ROMÂNIA
Avocatul Poporului
Str. George Vraca nr. 8, Sector 1, București
www.avp.ro
Tel.: +40-21-312.71.01, Fax: +40-21-312.49.21, E-mail: avp@avp.ro
Tel. dispecerat: +40-21-312.71.34, **E-mail**: petitii@avp.ro

RĂSPUNS COLECTIV

la sesizările primite din partea unor petenți și organizații guvernamentale cu privire la analizarea potențialului de neconstituționalitate al Ordonanței de urgență a Guvernului nr. 89/2022 privind înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizat de autoritățile și instituțiile publice, precum și oportunitatea sesizării Curții Constituționale a României cu privire la acest act normativ

Cu privire la sesizările înregistrate la instituția Avocatul Poporului, având ca obiect neconstituționalitatea dispozițiilor Ordonanței de urgență a Guvernului nr. 89/2022 privind înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizat de autoritățile și instituțiile publice, precum și sesizarea Curții Constituționale în acest sens, **vă aducem la cunoștință următoarele aspecte:**

(i) Delegarea legislativă este reglementată de art. 115 din Constituția României. Astfel, potrivit dispozițiilor art. 115 alin. (4) *„Guvernul poate adopta ordonanțe de urgență numai în situații extraordinare a căror reglementare nu poate fi amânată, având obligația de a motiva urgența în cuprinsul acestora*".

Așadar, în cazul ordonanței de urgență, nu este necesară intervenția prealabilă a Parlamentului pentru ca Guvernul să o poată emite. Totuși, ordonanța de urgență impune existența unor situații deosebite și respectarea anumitor elemente *sine qua non*. Guvernul poate emite ordonanțe de urgență numai în **situații extraordinare** a căror reglementare nu poate fi amânată, **urgența trebuie motivată** în cuprinsul acestora, pot fi emise în domeniul legilor organice, cu excepția domeniului 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 public**. O ordonanță de urgență trebuie să indeplinească *simultan* toate aceste condiții.

În ceea ce privește ordonanțele de urgență ale Guvernului facem și precizarea că, în acest sens, Constituția României, instituie prin dispozițiile cuprinse în art. 115 alin. (4) - (6), competența Guvernului de a emite ordonanțe de urgență, în condițiile prevăzute expres în însăși norma constituțională. Cu ocazia dezbaterilor parlamentare, forul legislativ suprem - Parlamentul - are competența de a cenzura ordonanța de urgență a Guvernului atât sub aspectul legalității, cât și al oportunității, dispozițiile art. 115 alin. (8) din Constituție statuând că prin legea de aprobare sau de respingere se vor reglementa, dacă este cazul, măsurile necesare cu privire la efectele juridice produse pe perioada de aplicare a ordonanței. Ca atare, în procedura parlamentară, cele două Camere ale Parlamentului realizează atât un control de constituționalitate nejurisdicțional, cât și unul de oportunitate asupra ordonanței de urgență. Parlamentul nu numai că are competența de a respinge prin lege ordonanța de urgență, dacă apreciază că aceasta este neconstituțională, ci chiar obligația.

Referitor la **criticile extrinseci motivate din perspectiva lipsei caracterului urgent** al adoptării actului normativ, apreciem că argumentele invocate în expunerea de motive pot fi subsumate conceptelor constituționale de situație extraordinară și urgență.

Analizând obiectiv *Expunerea de motive* (motivarea situației extraordinare) a ordonanței de urgență criticată se constată că, printre altele, actul normativ a fost adoptat având în vedere faptul că:

- una dintre direcţiile de acţiune pentru asigurarea securităţii naţionale prevăzute în Strategia naţională de apărare a ţării pentru perioada 2020-2024, aprobată prin Hotărârea Parlamentului României nr. 22/2022, este reprezentată de realizarea infrastructurii necesare pentru digitalizarea României, cu scopul eficientizării aparatului administrativ şi al creşterii calităţii serviciilor publice, pentru transpunerea în realitate a acestei direcţii de acţiune fiind necesară implementarea unei infrastructuri de tip cloud în sectorul public,

- în jalonul nr. 153 din Planul naţional de redresare şi reziliență, se specifică faptul că implementarea unei infrastructuri de tip cloud în sectorul public cuprinde construcţia de centre de date Tier IV de la momentul conceperii pentru cele două centre principale, Tier III de la momentul conceperii pentru cele secundare, infrastructuri specifice găzduirii de sisteme informatice on-premise, iar de construirea urgentă a acestora depind transferul la timp al finanţării de către Comisia Europeană şi sporirea rezilienţei sistemelor şi reţelelor informatice ale statului român. În acest context, situaţia fiscal-bugetară reclamă accesarea fără întârzieri a finanţărilor disponibile prin PNRR cu respectarea termenului-limită de 30 iunie a.c. asumat de România prin PNRR pentru îndeplinirea jalonului.

