

Domnului Ministru Marcel Ioan Boloș
Ministerul Cercetării, inovării și digitalizării
office@research.gov.ro

Domnului Președinte Dragoș - Cristian Vlad
Autoritatea pentru digitalizarea României
cloud@adr.gov.ro

25 martie 2022

Stimate domnule ministru Marcel Ioan Boloș,
Stimate domnule președinte Dragoș – Cristian Vlad,

Asociația pentru Tehnologie și Internet (ApTI) este o organizație neguvernamentală care acționează pentru protecția drepturilor civile digitale prin garantarea unui mediu digital liber și deschis.

Comentariile de mai jos privesc aspectele prioritare din textul Ordonanței de urgență care reglementează guvernanta Cloud-ului Guvernamental. Subiectul pe care se va pronunța ApTI este acela al drepturilor civile digitale – aceasta este expertiza organizației. Nu ne vom pronunța cu privire la alte aspecte, deși este evident că textul acestei OUG este destul de vag și ar fi nevoie ca el să fie clarificat pe multe alte aspecte (de ex. care tipuri de servicii publice electronice vor intra în acest Cloud și care nu; care sunt limitele de utilizare pentru fiecare serviciu public electronic și cum sunt stabilite ele, etc.).

1. Proiectul trebuie promovat ca o lege, nu ca un OUG.

În ciuda unor declarații generice, nu este absolut nimic în preambulul sau în expunerea de motive a Ordonanței de Urgență care să justifice o situație extraordinară, a cărei reglementare nu poate fi amânată și care impune adoptarea de măsuri imediate pe calea ordonanței de urgență. Proiectul Cloud-ului guvernamental există în spațiul public în diverse formate și idei de cel puțin 10 ani, iar inacțiunea guvernelor în acest domeniu nu reprezintă o justificare în acest sens. Nici măcar termenele din PNRR, care au fost asumate de către România în mod voluntar, fără a preciza că

vreunul din actele normative adoptate ar trebuie să fie trecut printr-o procedură de urgență și evitând procesul democratic normal, nu justifică adoptarea acestui act normativ fără contribuția Parlamentului și fără o dezbatere largă a acestui proiect.

Mai mult, proiectul reglementează inclusiv aspecte legate de prelucrarea datelor personale în Cloud-ul Guvernamental și implicarea serviciilor secrete în acest proces, aspecte care pot aduce atingere dreptului la viața privată, ca drept fundamental precizat de Constituția României.

Conform art. 115 (6) din Constituție, *“ordonanțele de urgență nu pot fi adoptate în domeniul legilor constituționale, nu pot afecta regimul instituțiilor fundamentale ale statului, drepturile, libertățile și îndatoririle prevăzute de Constituție, drepturile electorale și nu pot viza măsuri de trecere silită a unor bunuri în proprietate publică.”*

Ne facem datoria de vă atrage atenția, la fel ca și în trecut, că a continua cu aceasta practică va duce la declararea neconstituționalității acestui OUG strict pe motive formale - deci practic și noi și dvs. o sa pierdem timp prețios în implementarea acestui proiect, în loc să beneficiem de un proces transparent, previzibil și deschis de consultare publică pentru a găsi cea mai bună variantă de act normativ pentru societatea românească.

2. SRI nu poate asigura securitatea datelor personale dintr-un sistem informatic, pentru că scopul său legal este de a culege informații (deci inclusiv date).

Propunerea de OUG prevede în art. 6 (1) că SRI va *“asigura securitatea cibernetică a Cloud-ului Guvernamental prin cunoașterea, prevenirea și contracararea atacurilor cibernetice, inclusiv a celor complexe, de tip APT, (...)”*.

Mai mult proiectul de ordonanță de urgență menționează în art. 9 că SRI va avea un rol de operator asociat, împreună cu celelalte instituții, deci va fi supus obligațiilor din GDPR (Regulamentul 679/2016), pentru că activitățile din proiect nu intră în domeniul exceptat de GDPR.

Subliniem că protecția împotriva amenințărilor de tip APT nu se poate realiza printr-o singură

soluție software și hardware, ci prin mai multe (protecția APT presupune integrarea de soluții cum ar fi sandbox, CASB, EDR, threat intelligence, forensic, analytics etc.). Rezultă că pentru a asigura protecția împotriva APT, **SRI va gestiona toate echipamentele și aplicațiile de securitate, inclusiv cu acces la întreg traficul de la sau spre Cloud.**

Amintim că obligația legală unică a SRI, conform art. 2 din Legea nr. 14/1992 este de a desfășura *“activități pentru culegerea, verificarea și valorificarea informațiilor (...)”*.

