerinţe minime de nivel 2) [10].

Pentru ambele tipuri de instituţii publice, Cerinţele minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr. 201/2017 stabilesc că conducătorul autorităţilor este obligat să desemnează, prin act administrativ, persoana (subdiviziunea) responsabilă de punerea în aplicare a sistemului de management al securităţii cibernetice în instituţie şi urmează să prezinte Ministerului Tehnologiei Informaţiei şi Comunicaţiilor informaţia respectivă în termen de cinci zile lucrătoare de la desemnarea acesteia.

Astfel, întru asigurarea securităţii informaţionale, persoanei responsabile îi sunt delegate spre îndeplinire cel puţin următoarele atribuţii:

1) organizarea sistemul de management al securităţii cibernetice în instituţie conform sistemului de management al securităţii cibernetice;

2) participarea cel puţin o dată pe an, la cursurile de formare organizate de Ministerul Tehnologiei Informaţiei şi Comunicaţiilor privind securitatea cibernetică şi, respectiv, organizează cursuri pentru angajaţii instituţiei;

3) asigurarea elaborării, implementării şi respectării prevederilor următoarelor documente: planul de acţiuni pentru asigurarea securităţii cibernetice al instituţiei, politica de securitate cibernetică a instituţiei, planul de instruire şi responsabilizare în securitatea cibernetică a personalului, regulamentele interne de securitate cibernetică, procedurile de recuperare.

Politica de securitate cibernetică, în calitate de document instituţional, trebuie să include:

- scopul şi obiectivele;
- principiile de organizare internă a managementului de securitate cibernetică;
- analiza situaţiei şi vulnerabilităţilor (disponibilitate, integritate şi confidenţialitate a datelor, precum şi analiza riscurilor şi căilor de remediere);
- declaraţia managementului instituţiei de susţinere a scopului şi principiilor securităţii cibernetice în instituţie.

Planul de instruire şi responsabilizare în securitatea cibernetică a personalului instituţiei include:

- instruirea în igiena şi etica cibernetică (programe/cursuri de formare în domeniul securităţii cibernetice);
- măsurile de securitate internă privind activitatea personalului (autorizaţie de acces, stabilirea drepturilor, obligaţiilor, restricţiilor, responsabilizarea angajaţilor, monitorizarea, proceduri de asistenţă ale utilizatorilor în cazuri de urgenţă);
- măsurile de securitate privind activitatea personalului/companiilor externe cooptate (coordonarea responsabilităţilor, acorduri de nedivulgare, autorizaţie de acces, monitorizare, planul de contingenţă (intervenţie) pentru suspendarea operaţiunilor de externalizare).

Regulamentele interne de securitate cibernetică trebuie să prevadă cel puţin următoarele:

- dezvoltarea, actualizarea, modificarea, mentenanţa sistemelor informaţionale;
- gestionarea activelor şi facilităţilor de comunicaţii electronice şi tehnologia informaţiei;
- stocarea copiilor de rezervă ale datelor, precum şi ale procedurilor de control;
- păstrarea datelor de acces, de jurnalizare a activităţilor;

- monitorizarea securităţii sistemului;
- regulile de gestionare a evenimentelor de securitate;
- procedurile de utilizare a datelor în cazuri excepţionale (de urgenţă)
- procedurile de evaluare a securităţii cibernetice.

Procedurile de recuperare includ:

- stabilirea procedurilor privind copierea de rezervă şi de recuperare în cazul unui incident de securitate cibernetică;
- descrierea acţiunilor măsurabile de recuperare;
- atribuirea responsabilităţilor pentru restabilirea funcţionalităţilor;
- stabilirea procedurilor de notificare [10].

La fel, ca şi în cazul documentării proceselor de instituţionalizare, prezentul articol pledează pentru extinderea obligatorie a acestor prevederi şi către sistemele informaţionale private, în special asupra celor care prezintă sau pot prezenta riscuri sporite.

Propunerea este orientată spre a impune sarcini suplimentare numai atunci când un sistem este susceptibil să prezinte un grad ridicat de risc pentru drepturile fundamentale şi pentru siguranţă. Pentru sistemele care nu prezintă un risc ridicat, pot fi impuse doar obligaţii foarte limitate în materie de transparenţă, de exemplu în ceea ce priveşte furnizarea de informaţii pentru a semnala utilizarea unui sistem de inteligenţă artificială atunci când interacţionează cu oamenii. Pentru sistemele cu grad ridicat de risc, cerinţele privind calitatea ridicată a datelor, documentaţia şi trasabilitatea, transparenţa, supravegherea umană, acurateţea şi robusteţea sunt strict necesare pentru a atenua riscurile la adresa drepturilor fundamentale. Existenţa unor norme armonizate şi a unor orientări de sprijin şi instrumente de asigurare a conformităţii îi va ajuta pe furnizori şi pe utilizatori să respecte cerinţele prevăzute şi va reduce la minimum costurile acestora.