- lipsa reglementării, la nivel primar, generează imposibilitatea implementării pe altă cale a soluţiilor prevăzute în ordonanţa de urgenţă, fiind domenii care capacitează întreaga administraţie publică centrală, managementul informaţiilor la nivelul serviciilor publice, dinamica serviciilor publice, adaptarea acestora la noile realităţi tehnologice şi digitale, precum şi reacţia de răspuns a statului la noile provocări în domeniul conceptului de securitate extinsă,

- neadoptarea ordonanţei de urgenţă poate avea drept consecinţe pierderea a peste 500 milioane de euro, pierderea credibilităţii României în faţa Comisiei Europene şi a partenerilor occidentali şi afectarea şansei României de a se adapta digital la noile realităţi privind guvernarea electronică, interoperabilitatea sistemelor informatice, regimul administrării virtuale a datelor din sectorul public şi relevanţa acestora pentru buna funcţionare a statului român,

- transformarea digitală este un obiectiv de interes strategic naţional, care cuprinde procesul de transformare digitală atât la nivelul serviciilor publice din România, cât şi la nivelul mediului de afaceri, în cazul căruia acest proces se referă la mecanismele de automatizare a proceselor de producţie şi robotizarea acestora, cu impact asupra competitivităţii şi calităţii produselor şi serviciilor pe piaţa europeană,

- în conformitate cu Strategia europeană pentru cloud computing, Strategia europeană privind datele, Declaraţia comună a statelor membre ale Uniunii Europene privind Noua generaţie de cloud în Europa, Cadrul european de interoperabilitate, precum şi aspectele prezentate anterior, se impune reglementarea de urgenţă a cadrului legal necesar realizării unei infrastructuri de tip cloud în sectorul public şi a cadrului legal de organizare şi funcţionare a infrastructurilor informatice şi a serviciilor de tip cloud în procesul de transformare digitală.

De asemenea, potrivit celor susținute de autoritățile competente în domeniu, cu privire la înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizat de autoritățile și instituțiile publice, *tehnologia cloud computing generează numeroase beneficii pentru instituțiile publice: scalabilitate, elasticitate, performanță ridicată, rezistență și siguranță, eficientizare a costurilor, dar și rentabilitate.* ***Cloud-ul guvernamental oferă infrastructura necesară*** *pentru toate instituțiile care au obligația să preia și să stocheze informațiile beneficiarilor de servicii publice, precum și să le protejeze datele. De asemenea,* ***cloud-ul guvernamental are capacitatea de a optimiza funcționarea tuturor serviciilor publice electronice*** *din România*[1].

[1] Autoritatea pentru Digitalizarea României, https://www.adr.gov.ro/cloud/.

Totodată, potrivit Ministerului Cercetării, Inovării și Digitalizării *cloud-ul guvernamental este o componentă esențială a procesului de transformare digitală, care va facilita trecerea României către o economie bazată pe date, sigură și dinamică, o economie digitală aliniată cu direcțiile strategice de acțiune ale Uniunii Europene în ceea ce privește guvernanța datelor.* Mai mult, ***cloud-ul guvernamental este asumat prin Programul Național de Redresare și Reziliență (PNRR) ca pilon fundamental al accelerării transformării digitale a administrației (investiția în cloud fiind una dintre cele de importante din întreg PNRR, cu o valoare de 574 milioane de euro finanțați prin Componenta C7 PNRR – Transformare digitală).*** Astfel, *acesta va reuni toate proiectele aflate deja în implementare din domeniul e-guvernării, stabilind un cadrul legal care să stabilească o modalitate unitară privind dezvoltarea sistemelor informatice la nivelul autorităților și instituțiilor publice.* Așadar, *cloud-ul guvernamental va produce beneficii precum reducerea costurilor și creșterea calității activităților sectorului public, inclusiv în ceea ce privește prestarea serviciilor publice*[2].

În ceea ce privește **justificarea urgenței** actului normativ în cauză, art. 115 alin. (6) din Constituție prevede că: "*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*". Din interpretarea textului constituțional se poate deduce că interdicția adoptării de ordonanțe de urgență este totală și necondiționată atunci când menționează că "*nu pot fi adoptate în domeniul legilor constituționale*" și că "*nu pot viza măsuri de trecere silită a unor bunuri în proprietate publică*". În celelalte domenii prevăzute de text, ordonanțele de urgență nu pot fi adoptate dacă "afectează", dacă au consecințe negative, dar, în schimb, pot fi adoptate dacă, prin reglementările pe care le conțin, au consecințe pozitive în domeniile în care intervin (a se vedea **Deciziile Curții Constituționale nr. 1/2014 și nr. 55/2022**).