Practic SRI nu poate garanta nici respectarea principiilor prelucrării datelor personale (în special folosirea datelor exclusiv în scopul furnizării serviciilor din cloud) și nici îndeplinirea obligației de securitate a datelor (nici ca operator, nici ca împuternicit), pentru că obligația sa legală din Legea nr. 14/1992 este contrară celor din Regulamentul UE 679/2016 GDPR (în special articolele 5, 6 și 32).

De altfel și **jurisprudența Curții Constituționale a României este constantă în acest domeniu**, chiar anterior intrării în vigoare a GDPR, o argumentație similară fiind inclusă în Decizia nr. 17/2015 a CCR cu privire la altă structură din cadrul SRI care ar fi trebuit să joace un rol similar cu cel pe care SRI urmează să îl joace acum în implementarea Cloud-ului guvernamental:

“Or, în condițiile în care Centrul Național de Securitate Cibernetică constituie o structură militară, în cadrul unui serviciu de informații, subordonată ierarhic conducerii acestei instituții, deci sub un control direct militar-administrativ, apare cu evidență că o atare entitate nu îndeplinește condițiile cu privire la garanțiile necesare respectării drepturilor fundamentale referitoare la viață intimă, familială și privată și la secretul corespondenței.”¹

În mod normal, această atribuție de a asigura securitatea sistemului ar putea să fie asigurată de DNSC - *“Principala responsabilitate a DNSC este asigurarea securității cibernetice a spațiului cibernetic național civil”* (art. 3 alin. 1 OUG 104/2021). Din păcate, DNSC are, conform art. 5 litera (b), funcția de autoritate competentă la nivel național de reglementare, supraveghere și control și asigură reglementarea și gestionarea securității cibernetice a României și a spațiului cibernetic național civil, iar conform punctului 5 de la același articol îndeplinește atribuțiile de

¹ Vezi par. 57 din DECIZIA CCR nr. 17 din 21 ianuarie 2015 asupra obiecției de neconstituționalitate a dispozițiilor Legii privind securitatea cibernetică a României.

autoritate națională pentru furnizorii (...) de servicii tip cloud. Deci DNSC nu poate să aibă un rol de *control* și de *controlat* în același timp.²

În acest context singura variantă legală instituțional ar fi păstrarea atribuțiilor de securitate informatică a Cloud-ului la STS, iar dacă acesta are nevoie de un ajutor specializat, el ar putea să achiziționeze serviciile de securitate informatică din sectorul privat, de la orice auditor sau laborator acreditat de către DNSC (furnizor care va avea rolul de persoană împuternicită în contextul prelucrării datelor personale).

3. Trebuie precizate clar pozițiile instituțiilor, din punctul de vedere al prelucrării datelor personale, pentru furnizarea serviciilor de Cloud.

Propunerea din articolul 9 actual este neclară și imprecisă cu privire la poziția corectă a părților din punctul de vedere al prelucrării datelor personale conform GDPR. Astfel trebuie să se precizeze clar că:

- pentru furnizarea serviciilor de Cloud (indiferent care dintre ele), instituțiile care îl administrează au rolul de **persoane împuternicite**, iar entitățile găzduite au rolul de **operatori**. Pe cale de consecință art. 9 alin. 3 din proiectul de OUG ar trebui modificat complet.
- instituțiile care îl administrează pot avea rolul de **operatori asociați** pentru alte date prelucrate, însă doar pentru activitățile comune de prelucrare unde stabilesc împreună scopul și mijloacele de prelucrare (de ex. pentru “asigurarea securității” doar STS are atribuții, deci nu pot fi ambele instituții operatori asociați).

