Republica Moldova

CURTEA CONSTITUȚIONALĂ

HOTĂRÂRE

PRIVIND EXCEPȚIA DE NECONSTITUȚIONALITATE

a unor prevederi din articolul 126 alin. (2) din Codul de procedură penală

(*garanțiile ridicării informației privind convorbirile telefonice*)

(*sesizarea nr. 49g/2023*)

CHIȘINĂU

19 decembrie 2023

În numele Republicii Moldova,
Curtea Constituțională, judecând în componența:

dnei Domnica MANOLE, *Președinte*,
dnei Viorica PUICA,
dlui Nicolae ROȘCA,
dnei Liuba ȘOVA,
dlui Serghei ȚURCAN,
dlui Vladimir ȚURCAN, *judecători*,
cu participarea dnei Iulia Vartic, *asistent judiciar*,

Având în vedere sesizarea înregistrată la 27 februarie 2023,
Examinând sesizarea menționată în ședință publică,
Având în vedere actele și lucrările dosarului,
Deliberând în camera de consiliu,

Pronunță următoarea hotărâre:

PROCEDURA

1. La originea cauzei se află sesizarea privind excepția de neconstituționalitate a unor prevederi din articolul 126 alin. (2) din Codul de procedură penală, ridicată din oficiu de dl judecător Ion Ghizdari, în cauza penală nr. 11-51/2023, pendinte la Judecătoria Ungheni.

2. Sesizarea privind excepția de neconstituționalitate a fost trimisă la Curtea Constituțională de judecătorul cazului, dl Ion Ghizdari, de la Judecătoria Ungheni, pe baza articolului 135 alin. (1) literele a) și g) din Constituție.

3. Prin decizia Curții Constituționale din 31 octombrie 2023, sesizarea a fost declarată admisibilă, fără a se prejudeca fondul cauzei.

4. În procesul examinării sesizării, Curtea Constituțională a solicitat opiniile Parlamentului, Președintelui Republicii Moldova, Guvernului, Procuraturii Generale și a Institutului de Reforme Penale.

5. În ședința publică a Curții a fost prezent dl judecător Ion Ghizdari, autorul excepției de neconstituționalitate. Parlamentul a fost reprezentat de dl Radu Radu, consultant principal al Serviciului reprezentare la Curtea Constituțională și organele de drept din cadrul Direcției generale juridice a secretariatului Parlamentului. Guvernul a fost reprezentat de dl Eduard Serbenco, secretar de stat în cadrul Ministerului Justiției.

ÎN FAPT

I. Circumstanțele litigiului principal

6. Pe rolul Judecătoriei Ungheni se află demersul Procurorului-șef al Procuraturii raionului Ungheni prin care se solicită, pe baza articolului 126 alin. (2) din Codul de procedură penală, autorizarea ridicării de la operatorii de telefonie mobilă a informației privind convorbirile telefonice ale unor persoane. La modul concret, prin demers se

solicită autorizarea ridicării informației privind destinația comunicației, tipul, data, ora și durata comunicației, tentativele de apel eșuate, echipamentul de comunicaţii al utilizatorului sau dispozitivul utilizat pentru comunicaţie (imei-ul telefonului mobil, denumirea locaţiei Cell ID), locul aflării echipamentului mobil de comunicaţii de la începutul comunicaţiei, locaţia geografică a celulei. Demersul în discuție a fost formulat în cadrul unei cauze penale privind pretinsa organizare a migrației ilegale, potrivit articolului 362^1 alin. (2) lit. c) din Codul penal.

7. În cadrul ședinței de examinare a demersului, dl judecator Ion Ghizdari a ridicat din oficiu excepția de neconstituționalitate a articolului 126 alin. (2) din Codul de procedură penală.

8. Printr-o încheiere din 24 februarie 2023, judecătorul cazului a trimis excepția de neconstituționalitate la Curtea Constituțională, în vederea examinării acesteia.

II. Legislația pertinentă

9. Prevederile relevante ale Constituției sunt următoarele:

Articolul 23
Dreptul fiecărui om de a-și cunoaște drepturile și îndatoririle

„(1) Fiecare om are dreptul să i se recunoască personalitatea juridică.

(2) Statul asigură dreptul fiecărui om de a-și cunoaște drepturile și îndatoririle. În acest scop statul publică și face accesibile toate legile și alte acte normative.

Articolul 30
Secretul corespondenței

„(1) Statul asigură secretul scrisorilor, al telegramelor, al altor trimiteri poştale, al convorbirilor telefonice şi al celorlalte mijloace legale de comunicare.

(2) De la prevederile alineatului (1) se poate deroga prin lege în cazurile când această derogare este necesară în interesele securității naționale, bunăstării economice a ţării, ordinii publice şi în scopul prevenirii infracţiunilor.”

Articolul 54
Restrângerea exercițiului unor drepturi sau al unor libertăți

„(1) În Republica Moldova nu pot fi adoptate legi care ar suprima sau ar diminua drepturile şi libertăţile fundamentale ale omului şi cetăţeanului.

(2) Exerciţiul drepturilor şi libertăţilor nu poate fi supus altor restrângeri decât celor prevăzute de lege, care corespund normelor unanim recunoscute ale dreptului internaţional şi sunt necesare în interesele securităţii naţionale, integrităţii teritoriale, bunăstării economice a ţării, ordinii publice, în scopul prevenirii tulburărilor în masă şi infracţiunilor, protejării drepturilor, libertăţilor şi demnităţii altor persoane, împiedicării divulgării informaţiilor confidenţiale sau garantării autorităţii şi imparţialităţii justiției.

(3) Prevederile alineatului (2) nu admit restrângerea drepturilor proclamate în articolele 20-24.

(4) Restrângerea trebuie să fie proporţională cu situaţia care a determinat-o şi nu poate atinge existenţa dreptului sau a libertăţii.”

10. Prevederile relevante ale Codului de procedură penală, adoptat prin Legea nr. 122 din 14 martie 2003, sunt următoarele:

Articolul 126
Temeiurile pentru ridicarea de obiecte sau documente

„(1) Organul de urmărire penală, în baza unei ordonanțe motivate, este în drept să ridice obiectele sau documentele care au importanţă pentru cauza penală dacă probele acumulate sau materialele activității speciale de investigaţii indică exact locul şi persoana la care se află acestea.

(2) Ridicarea de documente ce conțin informații care constituie secret de stat, comercial, bancar, **precum și ridicarea informației privind convorbirile telefonice** se fac numai cu autorizația judecătorului de instrucție.”

Articolul 132[1]
Dispozițiile generale privind activitatea specială de investigații

„[…]

(2) Măsurile speciale de investigații se dispun și se efectuează dacă sunt îndeplinite cumulativ următoarele condiții:

1) pe altă cale este imposibilă realizarea scopului procesului penal și/sau poate fi prejudiciată considerabil activitatea de administrare a probelor;

2) există o bănuială rezonabilă cu privire la pregătirea sau săvârșirea unei infracțiuni grave, deosebit de grave sau excepțional de grave, cu excepțiile stabilite de lege;

3) acțiunea este necesară şi proporțională cu restrângerea drepturilor şi libertăţilor fundamentale ale omului.”