În continuare, Curtea Constituțională a arătat că „*verbul «a afecta» este susceptibil de interpretări diferite, așa cum rezultă din unele dicționare. Din punctul de vedere al Curții, aceasta urmează să rețină numai sensul juridic al noțiunii, sub diferite nuanțe, cum ar fi: «a suprima», «a aduce atingere», «a prejudicia», «a vătăma», «a leza», «a antrena consecințe negative»*" (a se vedea, în acest sens, Decizia nr.1189/2008). Cu alte cuvinte, Guvernul nu are nicio competență de legiferare în domeniul legilor constituționale (*„ordonanțele de urgență nu pot fi adoptate în domeniul legilor constituționale"*) și cel al legilor care vizează măsuri de trecere silită a unor bunuri în proprietate publică (*„ordonanțele de urgență nu pot viza măsuri de trecere silită"*), acestea fiind în competența de legiferare exclusivă a Parlamentului, sub toate aspectele pe care le reglementează în conținutul lor normativ, și are o competență de legiferare limitată în domeniile care vizează regimul instituțiilor fundamentale ale statului, drepturile, libertățile și îndatoririle prevăzute de Constituție și drepturile electorale (*„ordonanțele de urgență nu pot afecta"*), cu privire la care aplicarea interdicției constituționale exprese este condiționată de adoptarea unor reglementări care suprimă, aduc atingere, prejudiciază, vatămă, lezează, în general, antrenează consecințe negative asupra drepturilor, libertăților și îndatoririlor constituționale.

În această din urmă ipoteză, dacă reglementările nu produc consecințele juridice menționate, **Guvernul partajează competența de legiferare cu Parlamentul, fiind ținut însă de obligația de a motiva în conținutul actului normativ existența unei situații extraordinare, a cărei reglementare nu poate fi amânată, precum și urgența reglementării.**

Așadar, ambele interdicții constituționale prevăzute la art.115 alin.(6) de a nu adopta ordonanțe de urgență care „pot afecta" regimul instituțiilor fundamentale ale statului (Parlamentul) au avut în vedere

[2] Potrivit adresei nr. 3163/05.07.2022 transmisă instituției Avocatul Poporului (înregistrată sub nr. 16443/05.07.2022), prin care a fost expus punctul de vedere al Ministerului Cercetării, Inovării și Digitalizării cu privire la constituționalitatea și oportunitatea Ordonanței de Urgență nr. 89/2022 privind unele măsuri pentru adoptarea sistemului de guvernanță a Platformei de cloud guvernamental, precum și pentru stabilirea cadrului legal de organizare și funcționare a infrastructurilor informatice și a serviciilor de tip cloud în procesul de transformare digitală.

restrângerea competenței Guvernului de a legifera în aceste domenii esențiale în locul Parlamentului, iar nu lipsirea totală de competența de a legifera în materie.

Altfel spus, în măsura în care justifică o situație extraordinară și urgența reglementării, iar conținutul normativ al actului nu afectează drepturile cetățenilor și, implicit, modul de constituire al Parlamentului, deci regimul unei instituții fundamentale a statului, **Guvernul poate adopta ordonanțe de urgență în materia supusă controlului** (a se vedea, *ad similis*, **Decizia Curții Constituționale nr. 150/2020**).

Pentru aceste argumente, întrucât nu există o interdicție absolută cu privire la competența Guvernului de a legifera în materia reglementată prin Ordonanța de urgență a Guvernului nr.89/2022, nu se poate reține încălcarea, *de plano*, a dispozițiilor art.61 alin.(1) coroborate cu art.115 alin.(6) din Constituție, ci este necesar să se stabilească dacă actul normativ afectează o instituție fundamentală a statului, precum și drepturi fundamentale ale cetățenilor.

În acest sens, examinând susținerile petenților se constată că aceștia critică ordonanța de urgență cu privire la *reglementarea aspectelor 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***. De asemenea, petenții rețin că *art. 9 propus reușește **să nu reglementeze nimic clar**, oferind posibilitatea instituțiilor Ministerul Cercetării, Inovării și Digitalizării, Autoritatea pentru Digitalizarea României, Serviciul de Telecomunicații Speciale și Serviciul Român de Informații) **să joace orice rol de prelucrare** (operator sau persoană împuternicită) și copiind referințe la legislațiile actuale care oricum ar fi aplicabile, dar lăsând aspectele practice fie nereglementate (ceea ce înseamnă probabil că vor trebuie reglementate contractual sau prin alte legislații secundare între părți), fie făcând trimitere directă la o viitoare legislație secundară [art. 10 alin. (8)]*.