Ca atare propunem modificarea în consecință a art. 9, după cum urmează:

Art. 9 (1) Pentru toate prelucrările de date cu caracter personal din cadrul serviciilor publice electronice accesibile prin Cloud-ul Guvernamental, entitățile găzduite vor avea calitatea de

² A se vedea mutatis mutandis explicațiile CCR din cazul legii securității cibernetice mai sus citate în care s-a propus ca o singură instituție să aibă toate atribuțiile din domeniul reglementat: “Or, o atare situație este inacceptabilă într-o societate guvernată de principiile statului de drept. Dispozițiile legale sunt susceptibile de a genera o aplicare discreționară, chiar abuzivă a legii, fiind nepermis ca toate atribuțiile din domeniul reglementat să fie concentrate în sarcina unei singure instituții.”

operatori de date cu caracter personal, iar ADR și STS calitatea de persoane împuternicite, în contextul și cu atribuțiile specifice prevăzute de Regulamentul UE 679/2016. Conform art. 27 (3) din acest Regulament, părțile vor stabili un contract care stabilește obiectul și durata prelucrării, natura și scopul prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate și obligațiile și drepturile operatorului, în funcție de tipologia de serviciu accesată și a serviciului public electronic stabilit de entitatea găzduită.

(2) ADR și STS pot prelucra date cu caracter personal, în calitate de operatori asociați, pentru activitățile comune de prelucrare a datelor prevăzute la art. 3 – 7 din prezenta lege în contextul și cu atribuțiile specifice prevăzute de Regulamentul UE 679/2016. Pentru restul activităților specifice de prelucrare, ADR sau STS vor avea rolul de operator de date cu caracter personal, în mod independent. În aceste cazuri revine părților obligația de a informa corect persoanele vizate cu privire la rolul și activitățile de prelucrare conform art. 13-14 din Regulamentul UE 679/2016.

(3) Înainte de a demara orice proces de dezvoltare software a Cloud-ului, se va semna un acord între aceste instituții publice menționate la art. 1 alin. (2) care va detalia într-un mod transparent responsabilitățile fiecăruia în ceea ce privește îndeplinirea obligațiilor care le revin în temeiul Regulamentului General de Protecție a Datelor, în special în ceea ce privește exercitarea drepturilor persoanelor vizate și îndatoririle fiecăruia de furnizare a informațiilor prevăzute la articolele 13 și 14 din Regulamentul UE 679/2016, conform obligațiilor din articolul 26 din Regulamentul UE 679/2016, și se va realiza o analiză de evaluare a impactului conform art. 35 din Regulamentul UE 679/2016, inclusiv prin consultarea ANSPDCP.

4. O lege nu trebuie să interzică anumite soft-uri doar pentru că au o licență liberă.

Art. 10 alin. (2) și (3) prevede faptul că “softul aferent migrării” în Cloud “sunt” proprietate publică a statului, la fel ca și “componentele aferente securității cibernetice” (presupunem că este vorba despre hardware și software).

Textul pare a face confuzie între proprietatea asupra bunurilor fizice, unde există conceptul de proprietate publică a statului, și drepturile de proprietate intelectuală, unde contează titularul

acestor drepturi, iar conceptul de proprietate publică nu are niciun sens.

Chiar și condițiile în care textul ar vrea să promoveze ideea că titularul drepturilor de proprietate intelectuală asupra acestor programe de calculator trebuie să fie ADR, trebuie să subliniem că în practică o să fie aproape imposibil acest lucru (sau o să fie posibil la niște costuri imense și inutile), în condițiile în care - având în vedere și tipurile diferite de sisteme care vor trebui migrate - aceste programe de calculator există sub diverse tipologii de licențe - comerciale, libere, ca serviciu (SaaS) sau poate chiar titularul drepturilor de proprietate intelectuală este altă instituție publică (de ex. Ministerul Finanțelor sau STS sau chiar Guvernul României).

5. Este necesară organizarea unei dezbateri publice.

În calitate de asociație legal constituită și în temeiul art. 6 alin. 7 din Legea nr. 52/2003 privind transparența decizională în administrația publică, vă adresăm prezenta cerere pentru a solicita **organizarea unei întâlniri în care să se dezbată public proiectul de Ordonanței de urgență care reglementează guvernarea Cloud-ului Guvernamental**. Reamintim că, potrivit art. 6 alin. 7 din Legea nr. 52/2003, organizarea unei întâlniri în care să se dezbată public proiectul de lege este **obligatorie** dacă acest lucru a fost cerut în scris de către o asociație legal constituită. Având în vedere că în mass-media au apărut mai multe critici ale acestui proiect de ordonanță de urgență, credem că este necesară o dezbateră reală a tuturor aspectelor menționate.

Cu considerație,

Bogdan Manolea, Director executiv

[+40 721 205 603](tel:+40721205603)

www.apti.ro