Articolul 134[4]
Colectarea informației de la furnizorii de servicii de comunicații electronice

„Colectarea informației de la furnizorii de servicii de comunicaţii electronice şi a traficului de date computerizate constă în colectarea de la instituţiile de telecomunicaţii, de la operatorii de telefonie fixă sau mobilă, de la operatorii de internet a informaţiilor transmise prin canale tehnice de telecomunicații (telegraf, fax, paging, computer, radio şi alte canale), fixarea secretă a informațiilor transmise sau primite prin intermediul liniilor tehnice de legături de telecomunicaţii de către persoanele supuse măsurii speciale de investigaţii, precum și obţinerea de la operatori a informației deţinute despre utilizatorii serviciilor de telecomunicaţii, inclusiv de roaming, şi despre serviciile de telecomunicații prestate acestora, la care se atribuie:

1) posesorii numerelor de telefon;

2) numerele de telefon înregistrate pe numele unei persoane;

3) serviciile de telecomunicaţii prestate utilizatorului;

4) sursa de comunicaţii (numărul de telefon al apelantului; numele, prenumele şi domiciliul abonatului sau utilizatorului înregistrat);

5) destinaţia comunicaţiei (numărul de telefon al apelatului sau numărul la care apelul a fost rutat, redirecţionat; numele, prenumele, domiciliul abonatului sau utilizatorului respectiv);

6) tipul, data, ora şi durata comunicaţiei, inclusiv tentativele de apel eşuate;

7) echipamentul de comunicaţii al utilizatorului sau alt dispozitiv utilizat pentru comunicaţie (imei al telefonului mobil, denumirea locaţiei Cell ID);

8) locul aflării echipamentului mobil de comunicaţii de la începutul comunicaţiei, locaţia geografică a celulei."

DREPT COMPARAT

11. **În România**, organul de urmărire penală sau instanța de judecată poate dispune ca orice furnizor de rețele publice de comunicații electronice sau furnizor de servicii de comunicații electronice destinate publicului să-i comunice date referitoare la abonați, utilizatori şi la serviciile prestate de acestea (articolul 170 din Codul de procedură penală). Totuși, norma precizează că aceste date nu se referă la conținutul comunicațiilor și nici la cele care fac obiectul metodei speciale de supraveghere sau cercetare prevăzute la articolul 138 alin. (1) lit. j) din Codul de procedură penală, care vizează obținerea datelor de trafic şi de localizare prelucrate de către furnizorii de rețele publice de comunicații electronice ori furnizorii de servicii de comunicații electronice destinate publicului. Așadar, legislatorul român a făcut o distincție clară între informațiile care pot fi ridicare de la furnizorul de rețele publice de comunicații electronice pe baza articolului 170 din Codul de procedură penală și datele care pot fi obținute pe baza măsurii speciale de supraveghere sau cercetare.

12. Mai mult, articolul 152 din Codul de procedură penală al României reglementează condițiile în care organele de urmărire penală, cu autorizarea prealabilă a judecătorului de drepturi şi libertăţi, pot solicita date de trafic şi localizare prelucrate de către furnizorii de reţele publice de comunicaţii electronice ori furnizorii de servicii de comunicaţii electronice destinate publicului. **Aceste condiții se referă la**: (*i*) existența unei suspiciuni rezonabile privind **comiterea unui șir de infracțiuni menționate expres** (a se vedea alin. (1) lit. a) din articolul 152 din Codul de procedură penală); (*ii*) existența unor motive justificate pentru a se crede că datele solicitate constituie probe; (*iii*) imposibilitatea obținerii acestor probe în alt mod sau obținerea acestora ar presupune dificultăţi deosebite ce ar prejudicia ancheta ori există un pericol pentru siguranța persoanelor sau a unor bunuri de valoare; (*iv*) caracterul proporțional al limitării drepturilor și libertăţilor fundamentale, date fiind particularităţile cauzei, importanţa informaţiilor ori a probelor ce urmează a fi obţinute sau gravitatea infracţiunii.

13. Curtea Constituțională a României a reținut că datele care pot face obiectul măsurii speciale de supraveghere sau cercetare de la articolul 152 din Codul de procedură penală sunt păstrate de furnizorii de servicii de telecomunicații, au un caracter predominant tehnic și nu vizează conținutul comunicării. Totuși, aceste date conduc la concluzii foarte precise privind viața privată a persoanelor ale căror date au fost păstrate, concluzii ce pot viza obiceiurile din viața cotidiană, locurile de ședere permanentă sau temporară, deplasările zilnice sau alte deplasări, activitățile desfășurate, relațiile sociale ale acestor persoane şi mediile sociale frecventate de ele. Din acest motiv, această ingerință în dreptul la viața privată și secretul corespondenței trebuie să fie clară, previzibilă și lipsită de echivoc, astfel încât să îndepărteze, pe cât de posibil, un eventual arbitrariu sau abuz (a se vedea Decizia 440/2014 [A/R, § 56]).

14. **În Germania**, ridicarea datelor de trafic stocate de furnizorul de servicii de telecomunicații de către autoritățile de anchetă este reglementată de articolul 100g din

Codul de procedură penală. Această normă a făcut obiectul unei plângeri constituționale la Curtea Constituțională Federală a Germaniei, care a examinat compatibilitatea garanțiilor existente cu dreptul la secretul corespondenței, al trimiterilor poștale și al telecomunicațiilor prevăzut de Articolul 10 (1) din Legea fundamentală. În acest sens, Curtea a reținut că § 113a din Legea privind telecomunicațiile obliga furnizorii de servicii de telecomunicații accesibile publicului să păstreze, practic pentru o perioadă de șase luni și fără motive concrete, toate datele de trafic referitoare la telecomunicații (comunicații prin linii fixe, telefoane mobile, telefax, transmitere de mesaje text și mesaje multimedia), comunicații prin e-mail și acces la internet. Aceste date nu vizează conținutul comunicării, ci doar apelurile, durata lor și locația din care au fost efectuate. Articolul 100g din Codul de procedură penală permitea **utilizarea acestor date pentru investigarea unor infracțiuni considerabile și infracțiuni comise prin intermediul telecomunicațiilor**, fără a preciza o listă exhaustivă a acestora, iar caracterul proporțional al acestei utilizări trebuia evaluat în fiecare caz particular de judecători. Astfel, prin Decizia sa nr. 11/2010, Curtea Constituțională Federală germană a constatat că utilizarea datelor stocate în conformitate cu § 113a din Legea privind telecomunicațiile ar putea fi determinată de aproape orice faptă penală. Acest fapt nu corespunde garanțiilor consacrate de articolul 10 (1) din Legea fundamentală, pentru că extinde câmpul de aplicare al datelor stocate, inclusiv din perspectiva dreptului Uniunii Europene (a se vedea §§ 278-279).

15. În redactarea actuală, articolul 100g din Codul de procedură penală reglementează două situații în care este posibilă ridicarea datelor de trafic. Prima situație se referă la suspiciunea că o persoana **a comis una din infracțiune stabilite expres la alineatul (2) din același articol**. Cea de-a doua situație vizează comiterea unei infracțiuni prin intermediul telecomunicațiilor, în situația în care alte mijloace de stabilire a faptelor nu ar oferi nicio perspectivă de succes. Totodată, norma menționează că utilizarea datelor de localizare stocate în trecut poate fi admisă doar în cea de-a a doua situație. În primul caz, utilizarea datelor de localizare este permisă doar în legătură cu datele de trafic în timp real sau care vor apărea în viitor.

16. **În Franța**, până în 2021, ridicarea informațiilor privind conversațiile telefonice, care includeau și locația telefonului, era autorizată de procuror pentru investigarea preliminară a tuturor infracțiunilor pe baza articolului 77-1-2 din Codul de procedură penală. Totodată, geolocalizarea, ca o măsură specială de investigație, era autorizată de judecătorul de drepturi și libertăți **pentru investigarea unor infracțiuni care prevăd pedeapsa închisorii mai mare de 3 ani**. Deși ambele măsuri pot conduce la identificarea locației persoanei, printr-o interpretare a Curții de Casație le-a fost stabilit un câmp de aplicare diferit. Astfel, procedura de ridicare reglementată de articolul 77-1-2 din Codul de procedură penală putea viza doar identificarea *a posteriori* a locației generate de telefonul mobil, pe când geolocalizarea se referea la urmărirea în timp real a locației. Distincția clară făcută în jurisprudența Curții de Casație între aceste două proceduri a constituit un argument în analiza Curții Europene din hotărârea *Ben Faiza v. Franța*, 8 februarie 2018, cu privire la baza legală a ingerinței în exercițiul dreptului la viața privată (a se vedea §§ 71-72).

