Cod ECLI ECLI:RO:TBBIH:2024:001.######

#######
TRIBUNALUL BIHOR
SECŢIA PENALĂ

Operator de date cu caracter personal nr. 9009
Dosar nr. ####/111/2021

SENTINŢA PENALĂ nr. ###/P/2024

Şedinţa publică din data de 17 septembrie 2024
Completul constituit din:
Preşedinte: ######## #######
Grefier: ###### ###### ####

Ministerul ###### a fost reprezentat de procuror ##### #######,
din cadrul Parchetului de pe lângă Tribunalul Bihor,

Pe rol se află soluţionarea cauzei penale, privind pe inculpata ##### ####### #####, trimisă în judecată, în stare de libertate, pentru săvârşirea infracţiunilor de:

- acces ilegal la un sistem informatic, prev. de art. 360 alin. 1, 2 şi 3 Cod penal (pct. 1 rechizitoriu);
- acces ilegal la un sistem informatic, prev. de art. 360 alin. 1, 2 şi 3 Cod penal (pct. 2 rechizitoriu);
- acces ilegal la un sistem informatic, prev. de art. 360 alin. 1, 2 şi 3 Cod penal (pct. 3 rechizitoriu);
- acces ilegal la un sistem informatic, prev. de art. 360 alin. 1, 2 şi 3 Cod penal (pct. 4 rechizitoriu);
- acces ilegal la un sistem informatic, prev. de art. 360 alin. 1, 2 şi 3 Cod penal, în concurs cu divulgarea informațiilor secrete de serviciu sau nepublice, prev. de art. 304 alin. 1 Cod penal (pct. 5 rechizitoriu);
- acces ilegal la un sistem informatic, prev. de art. 360 alin. 1, 2 şi 3 Cod penal, în concurs cu divulgarea informațiilor secrete de serviciu sau nepublice, prev. de art. 304 alin. 1 Cod penal (pct. 6 rechizitoriu);
- acces ilegal la un sistem informatic, prev. de art. 360 alin. 1, 2 şi 3 Cod penal (pct. 7 rechizitoriu);
- acces ilegal la un sistem informatic în formă continuată (două acte materiale), prev. de art. 360 alin. 1, 2 şi 3 Cod penal, cu aplic. art. 35 Cod penal (pct. 8 rechizitoriu);

- acces ilegal la un sistem informatic, prev. de art. 360 alin. 1, 2 şi 3 Cod penal, în concurs cu divulgarea informațiilor secrete de serviciu sau nepublice, prev. de art. 304 alin. 1 Cod penal (pct. 9 rechizitoriu);

- acces ilegal la un sistem informatic, prev. de art. 360 alin. 1, 2 şi 3 Cod penal (pct.10 rechizitoriu);

- acces ilegal la un sistem informatic în formă continuată (5 acte materiale), prev. de art. 360 alin. 1, 2 şi 3 Cod penal, cu aplic. art. 35 Cod penal (pct. 11 rechizitoriu).

Dezbaterile au avut loc la termenul din data de 29.03.2024, fiind consemnate în încheierea de şedinţă din acea dată şi care face parte integrantă din prezenta sentinţă, când tribunalul, având nevoie de timp pentru deliberarea, motivarea şi redactarea hotărârii, a stabilit pronunţarea pentru data de 28.05.2024, când a amânat pronunţarea succesiv pentru data de astăzi, 17.09.2024, când a hotărât următoarele:

TRIBUNALUL

Deliberând asupra cauzei penale de faţă, constată următoarele:

Prin Rechizitoriul emis la data de 27.10.2021 în dosarul penal nr. ###/P/2020 al Parchetului de pe lângă Tribunalul Bihor, s-a dispus trimiterea în judecată, în stare de libertate, a inculpatei ##### ####### #####, având CNP ##########, cetăţean român, cu domiciliu în sat #######, nr. 163, #### #####, agent de poliţie în cadrul I.P.J. Bihor - ###. Mun. ###### – Biroul de Ordine #######, pentru săvârşirea infracţiunilor de:

- acces ilegal la un sistem informatic, prev. de art. 360 alin. 1, 2 şi 3 Cod penal (pct. 1 rechizitoriu);

- acces ilegal la un sistem informatic, prev. de art. 360 alin. 1, 2 şi 3 Cod penal (pct. 2 rechizitoriu);

- acces ilegal la un sistem informatic, prev. de art. 360 alin. 1, 2 şi 3 Cod penal (pct. 3 rechizitoriu);

- acces ilegal la un sistem informatic, prev. de art. 360 alin. 1, 2 şi 3 Cod penal (pct. 4 rechizitoriu);

- acces ilegal la un sistem informatic, prev. de art. 360 alin. 1, 2 şi 3 Cod penal, în concurs cu divulgarea informațiilor secrete de serviciu sau nepublice, prev. de art. 304 alin. 1 Cod penal (pct. 5 rechizitoriu);

- acces ilegal la un sistem informatic, prev. de art. 360 alin. 1, 2 şi 3 Cod penal, în concurs cu divulgarea informațiilor secrete de serviciu sau nepublice, prev. de art. 304 alin. 1 Cod penal (pct. 6 rechizitoriu);

- acces ilegal la un sistem informatic, prev. de art. 360 alin. 1, 2 şi 3 Cod penal (pct. 7 rechizitoriu);

- acces ilegal la un sistem informatic în formă continuată (două acte materiale), prev. de art. 360 alin. 1, 2 şi 3 Cod penal, cu aplic. art. 35 Cod penal (pct. 8 rechizitoriu);

- acces ilegal la un sistem informatic, prev. de art. 360 alin. 1, 2 şi 3 Cod penal, în concurs cu divulgarea informațiilor secrete de serviciu sau nepublice, prev. de art. 304 alin. 1 Cod penal (pct. 9 rechizitoriu);

- acces ilegal la un sistem informatic, prev. de art. 360 alin. 1, 2 şi 3 Cod penal (pct.10 rechizitoriu);

- acces ilegal la un sistem informatic în formă continuată (5 acte materiale), prev. de art. 360 alin. 1, 2 şi 3 Cod penal, cu aplic. art. 35 Cod penal (pct. 11 rechizitoriu).

Situaţia de fapt reţinută în actul de sesizare, în esenţă, a constat în:

- Fapta inculpatei ##### (fostă ###) ####### #####, agent şef adjunct de poliţie în cadrul ###.Mun.######-Biroul Ordine #######, care în noaptea de 21 august 2017, ora 00:30-00:39, în exercitarea în exercitarea atribuţiilor de serviciu, aflându-se în incinta Poliţiei Municipiului ###### - Biroul Supravegheri Video", folosind userul şi parola proprie, a accesat şi interogat nelegal, cu depăşirea limitelor autorizării, mai multe baze de date administrate de M.A.I.-D.E.P.A.B.D., şi anume ######## Auto, ######## Persoane ,respectiv ######## Paşapoarte, cu privire la numiţii ###### ###### (evidenţa Persoanei), ####### ###### (evidenţa Persoanei, ######## Auto şi Paşapoarte) şi ######## ###### (evidenţa Populaţiei), scopul verificărilor nefiind unul în interes de serviciu, ci personal, întruneşte elementele constitutive ale infracţiunii de acces ilegal la un sistem informatic, prev. de art.360 alin.1,2 şi 3 cod penal.

- Fapta inculpatei ##### ####### #####, care, la data de 11.03.2018, în intervalul orar 17.12 – 17.37, fără nicio justificare, a accesat şi efectuat interogări în bazele de date ######## Persoanelor, ######## Paşapoarte şi ######## Auto, privind pe numita ####### ####### ######, persoană aflată în cercul relaţional al numitului ###### ######, precum şi cu privire la membrii de familie ai acesteia (####### #### ####### – tatăl, ####### ####### ######-mama şi ####### #### ##### – Fratele), întruneşte elementele constitutive ale infracţiunii de acces ilegal la un sistem informatic, prev. de art.360 alin.1,2 şi 3 cod penal.

- Fapta inculpatei ##### ####### #####, care, la data de 24.04.2018, în intervalul orar 14.53 – 14.55, fără nicio justificare, în timp ce îşi exercita atribuţiile de serviciu în sediul Poliţiei Mun.######, a accesat şi efectuat interogări în bazele de date ######## Persoanelor, ######## Paşapoarte şi ######## Auto, privind pe numitului ### ###### ###### (prietenul numitei ##### ####### la acea vreme, actualul soţ al acesteia), respectiv a familiei acestuia (### #### ###### - tatăl, chestor de poliţie, şi ### ######## #####-mama sa), în interes personal, cu depăşirea limitelor autorizării, întruneşte elementele constitutive ale infracţiunii de acces ilegal la un sistem informatic, prev. de art.360 alin.1,2 şi 3 cod penal.

- Fapta inculpatei ##### ####### #####, care, în noaptea de 23.10.2018, în intervalul orar 00:08 – 00:09, fără nicio justificare, în timp ce îşi exercita atribuţiile de serviciu în sediul Poliţiei Mun.######, a accesat şi efectuat interogări în bazele de date ######## Auto, privind autoturismul PORSCHE #######, de culoare roşie, cu numarul de înmatriculare #########, înmatriculat pe SC ###### SRL, autoturism folosit la acea vreme de numita ##### ####### ########, în interes personal, cu depăşirea limitelor autorizării, întruneşte elementele constitutive ale infracţiunii de acces ilegal la un sistem informatic, prev. de art.360 alin.1,2 şi 3 cod penal.

- Faptele inculpatei ##### ####### #####, care, în seara zilei de 15.11.2018, în intervalul orar 21:51 – 22:28, la instigarea suspectei ###### ####### #######, fără nicio justificare, în timp ce îşi exercita atribuţiile de serviciu în sediul Poliţiei Mun.######, a accesat şi efectuat interogări în baza de date „######## Persoanelor" în interesul personal al suspectei, cu privire la entităţile „##### ####", „##### ##### #######", „##### ########" şi „##### ###", cu

depăşirea limitelor autorizării, după care a divulgat datele de identificare acelor persoane (numele, legături de rudenie, anul naşterii, domiciliul) suspectei ###### ####### #######, întrunesc elementele constitutive ale infracţiunii de acces ilegal la un sistem informatic, prev. de art.360 alin.1,2 şi 3 cod penal, în concurs real cu infracţiunea de divulgare informațiilor secrete de serviciu sau nepublice, faptă prev. și ped. de art. 304 alin. 1 C.p.