Totodată, se apreciază că prin art. 6 din aceeași ordonanță de urgență „***se creează atribuții suplimentare ale SRI**, de asigurare a securității cibernetice a cloud-ului [atribuție aproape identică cu cea a STS din art. 5 alin. (4)] contrar atribuțiilor legale ale acestui serviciu stabilite conform art. 2 din Legea nr. 14/1992, respectiv aceea 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 persoană împuternicită), 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)".*

Față de aceste critici se impun următoarele precizări.

Potrivit art. 1 din ordonanța de urgență criticată, aceasta *reglementează regimul juridic general privind înființarea, administrarea și dezvoltarea, la nivel național, a unei infrastructuri de tip cloud hibrid, denumită Platforma de cloud guvernamental*. De asemenea, se prevede că această platformă va funcționa conform Ghidului de guvernanță a platformei de Cloud guvernamental aprobat, prin hotărâre a Guvernului, în termen de maximum 90 de zile de la data intrării în vigoare a ordonanței de urgență.

Autoritățile responsabile de realizarea Cloudului privat guvernamental sunt Ministerul Cercetării, Inovării și Digitalizării (MCID) și Autoritatea pentru Digitalizarea României (ADR), în colaborare cu Serviciul de Telecomunicații Speciale (STS) și Serviciul Român de Informații (SRI), conform competențelor prevăzute de ordonanța de urgență în cauză și a legilor speciale în care sunt reglementate competențele fiecărei instituții sau autorități în parte.

În acest caz, potrivit art. 3 din actul normativ criticat, Ministerul Cercetării, Inovării și Digitalizării (MCID) stabilește „*(1)Politicile, strategia, standardele și criteriile de implementare, operare, utilizare, întreținere și dezvoltare ulterioară a Platformei se stabilesc prin hotărârea prevăzută la art. 1 alin. (4). (2)**Cadrul de management și stocare a datelor în Platformă, inclusiv stabilirea categoriilor de date prelucrate în Platformă și găzduite de Cloudul privat guvernamental, cloud privat, cloud public, după caz, se realizează prin hotărâre de Guvern, la propunerea MCID**, în termen de maximum 90 de zile de la data intrării în vigoare a hotărârii prevăzute la art. 1 alin. (4)".*

Mai mult, conform art. 5 din aceeași ordonanță de urgență se prevede că ***Serviciul de Telecomunicații Speciale (STS) asigură infrastructura de bază a Cloudului privat guvernamental.*** Astfel, **STS asigură** implementarea, administrarea tehnică și operațională, securitatea cibernetică, mentenanța și **dezvoltarea ulterioară a serviciilor specifice Cloudului privat guvernamental, prevăzute la art. 2 lit. k), l) și q)**, precum și accesul securizat, conectivitatea și interconectarea la serviciile specifice Cloudului privat guvernamental pentru entitățile găzduite sau interconectate în cloud și securitatea cibernetică a Cloudului privat guvernamental prin prevenirea și contracararea atacurilor cibernetice, pentru serviciile prevăzute la art. 2 lit. k), l) și q), inclusiv a atacurilor de tip DDoS îndreptate împotriva Cloudului privat guvernamental, în conformitate cu atribuțiile prevăzute prin actele normative în vigoare.

Pentru îndeplinirea acestor atribuții STS va achiziționa serviciile de proiectare și asistență tehnică, lucrările de investiții, inclusiv instalațiile, dotările și echipamentele tehnologice aferente clădirii, precum și echipamentele hardware, programele software, aplicațiile informatice și licențele necesare realizării, dezvoltării ulterioare, mentenanței și funcționării serviciilor prevăzute la art. 2 lit. k), l) și q) din Cloudul privat guvernamental.

În ceea ce privește atribuțiile Serviciul Român de Informații (SRI), acestea sunt reglementate de art. 6 din ordonanța de urgență, care prevede că *„(1)**SRI asigură securitatea cibernetică a Cloudului privat guvernamental** prin **cunoașterea, prevenirea și contracararea atacurilor, amenințărilor, riscurilor și vulnerabilităților cibernetice**, inclusiv a celor complexe, de tip APT, îndreptate împotriva serviciilor Cloudului privat guvernamental **prevăzute la art. 2 lit. u) și a entităților găzduite**. (2) **SRI cooperează cu STS, conform competențelor fiecărei instituții**, pentru cunoașterea, prevenirea și contracararea atacurilor cibernetice complexe, de tip APT, îndreptate împotriva serviciilor specifice Cloudului privat guvernamental prevăzute la art. 2 lit. l) și q), prin schimbul nemijlocit și automat al informațiilor referitoare la incidentele de securitate, fără a transfera date de conținut”*. Totodată, *„(4) SRI asigură implementarea, administrarea tehnică și operațională, mentenanța, precum și dezvoltarea ulterioară a serviciilor de securitate cibernetică ale Cloudului privat guvernamental, prevăzute la alin. (1)”*.