17. Totuși, prin Decizia nr. 2021-952 QPC din 3 decembrie 2021, Consiliul Constituțional francez a menționat că ridicarea datelor privind conversațiile telefonice nu asigură un echilibru corect între dreptul la respectarea vieții private și necesitatea investigării infractorilor. În opinia Consiliului Constituțional, legislatorul nu a oferit acestei proceduri garanții **necesare să asigure caracterul proporțional al acțiunilor de cercetare având în vedere gravitatea infracțiunii** (a se vedea §§ 13-14). După această decizie, legislatorul francez a modificat articolul 60-1-1 din Codul de procedură penală și a stabilit că ridicarea datelor de trafic și locație a telefonului poate fi dispusă dacă infracțiunea vizată p**revede pedeapsa închisorii mai mare de 3 ani**, dacă infracțiunea a fost comisă prin intermediul comunicațiilor electronice și doar pentru a identifica autorul infracțiunii.

18. Gradul ridicat de intruziune prin identificarea locației persoanei prin intermediul telefonului mobil a fost comparat în cazul *Carpenter v. United States,* 585 U.S, 22 iunie 2018, cu cel al supravegherii prin intermediul brățării electronice. Președintele Curții Supreme a Statelor Unite ale Americii, judecătorul John Roberts, a scris în opinia majoritară din această cauză că înregistrările privind locația telefonului mobil ridică probleme din perspectiva vieții private și mai mari decât monitorizarea GPS a unui vehicul. Un telefon mobil își urmărește fidel proprietarul dincolo de străzile publice și în reședințele private, în cabinetele medicale, la sediile partidelor politice și în alte locații care pot fi identificate. În această cauză, Curtea Supremă a refuzat să aplice teoria părții terțe, care presupune existența unei așteptări reduse privind protecția confidențialității informației atunci când persoana oferă voluntar această informație unor persoane terțe. Ea a notat că, în afară de deconectarea telefonului, nu există altă cale pentru a evita stocarea datelor de localizare. Prin urmare, Curtea Supremă a conchis că ridicarea a peste 12 000 de puncte de localizare a telefonului mobil pentru o perioadă de 127 de zile, pe care s-a bazat parțial condamnarea dlui Carpenter pentru comiterea unui jaf, nu a respectat garanțiile Amendamentului al patrulea din constituție.

Jurisprudența relevantă a Curții de Justiție a Uniunii Europene

19. În hotărârea din cauza *Tele2 Sverige și Watson și Alții*, C-203/15 și C-698/15, din 21 decembrie 2016, care avea la bază trimiteri preliminare din partea Curții de Apel Administrative din Stockholm, Suedia, și a Curții de Apel din Anglia și Țara Galilor, Curtea de Justiție a Uniunii Europene a reținut că articolul 15 § 1 din Directiva privind confidențialitatea și comunicațiile electronice se opune legislației care permite accesul autorităților la datele de trafic si la datele de localizare stocate dacă: (a) scopul pe care îl urmărește **nu este limitat la combaterea infracționalității grave** și (b) un asemenea acces nu este supus unui control prealabil de către un tribunal sau de un alt organ independent.

20. Constatările au fost confirmate în jurisprudența ulterioară a Curții de Justiție a Uniunii Europene referitoare la accesul autorităților la datele de trafic. De exemplu, în cauza *Prokuratuur*, C-746/18, 2 martie 2021, Curtea de Justiție a concretizat că articolul 15 § 1 din Directivă **permite accesul la datele de trafic sau datele de localizare stocate doar în scopul combaterii crimelor grave sau amenințării grave la adresa securității**, indiferent de durata perioadei pentru care se solicită accesul la datele de trafic sau de volumul datelor disponibile în această privință. Totodată, Curtea

de Justiție a menționat că acest acces trebuie autorizat în fața unui organ independent, și nu de către Ministerul Public, care gestionează urmărirea penală (a se vedea, în mod similar, *Commissioner of the Garda Síochána și Alții*, nr. C-140/20, 5 aprilie 2022).

21. Totodată, în hotărârea din 2 octombrie 2018, din cauza *Ministerio Fiscal*, C-207/16, Curtea de Justiție a considerat că accesul autorităților la date cum ar fi numele, prenumele și, dacă este necesar, la adresele proprietarilor de SIM carduri activate cu un telefon mobil furat nu reprezintă o ingerință suficient de gravă și, prin urmare, este permisă pe baza articolului 15 § 1 din Directiva privind confidențialitatea și comunicațiile electronice, chiar dacă nu este justificată de necesitatea prevenirii și investigării infracțiunilor grave.

ÎN DREPT

I. **Argumentele autorului excepției de neconstituționalitate**

22. Autorul excepției susține că textul „precum și ridicarea informației privind convorbirile telefonice” din articolul 126 alin. (2) din Codul de procedură penală este neclar, pentru că nu stabilește condițiile în care poate fi dispusă ridicarea informației și nici categoriile de informații care pot fi ridicate. Astfel, acest procedeu probatoriu, care poate fi aplicat în privința tuturor categoriilor de infracțiuni, reprezintă o ingerință neprevăzută de lege în exercițiul dreptului la secretul corespondenței, în sensul articolului 8 din Convenție.

23. Totodată, autorul afirmă că, în lipsa categoriilor precise de informații, ridicarea poate viza toate informațiile prevăzute la articolul 134^4 din Codul de procedură penală. Totuși, articolul 134^4 din Codul de procedură penală reglementează o măsură specială de investigație care poate fi dispusă doar ca o măsură *ultima ratio*, necesară și proporțională și doar dacă există o bănuială rezonabilă cu privire la pregătirea sau săvârșirea unei infracțiuni grave, deosebit de grave sau excepțional de grave. Pe de altă parte, controlul judecătoresc al ridicării informației privind convorbirile telefonice vizează doar proporționalitatea procedeului probatoriu.

24. Așadar, deși ambele măsuri permit o ingerință la fel de intruzivă în dreptul la secretul corespondenței, Codul de procedură penală a stabilit condiții generale pentru aplicarea articolului 126 alin. (2), în detrimentul celor precise aplicabile măsurii speciale de investigație prevăzută la articolul 134^4.

25. În fine, autorul conchide că prevederea contestată este contrară articolelor 23 și 30 din Constituție

II. Argumentele autorităților și organizațiilor care și-au prezentat opiniile

26. Președintele Republicii susține că norma contestată reglementează un procedeu probatoriu care trebuie autorizat de judecătorul de instrucție. În acest sens, judecătorul de instrucție este obligat să detalieze mandatul de ridicare a informației privind convorbirile telefonice, stabilind limitările necesare care să asigure proporționalitatea ingerinței în exercițiul dreptului la secretul corespondenței. La modul concret, judecătorul trebuie să aibă în vedere caracterul necesar al ridicării, gravitatea infracțiunii pentru care se solicită ridicarea informației, existența unei suspiciuni

rezonabile privind comiterea infracțiunii, caracterul proporțional al ridicării și modul în care vă fi realizată ridicarea informației.

27. Totodată, cu referire la informațiile care pot fi ridicate pe baza acestui procedeu probatoriu, opinia prezentată de Președintele Republicii face trimitere la articolul 134^4 din Codul de procedură penală. Așadar, pe baza normei contestate pot fi solicitate de la operatorii de telefonie fixă sau mobilă aceleași informații ca în cadrul măsurii speciale de investigație prevăzute de articolul 134^4 din Codul de procedură penală.

28. În opinia prezentată de Parlament se menționează că norma contestată reprezintă un procedeu probatoriu care constă în ridicarea informației privind conversațiile telefonice. Având în vedere natura informațiilor care sunt ridicate pe baza acestui procedeu probatoriu, măsura în discuție comite o ingerință în dreptul persoanei la secretul corespondenței. Totuși, Parlamentul susține că această ingerință este prevăzută de lege, legea este clară și previzibilă, urmărește un scop legitim, iar caracterul proporțional al acesteia trebuie examinat în fiecare caz particular de către judecătorul de instrucție. Astfel, pentru că există garanții suficiente să asigure respectarea dreptului la secretul corespondenței, Parlamentul invită Curtea să respingă argumentele autorului sesizării ca fiind neîntemeiate.