Drepturile fundamentale şi sistemele informaţionale

După cum am menţionat în conţinutul acestui articol, pe lîngă beneficii, noile sisteme informaţionale se pot impune şi printr-un cadru de risc sporit. Este de menţionat în special pericolele care pot afecta în mod negativ drepturile fundamentale. Drept urmare, prezentul articol reliefează importanţa încadrării legale a sistemelor informaţionale, şi obligativitatea etică a dezvoltatorilor de a verifica compatibilitatea sistemului cu respectul pentru drepturile fundamental umane. În legislaţia autohtonă, nu avem o obligaţii comprehensive în acest sens, însă acestea derivă din principiile generale de funcţionare a sistemelor informaţionale şi registrelor consacrate prin prevederile art. 14 a Legii cu privire la informatică [2] şi prevederile articolului 4 a Legii cu privire la registre [4]. În sensul celor menţionate, trebuie verificate dezvoltările tehnologice în coraport cu cel puţin următoarele drepturi: respectarea vieţii private şi protecţia datelor cu caracter personal, nediscriminarea şi egalitatea între femei şi bărbaţi. La fel, vom considera necesare

exerciţiile de verificare a acţiunilor de descurajator în ceea ce priveşte dreptul la libertatea de exprimare şi la libertatea de întrunire, de a asigura protecţia dreptului la o cale de atac eficientă şi la un proces echitabil, a dreptului la apărare şi a prezumţiei de nevinovăţie, precum şi a principiului general al bunei administrări. Drept mecanism general acceptat de verificare se impune testarea. Obligaţiile privind testarea ex ante, gestionarea riscurilor şi supravegherea umană vor facilita, de asemenea, respectarea altor drepturi fundamentale prin reducerea la minimum a riscului unor decizii eronate.

Concluzii

Practica de dezvoltare şi implementare a sistemelor informaţionale trebuie abordată drept un mecanism complex de acţiuni, iar eforturile statale urmează a fi consolidate în vederea fortificării capacităţii instituţiilor care gestionează sisteme informaţionale private să răspundă aşteptărilor utilizatorilor dar şi provocărilor contemporane. Realizarea acţiunilor îndreptate spre reglementarea cadrului obligaţional de utilizare a sistemelor informaţionale, sporirea cerinţelor de securitate, fortificarea capacităţii de a asigura drepturile fundamentale va contribui per ansamblu la sporirea încrederii în sistemele informaţionale şi dezvoltarea domeniului IT. Asumarea acţiunilor de fortificare, se impun drept prioritare la această etapă, atât pentru proprietarii de sisteme informaţionale cât şi pentru autorităţile publice împuternicite cu obligaţii de reglementare. Iminenţa este determinată şi de ascensiunea pe plan mondial a tendinţelor de dezvoltare a sistemelor bazate pe inteligenţă artificială. Astfel, în cazul în care măsurile de reglementare şi responsabilizare nu vor fi întreprins la moment, ulterior poate fi prea târziu.

Bibliografia şi resursele Web

1. Consiliul European, Reuniunea extraordinară a Consiliului European (1-2 octombrie 2020) – Concluzii, EUCO 13/20, 2020
2. Legea nr. 1069/2000 cu privire la informatică (Monitorul Oficial Nr. 73-74 art. 547)
3. Legea nr. 467/2003 cu privire la informatizare şi la resursele informaţionale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr. 6-12, art. 44);
4. Legea nr. 71/2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr. 70-73, art. 314);
5. Legea nr. 133/2011 privind protecţia datelor cu caracter personal (Monitorul Oficial Nr. 170-175 art. 492)
6. Hotărîrea Guvernului nr.794/2018 pentru aprobarea Regulamentului privind organizarea şi funcţionarea Sistemului informaţional judiciar (Monitorul Oficial al Republicii Moldova, 2018, Nr. 321-332 art. 857)
7. Hotărîrea Guvernului nr. 561/2007 cu privire la Sistemul Informaţional

Integrat Vamal **(** Monitorul Oficial al Republicii Moldova, 2007, Nr. 74-77 art. 597)
8. Hotărîrea Guvernului nr. 1401/2007 privind aprobarea Concepţiei Sistemului informaţional integrat automatizat "Migraţie şi azil" **(**Monitorul Oficial al Republicii Moldova, 2007, Nr. 203-206 art. 1478)
9. Hotărîrea Guvernului nr. 715/2018 cu privire la aprobarea Conceptului tehnic al Sistemului informaţional automatizat „Registrul de stat al achiziţiilor publice" (MTender) (Monitorul Oficial al Republicii Moldova, 2018, Nr. 309-320, art Nr : 847)
10. Hotărârea Guvernului nr. 201/2017. Cerinţele minime obligatorii de securitate cibernetică, aprobate prin (Monitorul Oficial al Republicii Moldova, 2017, nr. 109-118, art. 277);
11. Debate continues over the pros and cons of regulating artificial intelligence, disponibil la: https://www.osborneclarke.com/insights/debate-continues-pros-cons-regulating-artificial-intelligence
12. Federal Trade Commission Must Protect Civil Rights, Privacy in Online Commerce, comunicat de presă, 4 august, 2021, disponibil la: https://www.lawyerscommittee.org/federal-trade-commission-must-protect-civil-rights-privacy-in-online-commerce/
13. Cauza C- 131/ 12 Google Spain şi Google, disponibil la: https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN
14. Directiva 2016/1148 din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a reţelelor şi a sistemelor informatice, https://eur-lex.europa.eu/legal-content/ro/TXT/HTML/?uri=CELEX:32016L1148
15. Directiva 2016/1148 din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a reţelelor şi a sistemelor informatice, https://eur-lex.europa.eu/legal-content/ro/TXT/HTML/?uri=CELEX:32016L1148