În vederea îndeplinirii atribuțiilor prevăzute la art. 5 și 6, STS și SRI asigură echipamentele hardware, programele software, aplicațiile informatice și licențele necesare în acest scop, ***conform competențelor prevăzute prin prezenta ordonanță de urgență*** [art.7 din ordonanța de urgență].

Așadar, din examinarea textelor de lege indicate mai sus, reiese faptul că, SRI, în calitate de organ de stat specializat în securitatea națională a României, asigură securitatea cibernetică a Cloudului privat guvernamental exclusiv în ceea ce privește amenințările, riscurile și vulnerabilitățile cibernetice, inclusiv a celor complexe, de tip APT, îndreptate împotriva serviciilor Cloudului privat guvernamental **prevăzute la art. 2 lit. u) și a entităților găzduite.**

Ca atare, **atribuțiile SRI**, stabilite conform actului normativ criticat, se referă doar la asigurarea securității cibernetice a Cloudului privat guvernamental, **fără posibilitatea de a transfera și prelucra date de conținut din cloud**. În consecință, **SRI, în acest caz, nu poate desfășura activități specifice de culegere a informațiilor, ci doar cele specifice de securitate cibernetică**.

În situații similare, Curtea Constituțională a apreciat că *„tocmai datorită naturii și specificului primei etape (de reținere și stocare a datelor), din moment ce legiuitorul consideră necesară reținerea și stocarea datelor, prin **ea însăși doar această operațiune nu contravine dreptului la viață intimă, familială și privată, ori secretului corespondenței**. **Nici Constituția și nici jurisprudența Curții Constituționale nu interzic stocarea preventivă, fără o ocazie anume, a datelor de trafic și de localizare, cu condiția însă ca accesul la aceste date și utilizarea lor să fie însoțite de garanții și să respecte principiul proporționalității**”*. Prin urmare, Curtea a apreciat că *„abia raportat la cea de-a doua etapă, aceea a accesului și a utilizării acestor date, se ridică problema conformității reglementărilor legale criticate cu dispozițiile constituționale. Cu privire la cea de-a doua etapă a mecanismului reținerii datelor generate sau prelucrate de furnizorii de rețele publice de comunicații electronice și de furnizorii de servicii de comunicații electronice destinate publicului, respectiv accesul*

la aceste date şi folosirea lor, [...], Curtea a constatat că legea trebuie să ofere garanţiile necesare protecţiei dreptului la viaţă intimă, familială şi privată, a secretului corespondenţei şi a libertăţii de exprimare ale persoanelor ale căror date stocate sunt accesate (**Decizia Curții Constituționale nr. 295/2022, paragrafele 60, 61 și 137**).

În ceea ce privește **atribuțiile SRI**, în jurisprudența sa (a se vedea Decizia nr. 55/2022), Curtea Constituțională **a realizat o distincție între activitățile SRI permise și cele prohibite din punct de vedere constituțional.**

Astfel, Curtea a recunoscut constituționalitatea implicării SRI exclusiv în activități care au ca scop obținerea de informații care să asigure cunoașterea, prevenirea și înlăturarea amenințărilor interne sau externe la securitatea națională, fiind **prohibite din punct de vedere constituțional atribuțiile care țin de activitatea procesual penală**, activitate destinată constatării existenței sau inexistenței unei infracțiuni, identificării persoanei care a săvârșit-o, cunoașterii împrejurărilor care contribuie la aflarea adevărului în procesul penal, necesare pentru justa soluționare a cauzei, având ca scop tragerea la răspundere penală a persoanei vinovate. Așa fiind, Curtea a constatat că scopul în care sunt utilizate activitățile întreprinse în domeniul securității naționale este diferit de cel al activității procesual penale. Primele se axează pe cunoașterea, prevenirea și înlăturarea amenințărilor interne sau externe cu scopul realizării securității naționale, iar celelalte au ca scop tragerea la răspundere penală a persoanelor care au săvârșit infracțiuni. Astfel, într-o interpretare sistematică și teleologică, rezultă că **Legea nr. 51/1991** și **Codul de procedură penală au finalități diferite**, care se reflectă și în scopul pentru care este dispusă autorizarea unor activități specifice culegerii de informații care presupun restrângerea exercițiului unor drepturi sau libertăți fundamentale ale omului/măsura supravegherii tehnice. Cu alte cuvinte, existența unei situații care constituie amenințare la adresa securității naționale nu presupune în mod automat și necesar pregătirea sau săvârșirea unei infracțiuni contra securității naționale, mijloacele de preîntâmpinare a amenințărilor la adresa securității naționale neputându-se rezuma la combaterea infracțiunilor.