- Faptele inculpatei ##### ####### #####, care, în seara zilei de 15.11.2018, în intervalul orar 23:54 – 23:59, fără nicio justificare legală, în timp ce îşi exercita atribuţiile de serviciu în sediul Poliţiei Mun.######, a accesat şi efectuat interogări în bazele de date „######## Persoanelor", ######## Paşapoarte şi ######## Auto" în interesul său personal şi al concubinului său ######## ######, cu privire la persoana vătămată #### ####### #######, cu depăşirea limitelor autorizării, după care a divulgat datele de identificare a persoanei vătămate (numele, starea civilă, anul naşterii, autoturismele deţinute, ocupaţia) numitului ######## ######,coleg de serviciu cu persoana vătămată, întrunesc elementele constitutive ale infracţiunii de acces ilegal la un sistem informatic, prev. de art.360 alin.1,2 şi 3 cod penal, în concurs real cu infracţiunea de divulgare informațiilor secrete de serviciu sau nepublice, faptă prev. și ped. de art. 304 alin. 1 C.p.

- Fapta inculpatei ##### ####### #####, care, în la data de 18.11.2018, în intervalul orar 10;38 – 10:45, fără nicio justificare legală, în timp ce îşi exercita atribuţiile de serviciu în sediul Poliţiei Mun.######, a accesat şi efectuat interogări în bazele de date „######## Persoanelor", „######## Auto" şi „######## Paşapoarte", în interesul personal al suspectei, cu privire la entitatea „##### ##### #########", cu depăşirea limitelor autorizării, întruneşte elementele constitutive ale infracţiunii de acces ilegal la un sistem informatic, prev. de art.360 alin.1,2 şi 3 cod penal.

- Fapta inculpatei ##### ####### #####, care, la datele de 20.11.2018 (intervalul orar 03:33-03:48) şi 24.11.2018 (intervalul orar 01:23-01:25), în baza aceleiaşi rezoluţiuni infracţionale, sub justificarea nereală a efectuării unor verificări operative, a accesat şi efectuat interogări în bazele de date ######## Persoanelor şi ######## Paşapoarte, privind pe numita ###### #####, întrucât observase că susnumita figurează ca şi „prietenă" pe aplicaţia Facebook cu concubinul ei ######## ######, întruneşte elementele constitutive ale infracţiunii de acces ilegal la un sistem informatic în formă continuată, prev. de art.360 alin.1,2 şi 3 cod penal, cu aplic. art.35 c.pen. (două acte materiale).

- Faptele inculpatei ##### ####### #####, care, în seara zilei de 19.10.2018, date în intervalul orar 20.10-20:18, fiind determinată de suspectul ######## ######, fără nicio justificare legală, în timp ce îşi exercita atribuţiile de serviciu în sediul Poliţiei Mun.######, a accesat şi efectuat interogări în bazele de date „######## Persoanelor", ######## Paşapoarte şi ######## Auto" în interesul său personal şi al concubinului său ######## ######, cu privire la numita ####### ####### ######, cu depăşirea limitelor autorizării, după care a divulgat datele de identificare a persoanei vătămate (numele, starea civilă, anul naşterii, autoturismele deţinute, ocupaţia, adresa) suspectului ######## ######, persoană interesată de aflarea acestor date, întrunesc elementele constitutive ale infracţiunii de acces ilegal la un sistem informatic, prev. de art.360 alin.1,2 şi 3 cod penal, în concurs real cu infracţiunea de divulgarea informațiilor secrete de serviciu sau nepublice, faptă prev. și ped. de art. 304 alin. 1 C.p..

- Fapta inculpatei ##### ####### #####, care, la data de 22.11.2018, ora 17:45, sub justificarea nereală a efectuării unor verificări operative, a accesat şi efectuat interogări în bazele de date ######## Auto, privind pe numitul ### ######## ##### #### , întrucât dorea să apeleze la serviciile acestuia pentru a-i transporta lemne, întruneşte elementele constitutive ale infracţiunii de acces ilegal la un sistem informatic, prev. de art.360 alin.1,2 şi 3 cod penal.

- Faptele inculpatei ##### ####### #####, care, în perioada 26.10.2018 – 24.11.2018, şi anume la datele de 26.10 (ora 19:21), 27.10 (ora 06:10), 30.10 (ora 23:46), 31.10 (ora 02:38) şi 24.11 (ora 01:26), în timp ce ce afla la serviciu-sediul ###.Mun.######, în baza aceleiaşi rezoluţiuni infracţionale, sub justificarea nereală a efectuării unor verificări operative, a accesat şi efectuat interogări în bazele de date ######## Persoanelor şi ######## auto, privind pe numita ######## #####, întrucât avea suspiciuni ca aceasta ar fi avut o relaţie cu concubinul ei ######## ######, întruneşte elementele constitutive ale infracţiunii de acces ilegal la un sistem informatic în formă continuată, prev. de art.360 alin.1,2 şi 3 cod penal, cu aplic. art.35 c.pen. (5 acte materiale).

Situaţia de fapt astfel prezentată în rechizitoriu a fost reţinută de organul de urmarire penala pe baza următoarelor mijloace de probă:

- Procese verbale de consemnare a rezultatului verificărilor cu privire la accesările inculpatei în bazele de date DEPABD;

- Procese verbale de redare a unor convorbiri telefonice interceptate în baza mandatului de supraveghere tehnică;

- Declaţie persoană vătămată #### #######;

- Declaraţii martori;

- Declaraţii suspecţi;

- #### înscrisuri.

Procedura de cameră preliminară a fost finalizată prin Încheierea penală nr. ##/Î/CP/2022 pronunţată la data de 18.05.2022 de judecătorul de cameră preliminară din cadrul Tribunalului Bihor în dosarul nr. ####/111/2021/a1, prin care s-a respins, ca inadmisibilă, cererea de reunire a dosarului nr. ####/111/2021/a1 la dosarul nr. ####/111/2020/a1, s-a respins, ca inadmisibilă, sesizarea Curtii Constitutionale vizând neconstitutionalitatea disp. art. 45 alin. 2 Cod procedura penală, s-au respins, ca nefondate, cererile si exceptiile formulate de inculpata ##### (###) ####### #####, s-a constatat că Tribunalul Bihor este competent în soluţionarea prezentei cauze, s-a constatat legalitatea sesizării instanţei cu rechizitoriul nr. ###/P/2020 emis de Parchetul de pe langa Tribunalul Bihor, a administrării probelor şi a efectuării actelor de urmărire penală şi s-a dispus începerea judecăţii cu privire la inculpata ##### (###) ####### #####.

Împotriva Încheierii penale nr. ##/Î/CP/2022 pronunţată la data de 18.05.2022 de judecătorul de cameră preliminară din cadrul Tribunalului Bihor în dosarul nr. ####/111/2021/a1 a declarat contestaţie inculpata, iar prin Încheierea penală nr. ###/CCP/2022 din 15.12.2022 pronunţată de completul de cameră preliminară din cadrul Curţii de Apel ###### s-a dispus admiterea contestaţiei declarate de inculpata ##### ####### ##### împotriva Încheierii penale nr. ##/ÎCP/18.05.2022 pronunţată de judecătorul de cameră preliminară din cadrul Tribunalului Bihor, pe care a desfiinţat-o în parte, în sensul că:

S-a înlăturat dispoziţia prin care, în baza art. 346 alineat 2 Cod de procedură penală, s-au respins cererile şi excepţiile invocate de inculpata ##### ####### #####.

S-a reţinut că prin Încheierea din 17.10.2022 pronunţată de completul de cameră preliminară din cadrul Curţii de Apel ######, s-au admis în parte a cererile şi excepţiile invocate, constatându-se că prin Încheierea penală din 26.11.2021, pronunțată de judecătorul de cameră preliminară din cadrul Tribunalului Bihor în dosarul nr. ####/111/2020/al, definitivă prin Încheierea penală nr. ##/CCP/2022 din 24 iunie 2022 pronunţată de completul de cameră preliminară din cadrul Curţii de Apel ######, s-a reţinut cu putere de lucru judecat nulitatea Încheierii nr. ##/01.11.2018 şi a mandatelor de supraveghere tehnică nr. 134/UP/01.11.2018 și nr. 135/UP/01.11.2018.

În baza art.102 Cod de procedură penală, au fost excluse din dosarul de urmărire penală nr. ###/P/2020 al Parchetului de pe lângă Tribunalul Bihor, procesele-verbale de redare a convorbirilor telefonice/a mesajelor tip sms interceptate în baza Încheierii nr. ##/01.11.2018 pronunţate de judecătorul de drepturi şi libertăţi din cadrul Tribunalului Bihor în dosar nr. ####/111/2018 şi a mandatelor de supraveghere tehnică nr. 134/UP/01.11.2018 și nr. 135/UP/01.11.2018, inclusiv suporţii pe care aceste convorbiri/comunicări au fost stocate.

În aplicarea deciziei Curţii Constituţionale nr. 22 din 18 ianuarie 2018 (publicate în Monitorul Oficial al României nr.177 din 26.02.2018) s-a dispus excluderea materială din dosarul de urmărire penală nr. ###/P/2020 al Parchetului de pe lângă Tribunalul Bihor, a mijloacelor de probă administrate nelegal, inclusiv a suporţilor pe care conținutul tuturor acestor convorbiri/comunicări au fost stocate.

Au fost respinse în rest celelalte cereri şi excepţii invocate de inculpata ##### (###) ####### #####, cu privire la neregularitatea actului de sesizare, a administrării probelor în faza de urmărire penală şi a efectuării actelor de urmărire penală.

S-a constatat că prin Ordonanţa din data de 24.10.2022, procurorul a arătat că-şi menţine dispoziţia de trimitere în judecată.

S-au menţinut în rest dispoziţiile încheierii penale contestate, inclusiv cu privire la începerea judecăţii faţă de inculpată.