29. În opinia prezentată Curții, Guvernul menționează că „informații privind convorbirile telefonice” înseamnă informații ca apelurile efectuate și recepționate, tentativele de apel eșuate, numărul la care apelul a fost redirecționat, data, ora și durata convorbirilor și altele. Mai mult, Guvernul subliniază că această noțiune este utilizată în articolul 134^4 din Codul de procedură penală, care enumeră informațiile privind conversațiile telefonice care pot fi solicitate de la furnizorul de servicii de comunicație.

30. Totodată, Guvernul susține că există o practică judiciară consolidată în această privință, așa cum menționează și autorul sesizării, în care instanța de recurs casează încheierile de respingere și autorizează ridicarea informațiilor privind conversațiile telefonice pe baza articolului 126 din Codul de procedură penală, aplicând condițiile generale valabile pentru toate acțiunile de urmărire penală. Așadar, în opinia Guvernului, judecătorul de instrucție trebuie să verifice dacă ingerința este legală, urmărește un scop legitim și este proporțională, atunci când admite sau respinge demersul procurorului de ridicare a informațiilor privind conversațiile telefonice.

31. Cu referire la pretinsul paralelism legislativ între norma contestată și măsura specială de investigație prevăzută la articolul 134^4 din Codul de procedură penală, Guvernul subliniază că acestea reprezintă două acțiuni procesuale distincte din mai multe considerente. Pe baza articolului 126 din Codul de procedură penală pot fi ridicate informații privind conversațiile telefonice care deja sunt stocate de furnizorul de servicii de comunicație, pe când măsura specială de investigație de la articolul 134^4 vizează informații care nu sunt cunoscute la momentul solicitării. Mai mult, ridicarea de informații privind conversațiile telefonice reprezintă o acțiune care se realizează de ofițerul de urmărire penală și se consumă din momentul obținerii informațiilor. Pe de altă parte, măsura specială de investigație de colectare a informației de la furnizorii de servicii de comunicații electronice se realizează de ofițerul de investigație și este dispusă pentru o perioadă de până la 30 de zile cu posibilitatea prelungirii până la 6 luni. De asemenea, pentru autorizarea măsurii speciale de investigație trebuie să fie întrunite condițiile de la articolul 132^1 alin. (2) din Codul de procedură penală, iar

pentru autorizarea procedeului probatoriu de la articolul 126 din Codul de procedură penală este necesar să se cunoască exact locul și persoana la care se află aceste informații.

32. În fine, Guvernul susține că problema ridicată de autoul sesizării reprezintă o chestiune de aplicare și de interpretare a legii, sarcină care le revine instanțelor de drept comun, și invită Curtea să declare inadmisibilă sesizarea.

33. În opinia prezentată de Procuratura Generală se menționează că procedeul probatoriu de ridicare a informațiilor privind conversațiile telefonice reprezintă un mijloc indispensabil pentru investigarea infracțiunilor ușoare sau mai puțin grave. Procuratura susține că, deși normă contestată nu abundă în texte explicative, practica judiciară existentă a stabilit câmpul de aplicare al acesteia.

34. Cu referire la paralelismul legislativ pe care îl critică autorul sesizării, Procuratura susține că articolul 126 reglementează o acțiune procesuală diferită de cea prevăzută la articolul 134^4 din Codul de procedură penală. Procuratura Generală subliniază că aceste două acțiuni procesuale sunt distincte, invocând argumente similare cu cele din opinia Guvernului (a se vedea § 31 *supra*).

35. Totodată, Procuratura Generală susține că pe baza articolului 134^4 din Codul de procedură penală pot fi colectate informații care nu sunt cuprinse de noțiunea „informații privind convorbirile telefonice”, cum ar fi informația despre utilizatorii serviciilor de telecomunicație, inclusiv roaming, și despre serviciile prestate acestora.

36. În concluzie, Procuratura Generală susține că judecătorul de instrucție trebuie să aprecieze legalitatea, necesitatea și proporționalitatea ingerinței atunci când autorizează ridicarea informațiilor privind conversațiile telefonice, înlăturând astfel orice dubii privind interpretarea și aplicarea normei contestate.

37. În opinia prezentată de Institutul de Reforme Penale se menționează că ridicarea informațiilor privind conversațiile telefonice reprezintă o ingerință în exercițiul dreptului la secretul corespondenței. Deși această ingerință este prevăzută de lege, în opinie se notează că norma nu stabilește la modul concret categoria de infracțiuni pentru care este aplicabilă, așa cum o impune articolul 8 din Convenție. Formularea generică pe care o are articolul 126 din Codul de procedură penală conduce la ideea că această ingerință poate fi comisă și în cazul investigării infracțiunilor ușoare. Totodată, norma nu reglementează cercul de persoane care pot fi vizate de această ingerință și nici durata pentru care poate fi dispusă măsura în discuție.

38. Institutul de Reforme Penale consideră că aceste omisiuni se datorează modificării esențiale a Codului de procedură penală ca urmare a implementării considerentelor Curții Europene din cauza Iordachi și alții v. Republica Moldova, 10 februarie 2009. Deși majoritatea acțiunilor procesuale care comit o ingerință similară în exercițiul dreptului la viața privată au fost calificate ca măsuri speciale de investigație, articolul 126 alin. (2) a rămas în redactarea pe care o are încă din 2003, când a fost adoptat Codul de procedură penală.

39. În concluzie, Institutul susține că articolele 126 alin. (2) și 134^4 din Codul de procedură penală vizează informații similare și este dificil, la modul practic, să se determine aplicabilitatea acestora.

III. Aprecierea Curții Constituționale

A. Admisibilitatea

40. Prin Decizia sa din 31 octombrie 2023, Curtea a confirmat respectarea, în prezenta cauză, a condițiilor de admisibilitate a unei sesizări, stabilite în jurisprudența sa constantă.

41. Curtea a observat că excepția de neconstituționalitate, ridicată din oficiu, este formulată de subiectul căruia i s-a conferit acest drept, pe baza articolului 135 alin. (1) literele a) și g) din Constituție.

42. Obiectul sesizării îl constituie textul „precum și ridicarea informației privind convorbirile telefonice” din articolul 126 alin. (2) din Codul de procedură penală. Curtea a constatat că această prevedere nu a făcut anterior obiect al controlului de constituționalitate.

43. Excepția de neconstituționalitate a fost ridicată într-o cauză penală privind comiterea unei pretinse infracțiuni mai puțin grave în care partea acuzării solicită autorizarea ridicării informației privind convorbirile telefonice pe baza articolului 126 alin. (2) din Codul de procedură penală. Așadar, Curtea a admis că prevederea contestată ar putea fi aplicată la soluționarea cauzei.

44. În sesizare, autorul excepției a afirmat că prevederea contestată din articolul 126 alin. (2) din Codul de procedură penală contravine articolelor 23 (*dreptul fiecărui om de a-și cunoaște drepturile și îndatoririle*) și 30 (*secretul corespondenței*) din Constituție.

45. În jurisprudența sa, Curtea a subliniat că articolul 23 din Constituție nu poate fi invocat de sine stătător. Pentru a fi incident, autorul sesizării trebuie să demonstreze, în mod argumentat, existența unor ingerințe în drepturile garantate de Constituție. Abia în cadrul analizei caracterului justificat al ingerinței, Curtea poate aplica prevederile acestui articol (a se vedea DCC nr. 54 din 13 aprilie 2021, § 26; DCC nr. 161 din 29 noiembrie 2022, § 12).

46. Cu privire la incidența articolului 30 din Constituție, Curtea a reținut că acesta garantează caracterul secret al scrisorilor, al telegramelor, al altor trimiteri poștale, al convorbirilor telefonice şi al celorlalte mijloace legale de comunicare.

47. Totodată, articolul 8 din Convenția Europeană a Drepturilor Omului îi garantează persoanei dreptul la respectarea vieții sale private, de familie, a domiciliului său și a corespondenței sale.