Referitor la solicitările de acces la datele încărcate în cloudul guvernamental în vederea utilizării lor de către organele de stat cu atribuții în domeniul securității naționale, se reține că **acestea nu pot fi preluate de SRI pentru a fi utilizate în activitatea acestei instituții.**

În plus, oricare dintre instituțiile implicate în activitatea și susținerea cloudului guvernamental este obligată să respecte și, după caz, să prelucreze datele cu caracter personal potrivit dispozițiilor legii și cu respectarea garanțiilor necesare protecției dreptului la viață intimă, familială și privată, a secretului corespondenței și a libertății de exprimare ale persoanelor ale căror date stocate sunt accesate.

În acest sens, conform art. 9 din ordonanța de urgență privind prelucrarea datelor cu caracter personal *„(1)În procesul de dezvoltare, implementare, administrare și asigurare a securității cibernetice a Cloudului privat guvernamental,* ***autoritățile și instituțiile publice prevăzute la art. 1 alin. (6) prelucrează date cu caracter personal****, în calitate de operator sau persoană împuternicită de către entitățile găzduite sau interconectate, după caz, în conformitate cu responsabilitățile prevăzute la art. 3-7,* ***cu respectarea reglementărilor legale aplicabile în domeniul protecției datelor cu caracter personal.*** *(2)****Prelucrarea datelor cu caracter personal prin intermediul sistemelor informatice găzduite în Platformă se realizează de către reprezentanții autorităților și instituțiilor publice, cu respectarea reglementărilor legale aplicabile în domeniul protecției datelor cu caracter personal.*** *(3)****Autoritățile și instituțiile publice prevăzute la alin. (1) și (2) respectă regimurile de acces la date prevăzute la nivel național și european și acordă angajaților și reprezentanților lor drepturile de acces la date prelucrate prin intermediul sistemelor informatice găzduite în Platformă****, după caz, în vederea îndeplinirii prevederilor prezentei ordonanțe de urgență,* ***cu respectarea prevederilor Legii nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date*** *și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), cu modificările ulterioare, Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții*

*private în sectorul comunicațiilor electronice, cu modificările și completările ulterioare, Legii nr. 363/2018 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor sau al executării pedepselor, măsurilor educative și de siguranță, precum și privind libera circulație a acestor date, precum și ale Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor). (4)**Prevederile alin. (3) sunt aplicabile și în ceea ce privește raporturile autorităților și instituțiilor publice prevăzute la alin. (1) și (2) cu părți terțe, în vederea asigurării dezvoltării mentenanței și dezvoltării ulterioare a infrastructurii și serviciilor Platformei**. (5)În aplicarea prevederilor alin. (3) și (4), **autoritățile și instituțiile publice prevăzute la alin. (1) și (2) au obligația să se asigure că datele prelucrate sunt protejate în mod adecvat împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin măsuri de asigurare a confidențialității, integrității și disponibilității acestora**. (6)**Prezenta ordonanță de urgență respectă drepturile fundamentale și principiile recunoscute de Carta drepturilor fundamentale a Uniunii Europene, inclusiv dreptul la respectarea vieții private și de familie, dreptul la protecția datelor cu caracter personal, dreptul la proprietate și integrarea persoanelor cu dizabilități, astfel încât nicio prevedere din prezentul act normativ nu trebuie să facă obiectul unei interpretări sau puneri în aplicare care nu este conformă cu Convenția pentru apărarea drepturilor omului și a libertăților fundamentale a Consiliului Europei***".

Se observă și faptul că legiuitorul a reglementat aceste garanții acordate pentru asigurarea dreptului constituțional prevăzut de art. 26, în mod direct și expres, prin actul normativ în cauză (ca reglementare cu caracter primar care se bucură de forța juridică a legii și de o stabilitate în consecință) și nu printr-un act infralegal (a se vedea **Decizia Curții Constituționale nr. 498/2018**).

De asemenea, potrivit art. 12 din actul normativ *„(1)**Autoritățile și instituțiile publice găzduite în Cloudul privat guvernamental au următoarele obligații**: **a)prelucrează datele cu caracter personal în procesul de utilizare și furnizare a serviciilor publice prin intermediul Cloudului privat guvernamental, cu respectarea reglementărilor legale aplicabile în domeniul protecției datelor cu caracter personal, și se asigură de respectarea principiilor "confidențialității prin concepție" și "securității prin concepție" asupra sistemelor informatice migrate în Cloudul privat guvernamental**; b)stabilesc modul și perioada de prelucrare a datelor cu caracter personal, modul de realizare a accesului la aceste date, precum și modul de punere în aplicare a prevederilor art. 12-20 din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE în raport cu utilizarea și furnizarea serviciilor publice prin intermediul Cloudului privat guvernamental; [...]*", iar art. 13 alin. (3) lit. d) prevede că *„infrastructurile informatice de tip cloud menționate la alin. (1) trebuie realizate și implementate astfel încât să asigure următoarele categorii de facilități: [...] d) respectarea principiilor și prevederilor privind prelucrarea datelor cu caracter personal, precum și asigurarea controlului confidențialității, integrității și disponibilității datelor prin intermediul instrumentelor specifice serviciilor de tip cloud".*