La data de 11.04.2023, ca urmare a adresei instanţei, a fost înaintat de către Parchetul de pe lângă Tribunalul Bihor rechizitoriul remediat, conform dispoziţiilor completului de cameră preliminară din cadrul Curţii de Apel ###### (f. 152 – 177, vol. I).

La termenul de judecată din data de 21.04.2023, dupa citirea actului de sesizare, inculpata ##### (###) ####### ##### a arătat că doreşte să fie judecată conform procedurii de drept comun, sens în care la data de 07.06.2023 a depus la dosar cerere în probaţiune prin care a solicitat reaudierea unor martori audiaţi în faza de urmărire penală, precum şi audierea unor martori noi (f. 9 – 12, vol. II).

Prin Încheierea de şedinţă din data de 09.06.2023, instanţa a încuviinţat audierea martorilor ##### ##### şi ####### ####### #######, precum şi audierea martorilor audiaţi în cursul urmăririi penale #### #######, ####### ###### ######, ######## ######, ###### (#######) ######, ####### ####### ######, ### #### ######, ### ##### ####### ########, ##### ######, ####### #######, ######## ### ##### ####, ######## #####.

La termenul de judecată din data de 17.11.2023 a fost audiată martora #### ####### ###### (declaraţie f. 29).

La data de 17.11.2023 inculpata, prin apărător ales, a depus la dosar o cerere de schimbare a încadrării juridice (f. 36 – 43), iar la data de 04.12.2024 a depus un memoriu cu privire la cererea de schimbare a încadrării juridice (f. 52 – 56).

Prin Încheierea de şedinţă din data de 12.12.2023 s-a respins ca nefondată cererea de schimbare a încadrării juridice formulată de inculpata ##### ####### ##### din infracţiunea de acces ilegal la un sistem informatic, prev. de art. 360 alin. (1), (2) şi (3) Cod penal, raportat la infracţiunile descrise la pct. 1-11 din rechizitoriu, în infracţiunea de acces ilegal la un sistem informatic, prev. de art. 360 alin. (1) şi alin. (2) Cod penal şi s-au prorogat cererile de schimbare a încadrării juridice formulate de aceeaşi inculpată raportate la reţinerea formei continuate pentru infracţiunile de acces ilegal la un sistem informatic, prev. de art. 360 alin. (1), (2) Cod penal şi divulgarea informaţiilor secrete de serviciu sau nepublice, prev. de art. 304 alin. 1 Cod penal.

La termenul de judecată din data de 02.02.2024, inculpata, asistată de apărător ales, a renunţat la administrarea probatoriului încuviinţat şi a solicitat dezbaterea fondului cauzei, fiind dezbătut fondul la termenul de judecată din 29.03.2024, concluziile părţilor fiind consemnate în încheierea de şedinţă de la acel termen de judecată, care face parte integrantă din prezenta hotărâre.

Inculpata a depus la dosar soluţii de practică judiciară (f. 69 – 82, vol. II).

Totodată, la data de 11.04.2024 a depus la dosar concluzii scrise (f. 83 – 94) prin care a solicitat următoarele:

A. în principal, în temeiul art. 396 alin. (5) CPP, rap. la art. 16 alin. (1) lit. b) teza I CPP, achitarea inculpatei ##### ####### ##### pentru infracțiunile prevăzute de art. 360 și 304 CP.

B. în subsidiar, cu privire la infracțiunea prevăzută la art. 304 CP, în temeiul art. 396 alin. (6) CPP rap. la art. 16 alin. (1) lit. f) CPP, încetarea procesului penal ca urmare a intervenirii prescripției răspunderii penale.

În susținerea temeiurilor de achitare a arătat următoarele:

1. ASPECTE PRELIMINARE

avea dreptul de a se autentifica la bazele de date, în baza unui cont de utilizator asociat acesteia. Ceea ce i se impută este că aceasta a interogat bazele de date la care avea acces, în alt scop decât cel al exercitării atribuțiilor de serviciu. Prin urmare, teza depășirii limitelor autorizării se raportează la procesul de interogare a bazelor de date.

Conduita constând în autentificarea la bazele de date (accesul propriu-zis) nici măcar nu face obiectul acuzației în materie penală. Sub acest aspect, necesită delimitat accesul la un sistem informatic realizat prin procesul de autentificare (accesul propriu-zis) și interogarea bazelor de date (exploatarea accesului consumat anterior).

Astfel, cu toate că acuzarea face o trimitere generică la accesarea bazelor de date, în realitate aceasta se raportează la interogarea bazelor de date. Așa cum urmează a arăta infra, în mod regretabil, acuzarea se raportează la cele două sintagme ca și cum ar fi interschimbabile, făcând o confuzie între accesarea unui sistem informatic prin autentificarea ca și utilizator (autentificarea la bazele de date) și exploatarea accesului obținut anterior (interogarea bazelor de date prin căutarea unor informații, folosind anumite cuvinte cheie).

Că este așa rezultă cu evidență din probele esențiale folosite în acuzare – datele rezultate din logurile/rapoartele referitoare la interogarea bazelor de date – a se vedea în acest sens procesele-verbale de consemnare a verificărilor întocmite în 19.02.2019 și 19.10.2020 de către

lucrătorii DGA, menționate cu ocazia descrierii situației de fapt relevante pentru faptele reținute în acuzare. Din acestea,

Astfel, având în vedere că în aceste loguri se identifică la nivel de secundă momentul la care a avut loc interogarea bazelor de date, rezultă fără echivoc faptul că acuzația în materie penală este circumscrisă doar la această interacțiune la nivel logic. O asemenea constatare se transpune automat în excluderea conduitei anterioare (procesul de autentificare ta bazele de date) din sfera acuzației în materie penală.

În susținerea acestei teze, mai pot fi aduse cel puțin două argumente:

La fila 3 din rechizitoriu, chiar în paragraful anterior expunerii stării de fapt se statuează în sensul că doamna ##### „(...) a folosit discreționar, în mod repetat, bazele de date (...) la care avea acces în baza unui user și parole proprii, cu depășirea limitelor autorizării, și anume în interesul său personal sau a unor persoane aflate în cercul său relațional". Așadar, ceea ce se impută este folosirea bazelor de date, în sensul interogării acestora.

În secțiunea „încadrare juridică – Cadru legal și infralegal, analizarea elementelor constitutive ale infracțiunilor cercetate" se concluzionează faptul că „(„.) a rezultat fără dubiu că verificările respective în bazele de date efectuate de inculpata (...) Practic, inculpata a utilizat bazele de date cu conținut confidențial ca pe propriul său bun (...)".

Toate trimiterile generice făcute ulterior la „accesarea bazelor de date" se datorează confuziei despre care am făcut vorbire supra. Dintr-o analiză atentă rezultă totuși faptul că accesarea bazelor de date nu se raportează la procesul de autentificare, ci exclusiv ia interogarea bazelor de date. Astfel, cu privire la prima faptă imputată (fila 3 din rechizitoriu) se reține faptul că doamna ##### a „accesat" sistemul informatic în data de 21.07.2017, în intervalul orar 00:30-00:39. Or, din logurile existente la dosarul cauzei rezultă fără echivoc faptul că interogările ce fac obiectul acuzației în materie penală au fost efectuate începând cu 00:30:52. înainte de aceste interogări, doamna ##### a efectuat totuși o serie de alte interogări ale bazelor de date ce nu au făcut niciodată obiectul unei acuzații în materie penală. Rezultă așadar că între momentul accesării sistemului informatic (prin autentificare) și interogările ce fac obiectul prezentei cauze au existat interogări ce nu au fost asociate unei conduite ilicite.

Stabilirea corectă a limitelor judecății prezintă o importanță deosebită deoarece, așa cum urmează a arăta infra, interogarea bazelor de date nu poate fi subsumată noțiunii de „acces", lipsind așadar un element constitutiv al infracțiunii prevăzute la art. 360 CP.

De altfel, argumentele referitoare la lipsa tipicității subzistă chiar dacă ignorăm aspectele referitoare la stabilirea corectă a limitelor judecății. Astfel, toată jurisprudența la care a făcut trimitere apărarea este în sensul nereținerii acestei infracțiuni pentru stări de fapt similare sau identice cu cele din prezenta cauză.

B. ####### ART. 360 COD PENAL

Art. 360 CP reprezintă o transpunere a art. 2 din Convenția privind criminalitatea informatică [în continuare Convenția] și a art. 3 din Directiva 2013/40/UE [în continuare Directiva].

se poate susține că prin incriminarea faptei prevăzute la art. 360 CP se urmărește inclusiv protejarea confidențialității datelor informatice, punerea în pericol a valorii sociale se realizează doar la momentul consumării accesului la un sistem informatic. Prin urmare, o

eventuală conduită ulterioară în legătură cu datele informatice stocate pe un sistem informatic excedează sferei de aplicabilitate a textului de incriminare.

Legiuitorul national a incriminat următoarele conduite:

Accesarea unui sistem informatic (art. 360 CP) ca infracțiune mijloc (regula) sau scop (excepția), fără să prezinte relevanță conduita ulterioară a făptuitorului;

Interceptarea ilegală (art. 361 CP) și transferul neautorizat de date informatice (art. 364 CP), ce acoperă modalitățile de obținere fără drept a datelor informatice. Interogarea bazelor de date nu echivalează însă cu o interceptare de date (doamna ##### nu a „captat7' informația în timp ce aceasta a fost transmisă de la expeditor la destinatar) sau un transfer al acestora (prin interogare, datele informatice nu sunt copiate sau relocate într-o terță locație, fiind pur și simplu afișate pe monitor).

Astfel, dacă ceea ce se reproșează doamnei ##### este faptul că a vizualizat (prin interogarea bazelor de date) informații ce nu au legătură cu exercitarea atribuțiilor de serviciu ale acesteia, această acuzație în materie penală excedează de plano sferei de aplicabilitate a art. 360 CP.