48. Curtea a reținut în jurisprudența sa că articolul 8 din Convenția Europeană a Drepturilor Omului, împreună cu jurisprudența care-l dezvoltă, stă la baza interpretării articolului 28 din Constituție (a se vedea HCC nr. 29 din 12 decembrie 2019, § 39; HCC nr. 14 din 8 august 2023, § 40). Deși aspectele privind respectarea secretului corespondenței intră în câmpul de aplicare al dreptului la respectarea vieții private, Constituția Republicii Moldova garantează un drept separat la articolul 30. Prin urmare, Curtea a analizat dacă problema de constituționalitate ridicată de autorul sesizării face incident dreptul la respectarea secretului corespondenței, așa cum este garantat de articolele 30 din Constituție și 8 din Convenție.

49. În jurisprudența sa, Curtea Europeană a menționat că, în sensul articolului 8 din Convenție, comunicațiile telefonice se includ în noțiunea de „viață privată” și de „corespondență” (a se vedea *Iordachi și alții v. Republica Moldova*, 10 februarie 2009, § 29).

50. În cauza *Malone v. Regatul Unit*, 2 august 1984, Curtea Europeană a analizat, pentru prima data, dacă procesul de „contorizare", care implică utilizarea unui dispozitiv care înregistrează numerele apelate de pe un telefon și timpul și durata fiecărui apel, interferează cu vreun drept garantat de articolul 8 din Convenție. Deși Guvernul reclamat a susținut că, prin însăși natura sa, contorizarea trebuie deosebită de interceptarea comunicațiilor, Curtea Europeană nu a putut accepta că utilizarea datelor obținute astfel nu ridica vreo problemă pe baza articolului 8 din Convenție. În consecință, ea a reținut că înregistrările contorizării, în special, a numerelor apelate, constituie un element integrant al conversațiilor telefonice, iar divulgarea acestor informații poliției, fără acordul persoanei, constituie o ingerință în dreptul garantat de articolul 8 din Convenție (a se vedea *Malone v. Regatul Unit,* 2 august 1984, §§ 83 – 84).

51. Această constatare a fost reamintită de Curtea Europeană în cauza *Savotchko v. Republica Moldova*, 28 martie 2017, care viza transmiterea de către compania de telefonie al cărei acționar unic este statul a informației privind serviciile de telefonie fixă oferite reclamantei și utilizarea acestora împotriva ei în contextul procedurilor civile privind succesiunea. Astfel, utilizarea informației referitoare la conversațiile telefonice, în special momentul în care au fost efectuate și durata acestora, precum și numerele apelate, poate ridica o problemă în sensul articolului 8 din Convenție, aceste elemente constituind „o parte integrantă a comunicațiilor telefonice" (a se vedea *Savotchko v. Republica Moldova,* 28 martie 2017, § 29).

52. Așadar, Curtea a constatat că informațiile privind conversațiile telefonice cad sub incidența noțiunii de corespondență și sunt protejate de articolul 30 din Constituție și articolul 8 din Convenție. Mai mult, Curtea a menționat că aceste informații pot include datele de transfer sau datele de localizare care sunt stocate de furnizorii de rețele și/sau servicii de comunicații electronice în mod obligatoriu, pe baza articolului 20 alin. 3) lit. c) din Legea comunicațiilor electronice nr. 241 din 15 noiembrie 2007.

53. Totodată, ingerința în dreptul la respectarea vieții private poate fi justificată doar dacă, pe baza articolului 8 § 2 din Convenție, aceasta este prevăzută de lege, urmărește unul sau mai multe scopuri legitime la care face trimitere § 2 și este necesară într-o societate democratică pentru a atinge un asemenea scop. Expresia „prevăzută de lege" impune ca măsura contestată să aibă atât o bază în legea națională, cât și să fie compatibilă cu preeminența dreptului, care este expres menționată în Preambulul Convenției și inerent în obiectul și scopul articolului 8. Astfel, legea trebuie să întrunească exigențele calității: aceasta trebuie să fie accesibilă persoanei vizate și previzibilă în efectele pe care le produce (a se vedea *Roman Zakharov v. Rusia* [MC], 4 decembrie 2015, §§ 227 – 228).

54. În acest sens, Curtea notează că articolul 23 alin. (2) din Constituție implică adoptarea de către legislator a unor legi accesibile și previzibile (a se vedea HCC nr. 3 din 14 ianuarie 2021, § 23).

55. Totuși, trimiterea la exigența „previzibilității" în contextul interceptării comunicațiilor nu poate fi la fel ca în multe alte domenii. Previzibilitatea în contextul special al măsurilor secrete de supraveghere, cum ar fi interceptarea comunicațiilor, impune legislației naționale un nivel suficient de claritate, astfel încât să le ofere cetățenilor indicii cu privire la circumstanțele și condițiile în care autoritățile publice

sunt îndreptățite să recurgă la aceste măsuri (a se vedea *Roman Zakharov v. Rusia* [MC], 4 decembrie 2015, § 229). Această afirmație este prezentă în jurisprudența Curții Europene referitoare la calitatea legii care permite interceptarea comunicațiilor începând cu cauza *Malone v. Regatul Unit*, 2 august 1984.

56. Totodată, standardul calității legii în acest domeniu, dezvoltat de jurisprudența recentă a Curții Europene din cauzele *Roman Zakharov v. Rusia* [MC], 4 decembrie 2015, și *Liblik și alții v. Estonia*, 28 mai 2019, a fost considerat aplicabil, *mutatis mutandis*, accesului autorităților la datele privind comunicațiile, care însă nu vizează conținutul acestora, cum ar fi date de transfer și date de localizare. Astfel, în hotărârea *Ekimdzhiev și alții v. Bulgaria*, [MC], 11 ianuarie 2022, Curtea Europeană a menționat că retenția generală de date de către furnizorii de servicii de comunicații electronice și accesul la acestea de către autorități în cazuri particulare trebuie însoțite, *mutatis mutandis,* de garanțiile aplicabile măsurilor secrete de supraveghere (§ 395).

57. În contextul celor menționate, Curtea a considerat că sesizarea pretinde o examinare în fond pe baza articolelor 23 și 30 din Constituție.

B. FONDUL CAUZEI

a) Principii generale privind exigența calității legii în contextul special al măsurilor secrete de supraveghere

58. Principiile generale care guvernează chestiunea respectării exigenței calității legii de măsurile secrete de supraveghere au fost stabilite, în detaliu, în cauza *Roman Zakharov v. Rusia* [MC], 4 decembrie 2015.

59. Reamintind că „previzibilitatea” în contextul special al măsurilor secrete de supraveghere, cum ar fi interceptarea comunicațiilor, nu poate fi la fel ca în multe alte domenii, Curtea Europeană a subliniat că aceasta nu poate presupune că persoana trebuie să prevadă când autoritățile pot să-i intercepteze comunicațiile, astfel încât să-și adapteze conduita în modul corespunzător. În special atunci când o putere nelimitată acordată executivului este exercitată în secret, riscul arbitrariului este evident. Prin urmare, este esențial să existe reguli clare și detaliate cu privire la interceptarea conversațiilor telefonice, în special având în vedere că tehnologiile disponibile devin tot mai sofisticate. Legislația națională trebuie să fie suficient de clară încât să le ofere cetățenilor indicii cu privire la circumstanțele și condițiile în care autoritățile publice sunt îndreptățite să recurgă la aceste măsuri (a se vedea *Roman Zakharov v. Rusia* [MC], 4 decembrie 2015, § 229; *Liblik și alții v. Estonia*, 28 mai 2019, § 128).

60. Mai mult, de vreme ce implementarea în practică a măsurilor secrete de supraveghere nu este supusă controlului efectuat de către persoanele vizate sau de publicul larg, marja discreționară acordată executivului sau unui judecător exprimată în termenii unei puteri nelimitate ar fi contrară preeminenței dreptului (a se vedea *Roman Zakharov v. Rusia* [MC], citat supra, § 230).