În susținerea acestor prevederi sunt și dispozițiile art. 10 din ordonanța de urgență criticată, care menționează că *„Administratorii serviciilor furnizate la nivel de IaaS, PaaS și SaaS, precum și administratorii de securitate cibernetică **asigură jurnalizarea evenimentelor și accesului la datele entităților găzduite în Cloudul privat guvernamental, în scopul efectuării unor activități de audit de conformitate periodice pe linia protecției, calității, securității și trasabilității datelor, în vederea asigurării transparenței utilizării acestora**".* Astfel, *„ADR asigură dezvoltarea unei aplicații de jurnalizare și notificare a activității de prelucrare a datelor cu caracter personal ale persoanelor vizate, destinată utilizatorilor finali ai serviciilor publice furnizate de entitățile publice găzduite în*

Cloudul privat guvernamental", iar „*MCID dispune, cel puţin anual sau ori de câte ori este necesar,* ***efectuarea unor activităţi de audit de conformitate pe linia protecţiei, calităţii, securităţii şi trasabilităţii pentru Platformă sau, după caz, pentru anumite componente ale acesteia, finanţate prin bugetul acestuia***. Totodată, „*Autorităţile prevăzute la art. 1 alin. (6) întocmesc până la finalul primului trimestru al anului în curs un raport comun cu privire la activitatea de realizare şi administrare a Cloudului privat guvernamental pentru anul precedent, pe care îl comunică comisiilor pentru tehnologia informaţiei şi comunicaţiilor ale Camerei Deputaţilor şi Senatului*".

În concluzie, orice fel de ingerință a instituțiilor și autorităților implicate în activitatea desfășurată în cloudul guvernamental, fără respectarea regimului de prelucrare a datelor cu caracter personal sau încuviințarea organelor competente în acest caz (astfel cum sunt prevăzute de art. 30 din Codul de procedură penală), se sancționează potrivit legilor indicate în mod expres în cuprinsul art. 9 din actul normativ în cauză.

Totodată, pentru considerente asemănătoare, Curtea Constituțională, prin Decizia nr. 17/2015, a apreciat că, *pentru asigurarea unui climat de ordine, guvernat de principiile unui stat de drept, democratic,* ***înființarea sau identificarea unui organism responsabil cu coordonarea problemelor de securitate a sistemelor şi rețelelor cibernetice, precum şi a informației***, *care să constituie* ***punctul de contact pentru relaționarea cu organismele similare din străinătate***, *inclusiv al cooperării transfrontaliere la nivelul Uniunii Europene,* ***trebuie să vizeze un organism civil, care să funcționeze integral pe baza controlului democratic***, *iar nu o autoritate care desfăşoară activități în domeniul informațiilor, al aplicării legii sau al apărării ori care să reprezinte o structură a vreunui organism care activează în aceste domenii. În analiza Curții,* ***opțiunea pentru desemnarea în calitate de autoritate națională în domeniul securității cibernetice a unui organism civil***, *iar nu a unei entități militare cu activitate în domeniul informațiilor,* ***se justifică prin necesitatea preîntâmpinării riscului de a deturna scopul legii securității cibernetice în sensul folosirii atribuțiilor conferite prin această lege de către serviciile de informații în scopul obținerii de informații şi date cu consecința încălcării drepturilor constituționale la viață intimă, familială şi privată şi la secretul corespondenței*** (a se vedea **Decizia Curții Constituționale nr. 17/2015**).

Or, așa cum am dezvoltat anterior, din analiza Ordonanței de urgență a Guvernului nr. 89/2022 nu rezultă că SRI ar fi desemnată autoritate națională în domeniul securității cibernetice, astfel încât să poată fi reținută o similitudine de situație cu motivele care au determinat pronunțarea de către CCR a Deciziei nr. 17/2015 prin care s-a constatat neconstituționalitatea Legii prin care Serviciul Român de Informații era desemnat ca autoritate națională în domeniul securității cibernetice, calitate în care asigura coordonarea tehnică, organizarea şi executarea activităților ce privesc securitatea cibernetică a României, iar în acest scop, **în structura SRI se preconiza să funcționeze Centrul Național de Securitate Cibernetică**.