Ulterior finalizării procesului de autentificare, doamna ##### a dobândit acces și control asupra tuturor datelor informatice stocate în bazele de date. Prin urmare, nu se poate susține că s-a adus atingere confidențialității datelor informatice printr-o conduită ulterioară, constând în interogarea bazelor de date în vederea afișării informației pe monitor. #### o terță persoană s-ar fi autentificat fără drept la bazele de date, lezarea valorii sociale constând în confidențialitatea datelor informatice stocate pe sistemul informatic accesat s-ar fi prezumat la momentul consumării accesului (finalizarea procesului de autentificare), nemaifiind necesară o altă conduită.

2. Semnificația „accesului”

Potrivit ICCJ (HP nr. 68/2021), accesul constă într-o „interacțiune la nivel logic cu respectivul sistem, direct și nemijlocit ori de ia distanță, care să permită făptuitorului să beneficieze de resursele ori/și de funcțiile lui”.

În prezenta cauză discutăm despre un acces direct și nemijlocit la sistemul informatic (PC) aflat în incinta IPJ Bihor și un acces de la distanță la sistemele informatice unde sunt stocate bazele de date ce fac obiectul prezentei analize.

În acest caz, accesul echivalează cu autentificarea la aceste baze de date - proces ce se transpune într-o interacțiune logică și de la distanță cu sistemul informatic unde acestea sunt stocate. Cu alte cuvinte, accesul implică introducerea datelor de autentificare (user și parolă), acestea fiind prelucrate de către sistemul informatic ce returnează un răspuns cu privire la corectitudinea datelor introduse.

În momentul în care se finalizează procesul de autentificare la bazele de date utilizatorul beneficiază de resursele și funcțiile sistemului informatic, prin aceea că are posibilitatea de a interoga bazele de date (prin intermediul funcției de căutare) și de a vizualiza pe monitor conținutul unor date cu caracter personal.

3. Momentul consumării infracțiunii

Potrivit ICCJ (HP nr. 68/2021), „accesul fără drept la un sistem informatic, prevăzută de art. 360 alin. (1) din Codul penal, se consumă în momentul realizării elementului material al

laturii obiective, respectiv al accesului, când autorul, interacționând la nivel logic cu sistemul informatic, beneficiază de resursele ori/și de funcțiile lui".

În prezenta cauză, ulterior finalizării procesului de autentificare se putea beneficia de resursele ori/și funcțiile sistemelor informatice respective (a se vedea și supra), accesul fiind așadar unul consumat. Ulterior consumării acestui acces, conduita ulterioară de interogare a bazelor de date nu se transpune într-un nou acces, ci în exploatarea (valorificarea) accesului obținut anterior. Cu alte cuvinte, interogarea unei baze de date este subsecventă accesului și nu se identifică cu acesta.

Toate datele informatice stocate în bazele de date sunt deja accesibile la momentul finalizării procesului de autentificare. Procesul de interogare a bazelor de date are ca finalitate doar afișarea informației pe monitorul utilizatorului. Făcând o paralelă, autentificarea la baza de date echivalează cu deschiderea unui dulap folosind o cheie. În schimb, interogarea bazelor de date echivalează cu răsfoirea unor dosare aflate în dulapul deschis anterior.

Momentul consumării infracțiunii prezintă relevanță deosebită, deoarece, dacă se constată că accesul s-a realizat cu drept dar exploatarea ulterioară a accesului a fost una neconformă (fără legătură cu atribuțiile de serviciu), această din urmă conduită nu poate produce efecte cu titlu retroactiv.

4. Relevanța scopului special

Scopul special prezintă relevanță doar pentru reținerea variantei agravate prevăzute la art. 360 alin. (2) CP. Prin urmare, aplicabilitatea infracțiunii în formă de bază [art. 360 alin. (1) CP] nu poate fi analizată prin raportare la un element ce reprezintă un element constitutiv a unei variante agravate a aceleiași infracțiuni [art. 360 alin. (2) CP]. #### s-ar proceda de o asemenea manieră, circumstanța de calificare referitoare la scopul special ar deveni inclusiv element constitutiv al formei de bază. Or, de esența variantelor agravate este aceea că acestea au incluse în tipicitate circumstanțe suplimentare în raport cu forma de bază.

În concluzie, scopul special prezintă relevanță doar pentru reținerea variantei agravate prevăzute la art. 360 alin. (2) CP. Pentru reținerea variantei agravate este însă necesar să fie îndeplinite elementele constitutive ale formei de bază.

11. CU PRIVIRE LA SOLUȚIA DE ACHITARE

11.1. Achitarea pentru faptele constând în accesarea unui sistem informatic

În ceea ce privește soluționarea laturii penale, apreciem că trebuie reținut temeiul de achitare prevăzut la art. 16 alin. (1) lit. b) teza I CPP (fapta nu este prevăzută de legea penală).

În context, pentru a se putea reține art. 360 CP este necesară identificarea următoarelor elemente: [1] existența unui acces proptiu-zis, [2] realizat fără drept, [3] la un sistem informatic. Teza acuzării este aceea că accesul la un sistem informatic s-a realizat prin depășirea limitelor autorizării, cu scopul de a obține date informatice fără o legătură cu atribuțiile de serviciu.

Teza depășirii limitelor autorizării nu este incidență în prezenta cauză.

1.Interogarea bazelor de date nu echivalează cu un acces

Sub acest aspect a apreciat că trebuie făcută o distincție clară între autentificarea la bazele de date (accesul propriu-zis) și interogarea bazelor de date (exploatarea accesului obținut ca urmare a finalizării procesului de autentificare la bazele de date).

în vedere că art. 360 CP sancționează doar accesul fără drept, nu și o eventuală utilizare frauduloasă a accesului obținut cu drept, conduita imputată excedează de plano sferei de aplicabilitate a textului de incriminare.

Relevante în context sunt următoarele aspecte:

În momentul autentificării la bazele de date, utilizatorul dobândește acces la toate datele informatice stocate în acestea;

Interogarea bazelor de date se transpune într-o simplă comunicare cu acestea;

Interogarea bazelor de date nu se transpune într-un nou acces la un sistem informatic, aceasta având doar semnificația unei exploatări a accesului obținut anterior.

A susține că exploatarea accesului echivalează cu accesarea sistemului informatic se transpune într-o veritabilă analogie în defavoarea inculpatului.

În ceea ce privește art. 360 CP, legiuitorul a incriminat doar accesarea sistemului informatic. Orice conduită ulterioară consumării accesului, constând în exploatarea accesului obținut anterior, prezintă relevanță penală doar prin raportare la alte texte de incriminare - art. 361-364, art. 325, art. 249, art. 304 CP etc.

Făcând o analogie, conduita făptuitorului de a se autentifica la un cont de e-mail se pliază pe elementele constitutive ale art. 360 CP. în schimb, citirea corespondenței electronice recepționate de titularul contului respectiv nu constituie un acces distinct, ci o exploatare a accesului obținut anterior. Tocmai de aceea, dacă titularului contului de e-mail citește o corespondență electronică primită din eroare nu va răspunde pentru infracțiunea de acces ilegal la un sistem informatic prin raportare la teza depășirii limitelor autorizării, cu toate că acea corespondență nu i-a fost destinată. Aceasta întrucât, existența dreptului/autorizării de a accesa sistemul informatic se analizează la momentul autentificării în contul de e-mail, nu la momentul citirii/deschiderii corespondenței electronice.

2. Accesul la bazele de date (prin autentificare) s-a realizat cu drept

Teza depășirii limitelor autorizării avută în vedere de către legiuitor la art. 35 alin. (2) lit. b) din Legea nr. 161/2003 trebuie raportată la dispozițiile art. 35 alin. (2) lit. a) din lege, ce fac vorbire despre lipsa unei autorizări legale ori contractuale. Rezultă așadar următoarele:

Teza depășirii limitelor autorizării nu are autonomie, fiind esențială identificarea unor dispoziții legale ori contractuale care au fost încălcate de către inculpat, exclusiv la momentul consumării accesului;

Depășirea limitelor autorizării prin raportare la existența unui alt scop decât cel pentru care s-a conferit autorizarea nu este prevăzută de legea penală;

Noțiunea „fără drept” se referă așadar la existența unei autorizări legale sau contractuale în ceea ce privește accesarea sistemului informatic, nu la exploatarea accesului în alte scopuri;

Toate trimiterile făcute în cuprinsul rechizitoriului se referă la confidențialitatea, procesarea și dezvăluirea sau accesarea datelor cu caracter personal. Or, toate aceste aspecte vizează conduite ulterioare autentificării la bazele de date, fiind necesară o interogare a bazelor de date ce nu poate fi subsumată unui acces;

De altfel, chiar în Dispozițiile inspectorului general al Poliției ###### nr. 101/2007 și nr. 81/2018 se face vorbire despre „interogarea bazei de date. De asemenea, se face chiar o distincție între interogarea bazelor de date (art. 4) și accesarea acestora prin utilizarea contului de identificare și a parolei (art. 6). Or, în ceea ce privește accesarea bazelor de date se precizează

doar faptul că autentificarea nu se poate realiza prin folosirea parolei de acces aparținând altor polițiști - aceasta fiind ipoteza în care s-ar putea discuta despre un acces ilegal la un sistem informatic.

Scopul ilicit reprezintă doar o circumstanță de calificare prin raportare la prevederile art. 360 alin. (2) CP, fără a fi un element constitutiv al formei de bază. Prin urmare, înainte de analiza scopului special - constând în obținerea de date informatice - este necesară identificarea unui acces propriu-zis care să se realizeze fără drept.

Faptul că lipsa autorizării trebuie raportată în mod exclusiv la acces, fiind exclusă orice conduita ulterioară consumării accesului, rezultă fără echivoc inclusiv din considerentele ICCJ (HPnr. 68/2021):

Raportând această analiză în drept la starea de fapt din prezenta cauză observăm faptul că autorizarea a existat la momentul consumării accesului - autentificarea la bazele de date. Așadar, interogarea bazelor de date accesate anterior poate constitui infracțiune doar prin raportare la un text de incriminare autonom.

eronat a susține că depășirea limitelor autorizării se raportează la prelucrarea necorespunzătoare a datelor stocate în baza de date. Aceasta întrucât, prelucrarea datelor prin interogarea bazei de date nu se poate confunda cu accesul la un sistem informatic.