61. În jurisprudența sa cu privire la măsurile secrete de supraveghere, Curtea Europeană a dezvoltat un minim de garanții care trebuie stabilite în lege pentru a evita abuzul de putere: natura infracțiunilor care pot da naștere unui ordin de interceptare; definirea categoriilor de persoane ale căror telefoane pot fi interceptate; limitarea duratei interceptării telefonului; procedura care trebuie respectată pentru examinarea,

utilizarea și stocarea datelor obținute; măsurile de precauție avute în vedere la comunicarea informațiilor altor părți și circumstanțele în care înregistrările pot sau trebuie să fie șterse sau distruse (a se vedea *Roman Zakharov v. Rusia* [MC], § 231).

62. În cauzele în care în fața Curții Europene este contestată legislația care permite supravegherea secretă, legalitatea ingerinței este strâns legată de chestiunea îndeplinirii testului „necesității" și, prin urmare, Curtea analizează împreună exigențele „potrivit legii" și „necesității". În acest sens, „calitatea legii" presupune că legea națională trebuie să fie nu doar accesibilă și previzibilă în aplicarea sa, ci să asigure, de asemenea, că măsurile de supraveghere secrete sunt aplicabile doar atunci când sunt „necesare într-o societate democratică", în special prin oferirea de garanții adecvate și efective împotriva abuzului (a se vedea *Roman Zakharov v. Rusia* [MC], § 236, *Big Brother Watch și alții v. Regatul Unit* [MC], 25 mai 2021, § 334)

b) Principii generale privind accesul autorităților la datele de comunicații

63. În cauzele *Centrum För Rättvisa v. Suedia* [MC], 25 mai 2021, și *Big Brother Watch și alții v. Regatul Unit* [MC], 25 mai 2021, Curtea Europeană a examinat compatibilitatea legislațiilor naționale ale statelor reclamate privind regimul supravegherii secrete, inclusiv interceptarea în masă a comunicațiilor, cu dreptul la respectarea vieții private. Pentru că aceste cauze vizau interceptarea în masă, iar jurisprudența sa de la acea dată se referea la interceptarea direcționată, Curtea Europeană și-a pus problema necesității de a-și dezvolta jurisprudența. Deși nu a abordat în mod expres diferențele dintre interceptarea în masă și cea direcționată, Curtea Europeană a menționat că garanțiile celei din urmă trebuie să fie adaptate pentru a reflecta caracteristicile precise ale regimului interceptării în masă. Astfel, Curtea Europeană a stabilit că este imperios ca legislația națională să stabilească cu suficientă claritate categoriile în privința cărora interceptarea în masă a comunicărilor poate fi autorizată, circumstanțele în care comunicările unei persoane pot fi interceptate, autorizarea prealabilă de către un organ independent, controlul proporționalității și necesității măsurii întreprinse la fiecare etapă a procesului, perioada maximă pentru care poate fi dispusă măsura, procedura examinării, utilizării și stocării acestor date, precauțiile întreprinse pentru comunicarea datelor altor persoane și circumstanțele în care aceste date pot fi șterse sau distruse. Curtea Europeană a precizat că aceste garanții fundamentale constituie piatra de temelie a oricărei cereri pe baza articolului 8 referitoare la interceptările în masă (a se vedea *Centrum För Rättvisa v. Suedia* [MC], 25 mai 2021, §§ 254-262, și *Big Brother Watch și alții v. Regatul Unit* [MC], 25 mai 2021, §§ 340 – 343, § 348).

64. Curtea Europeană a pus în operă aceste principii în analiza sa dintr-o cauză recentă, *Ekimdzhiev și alții v. Bulgaria*, [MC], 11 ianuarie 2022, care a vizat inclusiv compatibilitatea legii statului reclamat referitoare la retenția și accesul datelor de comunicații. Curtea Europeană a menționat că, având în vedere dezvoltările tehnologice și sociale din ultimele două decenii în domeniul comunicațiilor electronice, în prezent, datele de comunicații pot să dezvăluie o mulțime de informații personale. Dacă sunt obținute în masă de către autorități, asemenea date pot fi utilizate pentru a reda imaginea privată a unei persoane prin cartografierea rețelelor sociale, urmărirea locației, urmărirea navigării pe internet, cartografierea tiparelor de

comunicare și pentru a obține informații referitoare la persoanele cu care a interacționat aceasta. Obținerea acestor informații prin interceptarea în masă poate fi la fel de intruzivă ca interceptarea în masă a conținutului comunicațiilor, motiv pentru care interceptarea, reținerea si ridicarea acestora de către autorități trebuie să fie analizate prin trimitere la aceleași garanții ca cele aplicabile conținutului. Din aceleași considerente, retenția generală a datelor de către furnizorii de servicii de comunicații electronice și accesul acestora de către autorități în cazuri particulare trebuie însoțite, *mutatis mutandis,* de garanțiile aplicabile măsurilor secrete de supraveghere (a se vedea §§ 394-395).

65. Curtea Europeană a reținut că dreptul bulgar reglementează de o manieră exhaustivă motivele pe baza cărora autoritățile pot solicita accesul la datele de comunicații reținute (*i.e.* protecția securității naționale, prevenirea și identificarea sau investigarea infracțiunilor grave, urmărirea persoanelor condamnate la închisoare pentru asemenea infracțiuni, urmărirea persoanelor care se află într-o situație care le poate pune viața în pericol și doar în privința datelor de localizare – desfășurarea operațiunilor de salvare a persoanelor aflate în primejdie). Mai mult, accesul la aceste date pot fi obținute doar de anumite autorități competente cu autorizarea prealabilă de către președintele tribunalului competent sau de un judecător căruia i-a fost delegată această competență. Totuși, s-a considerat că aceste garanții nu îndeplinesc standardul necesar de efectivitate în mai multe privințe. Curtea Europeană a observat că, deși cererile de acces sunt formulate în contextul procedurilor penale pendinte și este firesc să conțină informații privind pretinsa infracțiune în legătură cu care este solicitat accesul, legea nu stabilește vreo cerință expresă de a explica de ce datele în discuție sunt necesare în realitate. Astfel, legea nu stabilește clar pentru toate situațiile că accesul în fiecare caz particular poate fi solicitat și autorizat doar dacă ingerința comisă în drepturile persoanei vizate pe baza articolului 8 va fi cu adevărat necesară și proporțională (a se vedea *Ekimdzhiev și alții v. Bulgaria* [MC], § 398, §§ 400- 402).

66. Comparând această procedură cu cea a autorizării măsurilor secrete de supraveghere, Curtea Europeană a observat că legea nu le impunea autorităților care solicită accesul să ofere materiale în susținerea cererii de acces, fapt care poate să împiedice judecătorul, în multe cazuri, să verifice caracterul întemeiat al cererii. Mai mult, legea nu-i impunea judecătorului care examinează o asemenea cerere să motiveze dacă autorizarea accesului la datele de comunicații în discuție a fost, cu adevărat, necesară (*ibidem,* §§ 403 - 405).

67. Totodată, Codul de procedură penală bulgar nu reglementa procedura de stocare, accesare, utilizare, comunicare și distrugere a datelor de comunicații accesate de către autorități, iar aceste chestiuni nu erau acoperite nici de regulile privind dosarele de anchetă sau judecătorești. Prin urmare, asemenea date sunt pur și simplu păstrate în dosarele penale și pot fi accesate de oricine care are acces la acestea. Astfel, Curtea Europeană nu a putut accepta că legea nu oferă un nivel corespunzător de protecție a datelor care, uneori, vizează aspecte intime ale vieții private a unei persoane sau permit, într-un alt mod, o ingerință disproporționată în viața privată a persoanelor vizate sau în „corespondența” persoanelor juridice (a se vedea *ibidem,* [MC], § 409).