De altfel, DIRECTIVA (UE) 2016/1148 A PARLAMENTULUI EUROPEAN ŞI A CONSILIULUI din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (aflată în fază de proiect la data pronunțării Deciziei nr. 17/2015) a fost transpusă în totalitate prin Legea nr. 362 din 28 decembrie 2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor şi sistemelor informatice, prin care CERT-RO (devenit DNSC) a fost desemnată autoritate competentă la nivel național.

Directiva NIS, în forma sa adoptată în anul 2016, nu mai conține recomandările existente în faza sa de proiect (în anul 2015, anul pronunțării Deciziei nr. 17/2015) referitoare la atribuirea calității de autoritate națională în domeniul securității cibernetice a unui organism civil. Potrivit art. 8 din Directivă, *"(1) Fiecare stat membru desemnează una sau mai multe autorități competente la nivel național privind securitatea rețelelor și a sistemelor informatice („autoritatea competentă") care acoperă cel puțin sectoarele menționate în anexa II și serviciile menționate în anexa III. Statele membre pot atribui acest rol unei autorități sau unor autorități existente. (2) Autoritățile competente monitorizează aplicarea prezentei directive la nivel național. (3) Fiecare stat membru desemnează un punct unic de contact național privind securitatea rețelelor și a sistemelor informatice („punct unic de*

contact"). Statele membre pot atribui acest rol unei autorități existente. În cazul în care un stat membru desemnează o singură autoritate competentă, aceasta servește, de asemenea, ca punct unic de contact."

În cazul României, CERT-RO (autoritate existentă la data adoptării Legii nr. 362/2018) a fost desemnată atât autoritate națională competentă, cât și punct unic de contact.

(ii) Referitor la cele susținute de către petenți facem și mențiunea că, așa cum rezultă din motivarea actului normativ criticat, în considerarea faptului că reglementările criticate vizează interesul public şi constituie situaţii extraordinare a căror reglementare nu poate fi amânată, în temeiul art.115 alin.(4) din Constituţie, Guvernul României a adoptat Ordonanța de urgență a Guvernului nr. 89/2022 privind înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizat de autoritățile și instituțiile publice (modificată conform Rectificării din 7 iulie 2022).

În acest caz, apreciem faptul că nu trebuie pierdută din vedere importanța controlului parlamentar asupra ordonanțelor de urgență, în acord cu prevederile art.115 alin.(5) din Constituţie, prin intermediul căruia legiuitorul primar poate identifica, utilizând pârghiile specific procedurii parlamentare, soluția legislativă optimă, care să corespundă exigențelor constituționale. În acest sens, Curtea Constituțională, în jurisprudența sa, a statuat că în cazul ordonanţelor de urgenţă, aprobarea de către Parlament, în procedură de urgenţă, este obligatorie, tocmai pentru că, în acest din urmă caz, evenimentul legislativ a survenit în afara unei delegări din partea titularului dreptului de a legifera, astfel încât se impune controlul parlamentar asupra actului administrativ cu forţă de lege, în temeiul art. 61 alin. (1) din Constituţie (a se vedea **Decizia Curții Constituționale nr. 366/2014**).

În consecință, având în vedere cele expuse, apreciem că, modificarea/completarea sau chiar abrogarea, de către Parlament, a normelor legale în cauză sunt evenimente legislative posibile în actuala fază a procesului legislativ, având în vedere că Parlamentul poate respinge o ordonanţă de urgenţă atât pe motive de oportunitate, cât şi de constituţionalitate. Parlamentul are competenţa discreţionară de a respinge o ordonanţă de urgenţă ori de a o abroga, modifica sau completa, după caz, cu respectarea principiilor şi prevederilor Constituţiei (a se vedea **Decizia Curții Constituționale nr. 240/2020 și nr. 68/2017**).

În cazul actului normativ în cauză precizăm că, în cadrul procesului legislativ din Parlamentul României, a fost propus spre adoptare *Proiectul de lege pentru aprobarea Ordonanţei de urgenţă a Guvernului nr.89/2022 privind înfiinţarea, administrarea şi dezvoltarea infrastructurilor şi serviciilor informatice de tip cloud utilizate de autorităţile şi instituţiile publice* (*L 428/2022*), care se află în lucru, la comisiile permanente ale Senatului.

Ca atare, **Parlamentul poate decide soarta actului normativ al Guvernului, adoptând o lege de aprobare sau de respingere** potrivit art.115 alin. (7) din Constituţie.

Aşadar, **modificarea/completarea sau chiar abrogarea, de către Parlament, a normelor legale criticate sunt evenimente legislative posibile în această fază a procesului legislativ.**

Aspectele sesizate prin petiție rămân în atenția instituției Avocatul Poporului în vederea analizării acestora după adoptarea formei finale a legii pentru aprobarea ordonanței de urgență criticată.

AVOCATUL POPORULUI,

RENATE WEBER