În mod evident, o asemenea interpretare ar aduce atingere securității juridice, sfera de aplicabilitate a textului de incriminare putând fi extinsă în mod arbitrar prin simpla invocare a unui scop contrar celui pentru care angajatorul a conferit acces la sistemul informatic.

De altfel, dacă un eventual scop ilicit ar putea valida teza depășirii limitelor autorizării, orice folosire a unui sistem informatic în scopul săvârșirii sau pentru înlesnirea săvârșirii unei infracțiuni s-ar transpune automat în reținerea art. 360 CP.

3. Ulterior autentificării la bazele de date s-au efectuat interogări ce nu au făcut obiectul acuzației în materie penală

Independent de cele menționate supra, din logurile depuse la dosarul cauzei rezultă faptul că doamna ##### a efectuat inclusiv interogări ce nu au făcut în niciun moment obiectul acuzației în materie penală.

Din aceste loguri în format electronic, acuzarea a extras doar datele apreciate ca fiind relevante cauzei, omițând celelalte interogări – atât anterioare, cât și ulterioare - ale bazelor de date din care rezultă în mod vădit netemeinicia acuzației în materie penală. Cu titlu de exemplu, ne vom referi la logurile din data de 21.08.2017, relevante pentru fapta descrisă la pct. 1 din rechizitoriu:

Astfel, în acuzare se reține în mod exclusiv interogarea bazelor de date „evidența persoanelor”, „evidența pașapoarte” și „evidența auto”, în ceea ce îi privește pe numiții ######## ######, ###### ###### și ####### ###### ########. Toate aceste baze de date puteau fi interogate în baza aceleiași sesiuni de autentificare.

Procesul de autentificare s-a consumat însă anterior acestor interogări, aspect ce rezultă fără echivoc din faptul că înainte de interogarea bazei de date evidența persoanelor, cu privire la numitul ######## ######, a fost interogată baza de date evidența auto cu privire la numărul de înmatriculare #######. De altfel, din loguri rezultă faptul că sesiunea de autentificare a început la ora 00:06:02, doamna ##### efectuând nu mai puțin de 9 interogări înainte de interogările ce fac obiect prezentei cauze.

De asemenea, chiar ulterior interogărilor ce fac obiectul prezentei cauze, doamna ##### a efectuat multiple alte interogări ce nu au fost apreciate în niciun moment ca fiind ilicite.

4. Accesul la sistemul informatic nu s-a realizat prin depășirea unor măsuri de securitate în primul rând, în măsura în care fapta nu este tipică în forma ei de bază, analiza cu privire la tipicitatea unei variante agravate este lipsită de obiect. Totuși, analiza art. 360 alin. (3) CP prezintă relevanță în prezenta cauză deoarece trimiterea în judecată inclusiv cu privire la această variantă agravată evidențiază din nou confuzia pe care a făcut-o acuzarea între accesarea unui sistem informatic și exploatarea unui acces consumat anterior.

Atât potrivit DCCR nr. 27/2021 și nr. 183/2018, cât și potrivit HP nr. 68/2021, forma agravată prevăzută la art. 360 alin. (3) CP se poate reține doar atunci când făptuitorul utilizează „mijloace calificate” de acces, apte să depășească ori să eludeze protecția sporită instituită prin măsurile de securitate.

Cu alte cuvinte, nu este suficient ca sistemul informatic să fie unul securizat, fiind necesar ca făptuitorul să depășească, eludeze sau înlăture o măsură de securitate.

Forma agravată a infracțiunii prevăzută de art.360 alin. (3) din Codul penal există atunci când făptuitorul utilizează „mijloace calificate" de acces, apte să depășească ori să eludeze protecția sporită instituită prin măsurile de securitate. S-a reținut că textul de lege criticat nu prevede nicio condiție cu privire la modul concret în care restricția este nesocotită, motiv pentru care își menține actualitatea jurisprudența care, anterior Codului penal, a reținut incidența art.42 alin.(3) din Legea nr.161/2003

Curtea a reținut că forma agravată subzistă și atunci când nesocotirea restricției este facilitată de disfuncțiile sau carențele sistemului de protecție, care permit înlăturarea sau ocolirea/eludarea facilă a protecției.

Nu sunt incidente nici dispozițiile art. 360 alin.3 Cod penal care reglementează o formă agravată a infracțiunii de acces ilegal la un sistem informatic în ipoteza în care făptuitorul utilizează mijloace calificate de acces, apte să depășească sau să eludeze protecția sporită instituită prin procedurile, dispozitivele sau programele de securitate. (...) Forma agravată a infracțiunii se reține și atunci când nesocotirea restricției este facilitată de disfuncțiile sau de carențele sistemului de protecție, care permit eludarea facilă a protecției.

Astfel agravanta prevăzută la alin. (3) sancționează o formă calificată de acces echivalentă efracției - făptuitorul încalcă sau eludează măsurile de securitate în vederea consumării accesului. Or, în mod evident, în prezenta cauză, accesul a fost consumat anterior efectuării tuturor interogărilor bazelor de date.

De altfel, în alte situații în care s-a dispus trimiterea în judecată a unui polițist pentru interogarea bazelor de date în interes personal, încadrarea juridică a fost făcută exclusiv prin raportare la prevederile art. 360 alin. (1) și (2) CP - a se vedea în acest sens C.A. București, secția I penală, decizia nr. ###/A/2023 (depusă la dosarul cauzei).

De asemenea, inclusiv atunci când trimiterea în judecată a avut în vedere alin. (3), s-a dispus schimbarea de încadrare juridică prin înlăturarea acestei forme agravate

In prezenta cauză, nu discutăm despre o depășire sau eludare a măsurilor de securitate, deoarece procesul de autentificare s-a consumat anterior interogării bazelor de date. De altfel, autentificarea la bazele de date nu s-a realizat fără drept deoarece inculpata ##### a folosit

propriul cont de utilizator și chiar a efectuat interogări ale bazelor de date ce nu au făcut obiectul acuzației în materie penală.

Diferențele la nivel de formă între art. 42 alin. (3) din Legea nr. 161/2003 și art. 360 alin. (3) CP nu ar trebui să se transpună într-o extindere a sferei de aplicabilitate a art. 360 alin. (3) CP. Sub acest aspect, nu credem că discutăm despre o modificare de substanță a acestei circumstanțe de calificare, îndeosebi raportat la DCCR nr. 27/2021, DCCR nr. 183/2018 și potrivit HP nr. 68/2021. Ambele decizii ale Curții Constituționale au avut în vedere prevederile art. 360 alin. (3) CP, Curtea respingând criticile de neconstituționalitate prin clarificarea modului în care trebuie interpretată această variantă agravată a infracțiunii.

A susține că alin. (3) se reține de fiecare dată când este implicat un sistem informatic securizat, fără să prezinte relevanță în ce măsură au fost eludate sau nu măsurile de securitate implementate la nivelul acestuia (adică, identificarea unei forme calificate de acces), ar conduce la imposibilitatea reținerii art. 360 CP în formă de bază. Aceasta întrucât, este aproape imposibil de imaginat un sistem informatic care să nu aibă implementate „din fabrică" diverse măsuri de securitate, independent de activarea sau dezactivarea unor opțiuni suplimentare (e.g. cu privire la setarea unei parole, activarea sistemului de autentifica re în doi pași etc.) de către utilizator.

Așadar, apreciem că prevederile art. 360 alin. (3) CP nu suferă sub aspectul clarității și previzibilității, atât timp cât interpretarea textului de incriminare se află în concordanță atât cu rațiunea incriminării, cât și cu deciziile - obligatorii erga omnes - citate anterior.

11.2. Achitarea pentru fapta de divulgare a unor informații secrete de serviciu sau nepublice

Potrivit art. 304 alin. (1) CP, constituie infracțiune fapta de a divulga, fără drept, informații secrete de serviciu sau care nu sunt destinate publicității. Potrivit art. 304 alin. (2) CP, divulgarea constituie infracțiune dacă fapta este săvârșită de persoana care ia cunoștință de informațiile secrete de serviciu sau care nu sunt destinate publicității.

În principal, a apreciat că nu sunt îndeplinite elementele constitutive ale acestei infracțiuni raportat la următoarele aspecte:

Informațiile ce au făcut obiectul interogării bazelor de date nu au natura unor secrete de serviciu. Astfel, niciodată când se procedează la depunerea la dosarul cauzei a unui extras dintr-o astfel de bază de date nu se procedează la o declasificare.

Sintagma „informații nedestinate publicității” nu vizează orice date cu caracter personal care intră sub incidența regulamentului GDPR. în măsura în care s-ar concluziona faptul că orice divulgare a datelor cu caracter personal se transpune în reținerea art. 304 CP, ar însemna că încălcarea GDPR are întotdeauna o conotație penală.

Or, potrivit art. 12 din Legea nr. 190/2018, constituie contravenție procesarea nelegală a datelor cu caracter personal. Prin urmare, apreciem că nu putem discuta despre reținerea art. 304 CP în acele situații în care este incidentă răspunderea contravențională.

În mod evident, nu poate fi reținută în prezenta cauză urmarea referitoare la afectarea activității unei persoane. Prin urmare, se pune problema în ce măsură procesarea nelegală a datelor cu caracter personal se poate transpune în afectarea intereselor unor persoane. Inclusiv sub acest aspect, a apreciat că prezintă relevanță raportul dintre răspunderea penală și răspunderea contravențională. în măsura în care afectarea intereselor echivalează cu o atingere adusă vieții private, raportat la divulgarea unor date cu caracter personal, trebuia analizat în ce

măsură nu este aplicabilă răspunderea contravențională. Sub acest aspect, a apreciat că se poate discuta despre reținerea art. 304 CP doar în acele situații în care atingerea adusă intereselor unor persoane se transpune în lezarea unei valori sociale care nu este protejată de către GDPR - e.g. divulgarea unor informații din dosarele penale, divulgarea unor informații referitoare la urmărirea penală a unei persoane sau punerea în executare a unui mandat european de arestare.