68. Un alt aspect analizat de Curtea Europeană în cauza *Ekimdzhiev și alții v. Bulgaria* prin trimitere la garanțiile aplicabile măsurilor de supraveghere secretă a

vizat notificarea persoanei despre accesul de către autorități la datele de comunicații reținute. Pe baza jurisprudenței sale, Curtea Europeană a reținut că o asemenea notificare este impusă în toate cazurile, nu doar în cele în care datele au fost accesate ilegal, de îndată ce notificarea poate fi făcută fără a pune în pericol scopul măsurii (a se vedea *Ekimdzhiev și alții v. Bulgaria* [MC], § 416).

69. În fine, pentru că reglementările naționale nu respectau în totalitate exigența „calității legii" și nu erau apte să mențină „ingerința" provocată de sistemul de retenție și de acces al datelor de comunicații în Bulgaria la ceea ce este „necesar într-o societate democratică", Curtea Europeană a constatat încălcarea articolului 8 din Convenție (a se vedea *Ekimdzhiev și alții v. Bulgaria*, [MC], § 420 - 421).

c) Aplicarea principiilor generale în prezenta cauză

70. Curtea menționează că, spre deosebire de analiza Curții Europene din cazurile *Centrum För Rättvisa v. Suedia* [MC] 25 mai 2021, și *Big Brother Watch și alții v. Regatul Unit* [MC], 25 mai 2021 *Ekimdzhiev și alții v. Bulgaria* [MC], 11 ianuarie 2022, ea nu este chemată, în prezenta cauză, să analizeze legislația referitoare la retenția și accesarea de către autorități a datelor de comunicații, ci doar să stabilească, dacă accesul la datele în discuție pe baza articolului 126 alin. (2) din Codul de procedură penală respectă standardul calității legii în sensul jurisprudenței relevante a Curții Europene.

71. Totuși, Curtea nu poate să ignore trimiterea la cadrul legal general, care permite, la modul practic, realizarea accesului autorităților la datele de comunicații. În acest sens, Curtea menționează că Legea comunicațiilor electronice, care transpune un șir de directive ale Uniunii Europene, inclusiv Directiva 2002/58/CE privind confidențialitatea și comunicațiile electronice, care a făcut obiectul trimiterilor preliminare examinate de Curtea de Justiție a Uniunii Europene (a se vedea §§ 19-21 *supra*), obligă furnizorii de rețele și/sau servicii de telecomunicații electronice să păstreze, timp de un an, informațiile privind serviciile de telefonie fixă sau mobilă și, timp de 6 luni, informațiile care țin de rețeaua Internet și să asigure prezentarea acestora organelor împuternicite în condițiile legii. Informațiile sunt generate sau procesate în timpul furnizării propriilor servicii de comunicații electronice și sunt necesare pentru identificarea și urmărirea sursei de comunicații electronice, identificarea destinației, tipului, datei, orei și duratei comunicației, identificarea echipamentului de comunicații al utilizatorului sau a altui dispozitiv utilizat pentru comunicație, identificarea coordonatelor echipamentului terminal de comunicații mobile (a se vedea articolul 20 alin. (3) lit. c) din Legea comunicațiilor electronice). Aceste informații pot fi calificate, în sensul articolului 2 din aceeași Lege, ca date de transfer și date de localizare.

72. În acest sens, Curtea notează că articolul 126 alin. (2) din Codul de procedură penală face referire la noțiunea de informații privind conversațiile telefonice. Bineînțeles, aceste informații nu vizează conținutul conversațiilor, ci reprezintă date care sunt generate sau procesate în timpul furnizării serviciilor de comunicații electronice în sensul articolului 20 alin. (3) lit. c) din Legea comunicațiilor electronice. Totodată, Codul de procedură penală oferă la articolul 134^4 o listă a informațiilor atribuite serviciilor de comunicații electronice. Acestea se referă la posesorii

numerelor de telefon, la numerele de telefon înregistrate pe numele unei persoane, la serviciile de telecomunicații prestate utilizatorului, la sursa de comunicații (numărul de telefon al apelantului, numele, prenumele şi domiciliul abonatului sau utilizatorului înregistrat), la destinația comunicației (numărul de telefon al apelatului sau numărul la care apelul a fost rutat, redirecționat, numele, prenumele, domiciliul abonatului sau utilizatorului respectiv), la tipul, data, ora şi durata comunicației, inclusiv tentativele de apel eșuate, la echipamentul de comunicații al utilizatorului sau alt dispozitiv utilizat pentru comunicație (imei-ul telefonului mobil, denumirea locației Cell ID); locul aflării echipamentului mobil de comunicații de la începutul comunicației, locația geografică a celulei.

73. Așadar, atât textul contestat din articolul 126 alin. (2), cât și articolul 134^4 punctele 1)-8) din Codul de procedură penală vizează aceleași informații păstrate de furnizorii de servicii de comunicații electronice conform articolului 20 alin. (3) lit. c) din Legea comunicațiilor electronice, *i.e.* date de transfer și de localizare.

74. În acest sens, Curtea observă că, deși vizează aceleași informații, Codul de procedură penală reglementează două proceduri diferite pe baza cărora organele de urmărire penală le pot accesa. Astfel, informațiile privind convorbirile telefonice pot fi obținute în contextul unor proceduri penale atât pe baza unui procedeu probatoriu prevăzut de articolul 126, cât și pe baza măsurii speciale de investigație reglementate de articolul 134^4 din Codul de procedură penală.

75. Totuși, această diferență a fost scoasă în evidență de autoritățile care și-au prezentat opinia în fața Curții (a se vedea §§ 31, 34 *supra*), potrivit căreia, deși vizează aceleași informații, articolul 126 alin. (2) din Codul de procedură penală permite ridicarea istoricului datelor în discuție, iar articolul 134^4 din același Cod permite supravegherea în timp real a persoanei, nu are vreo relevanță din perspectiva respectării garanțiilor aplicabile, pentru că ambele cazuri vizează accesul autorităților la informațiile privind conversațiile telefonice ale persoanelor.

76. Astfel, pentru că accesul de către autorități la informațiile în discuție trebuie să fie însoțit, *mutatis mutandis*, de garanțiile aplicabile măsurilor secrete de supraveghere, Curtea trebuie să verifice dacă textul contestat din articolul 126 alin. (2) din Codul de procedură penală oferă minimul de garanții dezvoltate de Curtea Europeană (a se vedea *Ekimdzhiev şi alții v. Bulgaria* [MC], 11 ianuarie 2022, § 395).

77. Curtea notează că, potrivit articolului 126 alin. (2) din Codul de procedură penală, informațiile privind convorbirile telefonice care au importantă pentru cauza penală pot fi ridicate de către organul de urmărire penală, cu autorizarea judecătorului de instrucție, dacă probele acumulate sau materialele activității speciale de investigație indică exact locul și persoana la care se află acestea. Așadar, se pot deduce următoarele condiții necesare ridicării informațiilor privind convorbirile telefonice: **(*i*)** să fie solicitate în cadrul unei cauze penale; **(*ii*)** să fie solicitate de către organul de urmărire penală; **(*iii*)** să fie importante pentru cauza penală; **(*iv*)** să se cunoască exact locul și persoana la care se află; **(*v*)** să existe o autorizare prealabilă din partea judecătorului de instrucție.

78. Astfel, Curtea observă că accesul organului de urmărire penală la informațiile privind conversațiile telefonice pe baza normei contestate poate fi solicitat **în contextul oricăror cauze penale**. Prin urmare, această normă nu stabilește motivele pe baza cărora autoritățile pot avea acces la informațiile privind conversațiile telefonice (a se vedea, *a contrario*, *Ekimdzhiev și alții v. Bulgaria* [MC], § 398). Mai mult, norma în discuție menționează care este autoritatea competentă să solicite accesul la aceste informații, însă nu precizează categoriile de persoane ale căror date pot fi accesate (a se vedea, *mutatis mutandis*, *Roman Zakharov v. Rusia* [MC], § 231).