B. CU PRIVIRE LA PRESCRIPȚIA RĂSPUNDERII PENALE

Prin HP. nr. 67/2022, înalta ##### de Casație și Justiție a statuat următoarele:

Normele referitoare la întreruperea cursului prescripției sunt norme de drept penal material (substanțial) supuse din perspectiva aplicării lor în timp principiului activității legii penale prevăzut de art. 3 din Codul penal, cu excepția dispozițiilor mai favorabile, potrivit principiului mitior lex prevăzut de art. 15 alin. (2) din Constituție și art. 5 din Codul penal.

Toate infracțiunile prev. la art. 304 CP s-au consumat și epuizat înainte de modificarea art. 155 alin. (1) CP prin OUG nr. 71/2022. Prin urmare; discutând despre o cauză pendinte, sunt deplin aplicabile DCCR nr. 297/2018 și nr. 358/2022. ##### în vedere art. 5 alin. (1) CP referitor la legea penală mai favorabilă, plasată în timp între data publicării DCCR nr. 297/2018 (25 iunie 2018) și data intrării în vigoare a OUG nr. 71/2022 (30 mai 2022), pentru faptele ce fac obiectul prezentului dosar rămâne lipsită de efecte juridice instituția întreruperii termenului de prescripție. Aceasta întrucât, legea penală mai favorabilă din perioada 25 iunie #### # ## mai 2022 se transpune în reținerea art. 155 alin. (1) CP în forma ce nu includea nicio cauză de întrerupere a termenului de prescripție.

Prin urmare, pentru analiza termenelor de prescripție ale răspunderii penale ne putem raporta doar la termenele generale de prescripție prevăzute la art. 154 alin. (1) CP și calculate potrivit art 186 alin. (1) CP, fără a ne putea raporta la termenul de prescripție specială.

În consecință, în subsidiar, în ceea ce privește infracțiunea prevăzută la art. 304 CP, necesită constatată prescripția răspunderii penale.

Pentru toate aceste motive inculpata a solicitat instanţei să dispună:

A. în principal, în temeiul art. 396 alin. (5) CPP rap. la art. 16 alin. (1) lit. b) teza I CPP, achitarea inculpatei ##### ####### ##### pentru infracțiunile prevăzute de art. 360 și 304 CP.

B. în subsidiar, cu privire la infracțiunea prevăzută la art. 304 CP, în temeiul art. 396 alin. (6) CPP rap. la art. 16 alin. (1) lit. f) CPP, încetarea procesului penal ca urmare a intervenirii prescripției răspunderii penale.

La data de 27.05.2024 Parchetul de pe lângă Tribunalul Bihor a depus la dosar concluzii scrise (f. 99 – 100), prin care a solicitat condamnarea inculpatei ##### ####### #####, în baza art. 396 alin. 2 Cod procedură penală, la pedeapsa închisorii pentru cele 11 infracţiuni de acces ilegal la un sistem informatic, prev. de art. 360 alin. 1, 2 şi 3 Codpenal, stabilită în condiţiile art. 36 alin. 1 Cod penal, în cazul faptelor de la pct. 8 şi 11 din rechizitoriu, cu aplicarea pedepsei rezultante în condiţiile art. 39 alin. 1 lit. b) Cod penal, faptele fiind în concurs real prev. de art. 38 alin. 1 Cod penal. A solicitat suspendarea pedepsei închisorii sub supraveghere, în condiţiile art. 91 și urm. Cod penal.

În esenţă, s-a arătat că inculpatei i s-a reţinut, în cazul celor 11 fapte, că în timpul programului de lucru, exercitându-şi atribuţiile de serviciu în cadrul ###. Mun. ######, a accesat şi efectuat interogări în bazele de date ######## persoanelor, ######## paşapoarte şi ########

auto, în scop personal, privind persoane care nu aveau nici o legătură cu atribuţiile sale de serviciu.

S-a mai arătat că problemele în discuţie în timpul dezbaterilor au fost dacă sunt probleme de legalitate a incriminării faptei, prev. de art. 360 Cod penal şi momentul consumării faptelor reţinute în sarcina inculpatei.

În ce priveşte claritatea şi predictibilitatea definiţiei infracţiunii prev. de art. 360 din Codul penal, Curtea Constituţională, prin respingerea mai multor excepţii de neconstituţionalitate, a tranşat această problemă, arătând că termenii de „sistem informatic" şi „date informatice" sunt definiţi suficient de clar în Codul penal, iar noţiunea „fără drept" este definită în art. 35 din Legea nr. 161/2003 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei, care rămâne în continuare un reper pentru înţelegerea elementelor de conţinut ale infracţiunii prev. de art. 360 din Codul penal (Decizia Curţii Constituţionale nr. 183 din 2018).

Potrivit art. 35 alin. 2 din Legea nr. 161/2003, acţionează fără drept persoana care se află în una dintre următoarele situaţii:

a) nu este autorizată, în temeiul legii sau al unui contract;

b) depăşeşte limitele autorizării;

c) nu are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfăşura cercetări ştiinţifice sau de a efectua orice altă operaţiune într-un sistem informatic.

În alin. 1 lit. c) al aceiulaşi articol este definit şi programul informatic.

În condiţiile în care prevederile menţionate potrivit art. 34 din Legea nr. 161/2003, sunt incluse în dispoziţiile legale care reglementează prevenirea şi combaterea criminalităţii informatice, prin măsuri specifice de prevenire, descoperire şi sancţionare a infracţiunilor săvârşite prin intermediul sistemelor informatice, asigurându-se respectarea drepturilor omului şi protecţia datelor personale, apreciem că înţelegerea dispoziţiilor art. 360 din Codul penal nu ridică probleme.

În ce priveşte momentul consumării infracţiunii comisă de inculpată, apreciez că acesta este momentul interogării bazelor de date şi nu cel al intrării în contul de utilizator prin folosirea numelui de utilizator şi al parolei, pe care aceasta era autorizată să le folosească.

Fapta acesteia s-a consumat în momentul în care a accesat bazele de date ale diferitelor instituţii introducând date pe care nu era autorizată să le folosească (numele persoanelor, numere de înmatriculare etc.) întrucât interogarea nu s-a impus pentru exercitarea unei atribuţii de serviciu, limitele în care inculpatei i se permitea interogările fiind pe deplin explicate de procuror în secţiunea „ÎNCADRAREA JURIDICĂ – cadrul legal şi infralegal, analizarea elementelor constitutive ale infracţiunilor cercetate".

Faptul că interogările s-au efectuat de inculpată în afara atribuţiilor de serviciu rezultă fără dubiu din probele administrate în cursul urmăririi penale, pe care inculpata a arătat la ultimul termen de judecată că înţelege să nu le mai conteste.

Pentru cele trei infracţiuni de divulgarea informaţiilor secrete de serviciu sau nepublice prev. de art. 304 alin. 1 din Codul penal pentru care inculpata a fost trimisă în judecată prin rechizitoriului emis la data de 27.10.2021 în dosarul nr. ###/P/2020 de procurorul din cadrul

Parchetului de pe lângă Tribunalul Bihor, solicit încetarea procesului penal în temeiul art. 16 alin. 1 lit. f din Codul penal întrucât a intervenit prescripţia răspunderii penale. ##### în vedere că faptele au fost comise în luna noiembrie 2018 (15 noiembrie faptele de la pct. 5 şi 6 din rechizitoriu; 19 noiembrie fapta de la pct 9 din rechizitoriu) iar pedeapsa închisorii prevăzută de lege este între 3 luni şi 3 ani, termenul de 5 ani de prescripţie a răspunderii penale prev. de art. 154 alin. 1 lit. d din Codul penal s-a împlinit în luna noiembrie 2023, neexistând niciun caz de întrerupere astfel cum s-a stabilit prin Deciziile Curţii Constituţionale nr ######## şi 358/2022.

Analizând situaţia de fapt prin raportare la normele legale incidente şi coroborând ansamblul probatoriu administrat în cursul urmăririi penale, instanţa reţine următoarele:

Preliminar expunerii situaţiei de fapt, instanţa reaminteşte că inculpata, prin avocat, a renunţat la cercetarea judecătorească aplicabila procedurii de drept comun după ce, anterior, i-au fost încuviinţate mijloacele de probă, solicitate a fi administrate în faţa instanţei de fond.

În acelaşi plan, din perspectiva probelor administrate în cauză şi a apărărilor formulate pe fondul cauzei, instanţa observă că inculpata, prin avocat, nu contestă situaţia de fapt reţinută prin actul de sesizare, criticile acesteia fiind expuse doar în legătură cu realizarea tipicităţii obiective şi subiective a infracţiunilor care formează obiectul acţiunii penale. Drept urmare, din analiza coroborata a mijloacelor de probă administrate în cursul urmăririi penale care vor fi expuse cu privire la fiecare faptă, instanţa constata că se confirma situaţia de fapt expusă prin actul de sesizare, în modalitatea următoare:

I.ÎN FAPT

1.La data de 21 august 2017, în intervalul orar 00:30-00:39, potrivit procesului verbal de consemnare a rezultatului verificărilor întocmit în 19.10.2020 de lucrătorii D.G.A. delegaţi în cauză, de pe userul suspectei ##### (fostă ###) ######## ##### (ILECM) au fost efectuate în bazele de date ale M.A.I. verificări cu privire la persoana numiţilor ###### ###### (evidenţa Persoanei), ######## ###### (evidenţa Persoanei, ######## Auto şi Paşapoarte) şi ######## ###### (evidenţa Populaţiei), aceste verificări fiind efectuate neautorizat de inculpata ##### (###) ########, fără a se putea stabili motivul pentru care au fost efectuate aceste verificări, respectiv dacă inculpata a transmis unei/unor alte persoane datele accesate nelegal. Din acelaşi proces verbal rezultă că inculpata nu a menţionată în bazele de date motivul căutării, deşi avea această obligaţie, fiind inserată doar litera „a”.

Din adresa Poliţiei Mun.###### din 28.04.2021, rezultă că inculpata ##### ######## a fost planificată de serviciu în intervalul orar 20.08.2017 orele 19:00 – 21.08.2017, orele 07:00. Pe cale de consecinţă, inculpata se afla la serviciu la momentul accesării bazelor de date în intervalul orar 00:30 – 00:39 de pe userul ILECM (userul atribuit inculpatei – fapt comunicat de Direcţia pentru ######## Persoanelor şi Administrarea Bazelor de #### prin adresa din 03.01.2019), fiind astfel exclusă posibilitatea folosirii userului acesteia de către o altă persoană, fără acordul inculpatei.

Din cercetări a rezultat că accesarea şi logarea la aceste baze de date cu privire la entităţile verificate mai sus menţionate s-a efectuat fără drept, în afara atribuţiilor serviciu, fapt dovedit atât de declaraţiile martorilor audiaţi, cât şi de înscrisurile predate de ###.Mun.######.

Astfel, din fişa de intervenţie la eveniment din 19.08.2017, rezultă că lucrătorii de poliţie din cadrul Biroului Ordine ######## ###.Mun.###### au fost sesizaţi în acea noapte cu privire la comiterea unei agresiuni în incinta localului „RIVO ###### CLUB”, situat în ######,

str.Şanţului, în care au fost implicaţi numiţii ######## ###### şi ####### ######, aceştia fiind conduşi apoi la sediul Poliţiei Mun.######, în vederea întocmirii procesului verbal de constatare. În cuprinsul acelei fişe de intervenţie au fost stipulate şi datele de identificare ale acestora, şi anume CNP, domiciliul, numele etc. UIterior, la aceeaşi dată, fişa de intervenţie a fost implementată în sistemul S.N.R.I. (Sistemul Naţional de ######## Informative) de către agentul ######## ######. Apoi, la data de 21.08.2017, s-a întocmit o lucrare penală în legătură cu acel incident, fiind sesizat Parchetul de pe lângă Judecătoria ######, care a înregistrat dos.nr.####/P/2017. În acea cauză, s-a dispus începerea urmăririi penale sub aspectul săvârşirii infracţiunii prev. de art.193 alin.1 c.pen. prin ordonanţa organelor de cercetare penală din 19.08.2017.

Din declaraţia martorului ###### (fostă #######) ###### ########, rezultă că în vara anului 2017, în luna august, a fost implicată într-o agresiune împreună cu prietenul său de atunci ###### ########, care apoi a fost reclamată la poliţie de numitul ##### ####, sens în care au fost conduşi toţi trei la sediul ###.Mun.###### în acea noapte, unde au fost legitimaţi, în baza actelor de identitate pe care le aveau asupra lor. Nu cunoaşte dacă ea şi ######## ###### au fost verificaţi atunci în baza de date a poliţiei, însă ulterior au fost cercetaţi penal de către poliţiştii de la #####. Susnumita a menţionat că în acel scandal nu a fost implicat ###### ###### (persoană pe care îl cunoaşte de mult timp din oraş). Fiind întrebată, martorul a aratat că nu cunoaşte nicio poliţistă care să lucreze la ###.Mun.###### şi care să se ocupe cu verificări în baza de date. Fiindu-i indicat numele de ### ##### #######, aceasta a precizat că nu o cunoaşte. ##### că nu doreşte să se constitui parte civilă în cauză, în eventualitatea în care se va ajunge la concluzia că a fost căutată în baza de date cu încălcarea legii.

În acelaşi sens a declarat şi martorul ######## ######, care a arătat că în acea noapte când a avut loc altercaţia, a fost condus de organele de poliţie la sediul PMO, unde i s-a luat o declaraţie şi a fost legitimat de organele de poliţie, sens în care fie le-a dictat poliţiştilor datele sale de identificare, fie le-a înmânat cartea de identitate. ###### ###### nu a avut nicio participare la acel eveniment. Fiind întrebat, arată că nu i-a fost niciodată trimisă vreo fotografie prin nicio modalitate de comunicare la distanţă, din care să rezulte că ar fi fost căutat în bazele de date. Fiindu-i adus la cunoştinţă faptul că a fost căutat în baza de date – evidenţă persoane în noaptea de 21.08.2017, ora 0.30, după care la câteva minute, au fost căutaţi în baza de date de acelaşi lucrător de poliţie, numiţii ###### ###### şi ###### #######, acesta a declarat că nu şi explică această împrejurare. A mai menţionat că nu o cunoaşte pe inculpata ##### (###) #######, poliţista care l-a căutat în acea bază de date.

Pe cale de consecinţă, atâta vreme cât numiţii ###### (#######) ######, ######## ###### şi ###### ###### nu au fost implicaţi în noaptea de 21.08.2017 într-un eveniment (savârşirea unei contravenţii, infracţiuni etc.) de natură a necesita verificarea acestora în bazele de date administrate de M.A.I., rezultă că verificările efectuate de inculpată în bazele de date menţionate cu privire la cele trei entităţi sunt realizate cu depăşirea limitelor legale. #### adevărat că numiţii ###### (#######) ######, ######## ###### au fost implicaţi într-o agresiune cu două zile înainte de a avea loc accesarea bazelor de date de către inculpată, însă acel eveniment s-a produs pe tura de noapte a altor colegi de poliţie de la Biroul Ordine #######, care au implementat lucrarea în baza de date în acea noapte şi au sesizat parchetul competent,

fiind întocmit dosar penal încă din data de 19.08.2017, astfel că nu există niciun motiv plauzibil care să reclame intervenţia inculpatei în speţa respectivă.

Inculpata nu a dorit să dea declaraţii cu privire la acuzaţia adusă, astfel că nu s-a putut dovedi motivul pentru a efectuat verificări în bazele de date cu privire la cele trei persoane fizice, în condiţiile în care nici măcar nu ii cunoştea pe ###### ###### şi ######## ######.

In concluzie, se retine ca inculpata ##### (fostă ###) ####### #####, agent şef adjunct de poliţie în cadrul ###.Mun.######-Biroul Ordine #######, în noaptea de 21 august 2017, ora 00:30-00:39, în exercitarea în exercitarea atribuţiilor de serviciu, aflându-se în incinta Poliţiei Municipiului ###### - Biroul Supravegheri Video", folosind userul şi parola proprie, a accesat şi interogat mai multe baze de date administrate de M.A.I.- D.E.P.A.B.D., şi anume ######## Auto, ######## Persoane ,respectiv ######## Paşapoarte, cu privire la numiţii ###### ###### (evidenţa Persoanei), ####### ###### (evidenţa Persoanei, ######## Auto şi Paşapoarte) şi ######## ###### (evidenţa Populaţiei), scopul verificărilor nefiind unul în interes de serviciu, ci personal.

2. Potrivit procesului verbal de consemnare a rezultatului verificărilor întocmit în 19.10.2020 de lucrătorii D.G.A. delegaţi în cauză, la data de 11.03.2018, în intervalul orar 17.12 – 17.37, , fără nicio justificare, inculpata a accesat şi efectuat interogări în bazele de date ######## Persoanelor, ######## Paşapoarte şi ######## Auto, privind pe numita ####### ####### ######, persoană aflată în cercul relaţional al numitului ###### ######, precum şi cu privire la membrii de familie ai acesteia (####### #### ####### – tatăl, ####### ####### ######-mama şi ####### #### ##### – Fratele ei).

Din declaraţia martorului ####### ####### ###### rezultă că nu are cunoştinţă despre efectuarea de verificări în bazele de date ale Poliţiei cu privire la persoana sa sau a familiei mele, nu o cunoaşte pe ##### (###) #######, iar în cursul lunii martie a anului 2018, nu a avut vreo vreun contact cu lucrătorii de poliţie din ####### ##### #### ## ## ########## ########## ## ########## ## ###### ## #### ### #.A.I. Susnumita a mai arătat că îl cunoaşte pe numitul ###### ######, cu care a avut o relaţie în cursul anului 2015 şi are cunoştinţă că în anul 2018 a intervenit un conflict între acesta şi fostul prieten al martorei, numitul ###### #####.

Din adresa Poliţiei Mun.###### din 28.04.2021, rezultă că inculpata ##### ####### a fost planificată de serviciu pentru data de 11.03.2018, între orele 07:00 – 19:00. Pe cale de consecinţă, inculpata se afla la serviciu la momentul accesării bazelor de date în intervalul orar 17:21-17:37 de pe userul ILECM (userul atribuit inculpatei – fapt comunicat de Direcţia pentru ######## Persoanelor şi Administrarea Bazelor de #### prin adresa din 03.01.2019), fiind astfel exclusă posibilitatea folosirii userului acesteia de către o altă persoană, fără acordul inculpatei.

Inculpata nu a dorit să dea declaraţii cu privire la acuzaţia adusă, astfel că nu s-a putut dovedi motivul pentru a efectuat verificări în bazele de date cu privire la cele trei persoane fizice, în condiţiile în care nici măcar nu o cunoştea pe ####### #######.

În concluzie, se retine ca inculpata ##### ####### #####, la data de 11.03.2018, în intervalul orar 17.12 – 17.37, fără nicio justificare, a accesat şi efectuat interogări în bazele de date ######## Persoanelor, ######## Paşapoarte şi ######## Auto, privind pe numita ####### ####### ######, persoană aflată în cercul relaţional al numitului ###### ######, precum şi cu privire la membrii de familie ai acesteia (####### #### ####### – tatăl, ####### ####### ######-mama şi ####### #### ##### – Fratele).

3. La data de 24.04.2018 (la trei zile după ce numitul ###### ###### a căutat-o în bazele de date M.A.I. pe numita ####### ######## #####, folosind userul şi parola suspectei ##### #######, acesta fiind trimis în judecată în dos.###/P/2018 pt. săvârşirea infracţiunii prev. de art.360 alin.1,2,3 din c.penal, alături de ##### #######, pentru complicitate la infracţiunea prev. de art.360 c.pen.), în intervalul orar 14:53 – 14:55, de pe userul suspectei ##### ####### (ILECM), au fost efectuate verificări în bazele de date ######## Persoane, ######## Auto şi ######## Paşapoarte, cu privire la persoana numitului ### ###### ###### (prietenul numitei ##### ####### la acea vreme, actualul soţ al acesteia), respectiv a familiei acestuia (### #### ###### -tatăl, chestor de poliţie, şi ### ######## #####-mama sa).