79. Totodată, Curtea observă că, deși este necesară ordonanța motivată a organului de urmărire penală în care să se indice că ridicarea informațiilor privind convorbirile telefonice este importantă pentru cauza penală, această condiție nu este aptă să asigure caracterul „necesar într-o societate democratică" și proporțional al ingerinței (a se vedea, *mutatis mutandis*, *Ekimdzhiev și alții v. Bulgaria* [MC], § 402). Mai mult, în contextul precis al ridicării informațiilor privind conversațiile telefonice nu este relevantă condiția cunoașterii exacte a locului și a persoanei la care se află, pentru că în toate cazurile este vizat furnizorul de servicii de comunicații electronice (a se vedea § 71 *supra*).

80. Cu referire la condiția autorizării prealabile de către judecătorul de instrucție, Curtea reține că norma nu-i impune judecătorului să motiveze caracterul necesar și proporțional al ridicării informațiilor privind convorbirile telefonice, ci doar să verifice îndeplinirea condițiilor menționate la § 77 *supra (*a se vedea, *mutatis mutandis*, *Ekimdzhiev și alții v. Bulgaria* [MC], § 405).

81. Un alt aspect pe care articolul 126 alin. (2) omite să-l reglementeze vizează perioada pentru care poate fi dispusă obținerea informațiilor privind convorbirile telefonice. În lipsa acestei perioade, ridicarea informațiilor privind conversațiile telefonice este limitată doar de termenul maxim pentru care furnizorul de rețele și/sau de servicii de telecomunicații este obligat să le păstreze, *i.e.* un an pentru informațiile privind serviciile de telefonie fixă sau mobilă (a se vedea articolul 20 alin. (3) lit. c) din Legea comunicațiilor electronice).

82. Totodată, Curtea observă că nu este reglementată procedura notificării persoanei cu privire la informația privind conversațiile sale telefonice ridicate, iar regulile aplicabile stocării, păstrării și accesului la documentele care conțin informațiile în discuție sunt cele aplicabile documentelor care constituie probe, conform cerințelor generale prevăzute la articolul 157 din Codul de procedură penală.

83. Având în vedere considerentele sale de la §§ 78 - 82 *supra*, Curtea constată că procedura ridicării informațiilor privind convorbirile telefonice conform articolului 126 alin. (2) din Codul de procedură penală nu corespunde în totalitate condițiilor minime impuse de jurisprudența Curții Europene și garanțiilor prevăzute de articolele 23 și 30 din Constituție.

84. Totodată, Curtea notează că, în cazul măsurii speciale de investigație, articolele 132^1 și 134^4 din Codul de procedură penală prevăd anumite condiții și garanții în acest sens. Această măsură se autorizează de judecătorul de instrucție și trebuie să

îndeplinească cumulativ condițiile articolului 132^1 alin. (2) din Codul de procedură penală, care reglementează dispoziții generale privind activitatea specială de investigație. Astfel, măsura de la articolul 134^4 din Codul de procedură penală (*colectarea informației de la furnizorii de servicii de comunicații electronice*) trebuie să fie o *ultima ratio*, să vizeze o bănuială rezonabilă cu privire la pregătirea sau comiterea unei infracțiuni grave, deosebit de grave sau excepțional de grave, cu excepțiile stabilite de lege, și să aibă un caracter necesar și proporțional cu restrângerea drepturilor persoanei. Potrivit articolului 132^4 alin. (6) din Codul de procedură penală, aceasta poate fi dispusă pentru o perioadă de 30 de zile cu posibilitatea de a fi prelungită întemeiat până la 6 luni. De asemenea, articolul 132^5 din Codul de procedură penală reglementează procedura de consemnare a măsurilor speciale de investigații, de informare a persoanelor supuse acestor măsuri, de păstrare și distrugere a informațiilor obținute pe baza măsurilor speciale de investigație.

85. Așadar, Curtea nu poate identifica vreun motiv rezonabil care justifică o abordare legislativă diferită a condițiilor și garanțiilor ridicării informațiilor privind convorbirile telefonice conform articolului 126 alin. (2) și a colectării informațiilor similare în conformitate cu articolele 132^1, 132^4, 132^5 și 134^4 din Codul de procedură penală.

86. În acest context, Curtea observă că normele privind activitatea specială de investigație au fost introduse prin Legea nr. 66 din 5 aprilie 2012 pentru modificarea și completarea Codului de procedură penală în scopul implementării considerentelor Curții Europene din cauza *Iordachi și alții v. Republica Moldova,* 10 februarie 2009. Completările operate în acest sens de legea de modificare urmăreau să aducă legislația națională în conformitate cu standardul mai ridicat garantat de Convenția Europeană în materia măsurilor de supraveghere secretă. Totuși, articolul 126 alin. (2) a rămas în redactarea pe care o are încă de la adoptarea Codului de procedură penală în 2003.

87. Deși obținerea de către organul de urmărire penală a istoricului informațiilor privind conversațiile telefonice anterioare poate constitui un mijloc util de investigare și descoperire a infracțiunilor, **Curtea consideră că accesul la informațiile în discuție trebuie să fie însoțit, *mutatis mutandis*, de condițiile și garanțiile aplicabile măsurilor speciale de investigație** prevăzute la articolele 132^1, 132^4, 132^5 și 134^4 din Codul de procedură penală. Aceste condiții și garanții trebuie să fie adaptate la caracteristicile precise ale ridicării istoricului informațiilor privind conversațiile telefonice (a se vedea § 63 *supra*). Totodată, perioadă pentru care poate fi solicitată măsura în discuție trebuie raportată la condiția necesității și proporționalității ridicării informațiilor privind convorbirile telefonice și nu poate depăși termenul pentru care furnizorul de rețele și/sau de servicii de telecomunicații este obligat să le păstreze potrivit articolului 20 alin. (3) lit. c) din Legea comunicațiilor electronice.

88. În concluzie, Curtea constată că textul „precum și ridicarea informației privind convorbirile telefonice” din articolul 126 alin. (2) din Codul de procedură penală este constituțional, în măsura în care procedurii de ridicare a informațiilor privind

conversațiile telefonice îi sunt aplicabile, *mutatis mutandis*, condițiile și garanțiile măsurilor speciale de investigație.

89. Totodată, Curtea menționează că pot exista și alte soluții legislative care să asigure respectarea exigenței „prevăzute de lege” din articolul 8 § 2 din Convenție și a articolului 30 din Constituție, decât cele aplicabile măsurilor speciale de investigație pe care le reglementează Codul de procedură penală (a se vedea §§ 58 - 62 *supra*). Așadar, Curtea va emite o adresă Parlamentului, în vederea reglementării accesului organelor de urmărire penală la istoricul informațiilor privind conversațiile telefonice de o manieră conformă cu garanțiile minime stabilite în prezenta hotărâre și în jurisprudența Curții Europene.

Din aceste motive, în baza articolelor 135 alin. (1) literele a) și g), 140 alin. (2) din Constituție, 26 din Legea cu privire la Curtea Constituțională, 6, 61, 62 lit. a) și 68 din Codul jurisdicției constituționale, Curtea Constituțională

HOTĂRĂȘTE:

1. *Se admite* sesizarea privind excepția de neconstituționalitate a textului „precum și ridicarea informației privind convorbirile telefonice” din articolul 126 alin. (2) din Codul de procedură penală, adoptat prin Legea nr. 123 din 14 martie 2003, ridicată din oficiu de dl judecător Ion Ghizdari, în cauza penală nr. 11-51/2023, pendinte la Judecătoria Ungheni.

2. *Se recunoaște constituțional* textul „precum și ridicarea informației privind convorbirile telefonice” din articolul 126 alin. (2) din Codul de procedură penală, în măsura în care acestei proceduri îi sunt aplicabile, *mutatis mutandis*, condițiile și garanțiile măsurilor speciale de investigație.

3. Prezenta hotărâre este definitivă, nu poate fi supusă niciunei căi de atac, intră în vigoare la data adoptării și se publică în Monitorul Oficial al Republicii Moldova.

Președinte **Domnica MANOLE**

Chișinău, 19 decembrie 2023
HCC nr. 22
Dosarul nr. 49g/2023