Potrivit declaraţiei martorului ### ####, referitor la existenta vreunui contact cu lucratorii de politie din cadrul Politiei Municipiului ###### sau chiar din cadrul Inspectoratului de Politie ######## Bihor, acesta a arătat faptul ca in cursul anului 2018 cu siguranta nu am avut nici un fel de contact. Nu a fost oprit de catre lucratori de politie din cadrul acestei institutii si nici nu a avut nevoie de sprijinul sau ajutorul acestora. In ceea ce priveste efectuarea unor verificari cu privire la persoana sa si cu privire la membrii familiei sale in cursul zilei de 24 aprilie 2018, arată faptul ca nu îşi poate explica motivul efectuarii acestor verificari in bazele de date apartinand Ministerului Afacerilor Interne cu privire la cetatenii romani. A menţionat că familia sa este alcatuita din 4 membri: el, sotia sa ### #### ######## ##### si fii săi ### ##### #### si ### ###### ######. De asemenea, a mai arătat că fiul său ### ###### ###### este intr-o relatie de prietenie si locuieste impreuna cu numita ##### ####### ########.

Din adresa Poliţiei Mun.###### din 28.04.2021, rezultă că inculpata ##### ####### a fost planificată de serviciu pentru data de 24.04.2018, între orele 07:00 – 19:00. Pe cale de consecinţă, inculpata se afla la serviciu la momentul accesării bazelor de date în intervalul orar 14:53-14:55 de pe userul ILECM (userul atribuit inculpatei – fapt comunicat de Direcţia pentru ######## Persoanelor şi Administrarea Bazelor de #### prin adresa din 03.01.2019), fiind astfel exclusă posibilitatea folosirii userului acesteia de către o altă persoană, fără acordul inculpatei.

În concluzie, se retine ca inculpata ##### ####### #####, la data de 24.04.2018, în intervalul orar 14.53 – 14.55, fără nicio justificare, în timp ce îşi exercita atribuţiile de serviciu în sediul Poliţiei Mun.######, a accesat şi efectuat interogări în bazele de date ######## Persoanelor, ######## Paşapoarte şi ######## Auto, privind pe numitului ### ###### ###### (prietenul numitei ##### ####### la acea vreme, actualul soţ al acesteia), respectiv a familiei acestuia (### #### ###### -tatăl, chestor de poliţie, şi ### ######## #####-mama sa), în interes personal.

4.Potrivit procesului verbal de consemnare a rezultatului verificărilor întocmit în 12.02.2019 de lucrătorii D.G.A. delegaţi în cauză,la data de 23.10.2018, intervalul orar 00:08-00:09, suspecta ##### #######, în timpul exercitării exercitarea atribuţiilor de serviciu, a accesat si interogat, în interes privat, cu depăşirea limitelor autorizării, baza de date DEPABD – ######## Auto, pentru a identifica autoturismul PORSCHE #######, de culoare roşie, cu numarul de înmatriculare #########, înmatriculat pe SC ###### SRL, autoturism folosit la acea vreme de numita ##### ####### ######## (o cunoscută interpretă de muzică), care s-a aflat în ########## ## ######## #####.10.2018, când a avut două evenimente artistice, deplasarea efectuând-o cu autovehiculul mai sus menţionat, motiv pentru care s-a dispus prin ordonanţa din 21.02.2021 extinderea urmăririi penale şi efectuarea în continuare a urmăririi

penale faţă de suspecta ##### ####### #####, sub aspectul săvârşirii infracţiunii de acces ilegal la un sistem informatic, prev. de art.360 alin.1,2 şi 3 cod penal.

Din adresa Poliţiei Mun.###### din 28.04.2021, rezultă că inculpata ##### ####### a fost planificată de serviciu pentru data de 23.10.2018 (tură de noapte), în intervalul orar 19:00 (22.10.2018) - 07:00 (23.10.2018). Pe cale de consecinţă, inculpata se afla la serviciu la momentul accesării bazelor de date în intervalul orar 00:08-00:09 de pe userul ILECM (userul atribuit inculpatei – fapt comunicat de Direcţia pentru ######## Persoanelor şi Administrarea Bazelor de #### prin adresa din 03.01.2019), fiind astfel exclusă posibilitatea folosirii userului acesteia de către o altă persoană, fără acordul inculpatei.

Din declaraţia martorului ### ##### ####### din 11.02.2019 rezultă ca din cursul anului 2017 utilizează un autoturism marca PORSCHE #######, de culoare rosie, cu numărul de înmatriculare #########, autovehicul înmatriculat pe o societate comercială. Precizează faptul ca in cursul lunii octombrie 2018, in datele de 20 si 21, a avut doua evenimente artistice in Mun. ######, deplasarea efectuând-o cu autovehiculul menţionat mai sus.

Inculpata ##### nu a dorit să dea declaraţii cu privire la acuzaţia adusă, astfel că nu s-a putut stabili scopul efectuării de verificări în bazele de date cu privire la autoturismul utilizat de martorul mai sus menţionat, în condiţiile în care nici măcar nu o cunoştea personal pe aceasta.

În concluzie, se retine ca inculpata ##### ####### #####, în noaptea de 23.10.2018, în intervalul orar 00:08 – 00:09, fără nicio justificare, în timp ce îşi exercita atribuţiile de serviciu în sediul Poliţiei Mun.######, a accesat şi efectuat interogări în bazele de date ######## Auto, privind autoturismul PORSCHE #######, de culoare roşie, cu numarul de înmatriculare #########, înmatriculat pe SC ###### SRL, autoturism folosit la acea vreme de numita ##### ####### ########, în interes personal.

5. La data de 15.11.2018, la solicitarea unei cunoştinţe (persoană de sex feminin, care utiliza nr de telefon ##########, cu prenumele „####"), în intervalul orar 21:51 – 22:28, numita ### #######, în timp ce îşi exercita atribuţiile de serviciu la sediul Poliţiei Mun.######, a accesat bazele de date ######## Persoanelor şi ######## Auto, în vederea identificării şi aflării datelor personale ale unui anume ##### #######, care ar fi tatăl lui ##### ####, respectiv a soţiei acestuia (identificată ca ##### ####### ##### – decedată în 1992), fără însă a reuşi în cele din urmă identificarea persoanei solicitate de cunoştinţa sa, după care i-a comunicat acesteia datele personale ale persoanelor identificate în bazele de date.

În urma efectuării cercetărilor în cauză, cunoştinţa suspectei a fost identificată în persoana numitei ###### ####### #######.

Fiind audiată în calitate de martor şi ulterior în calitate de suspectă, numita ###### ####### ####### a declarat că cunoscut-o pe inculpata ##### ####### la un eveniment unde au făcut și schimb de numere de telefon. Datorită faptului că soțul ei ###### ######## a fost adoptat, a încercat să-l ajute în a-și regăsi sora mai mare despre care știa că se numește #######. Cu privire la acest aspect, susnumita a arătat că inculpata ##### ####### i-a spus la acel eveniment privat că lucrează la Poliţie, la dispecerat şi că în virtutea atribuţiilor de serviciu, are acces la bazele date la ######## Persoanelor. Astfel, aceasta s-a oferit ca, în eventualitatea în care are nevoie să găsească datele de identificare ale unei persoane, inculpata o poate ajuta, întrucât are acces la aceste informaţii, fiind poliţistă. ##### în vedere această discuţie, după cateva luni, a contactat-o pe ##### #######, în condiţiile în care soţul efectua căutări cu privire

la familia sa naturală (el fiind adoptat) şi a rugat-o pe aceasta să o ajute în acest sens, din moment ce aceasta îşi oferise deja ajutorul. Martora a mai menţionat că „Doresc să subliniez că eu nu am știut că efectuarea unor asemenea de în bazele de date, fără a exista o solicitare scrisă adresată Poliţiei, nu este permisă de lege. #### aș fi cunoscut acest aspect nu aș fi întrebat pe nimeni, însă inculpata ##### ####### nu m-a avertizat în acest sens, ci dimpotrivă, m-a încurajat".

Cele declarate de suspecta ###### ####### ####### se coroboreaza intru totul cu procesul-verbal de consemnare a rezultatului verificarilor intocmit la data de 19.02.20219.

În concluzie, se retine ca inculpata ##### ####### #####, în seara zilei de 15.11.2018, în intervalul orar 21:51 – 22:28, la instigarea suspectei ###### ####### #######, fără nicio justificare, în timp ce îşi exercita atribuţiile de serviciu în sediul Poliţiei Mun.######, a accesat şi efectuat interogări în baza de date „######## Persoanelor" în interesul personal al suspectei, cu privire la entităţile „##### ####", „##### ##### #######", „##### ########" şi „##### ###", după care a divulgat datele de identificare acelor persoane (numele, legături de rudenie, anul naşterii, domiciliul) suspectei ###### ####### #######.

6. În noaptea de 15.11.2018, în intervalul 23:54 – 23:59, în timpul convorbirii telefonice cu concubinul ei, suspectul ######## ######, inculpata ##### (###) ####### a accesat bazele de date ######## Persoanelor, ######## Paşapoarte şi ######## Auto, în vederea identificării şi aflării datelor personale ale numitei #### ####### #######, cu care concubinul ar fi intrat într-un conflict profesional, cei doi fiind colegi de muncă la o societate comercială (SC ############ ####### ######### ####### SRL), după care i-a comunicat telefonic lui ######## ###### aceste date cu caracter confidenţial, şi anume nume complet, starea civilă, anul naşterii, autoturismele pe care le a avut în proprietate şi ocupaţia.

Din procesul verbal de consemnare a rezultatului verificărilor întocmit în 19.02.2019, din care rezultă că inculpata a efectuat acele interogări în legătura cu persoana vătămată #### ####### #######, în bazele de date ######## Persoanelor, ######## Auto şi ######## Paşapoarte, în intervalul orar 23:54-23:59.

Fiind audiată în calitate de martor, numita #### ####### ####### a declarat că îl cunoaşte pe suspectul ########, cu care este coleg de serviciu la SC ############ ####### ######### ####### SRL, că nu a avut vreun conflict cu acesta. În schimb, a arătat că nu o cunoaşte pe ##### #######.

În concluzie, se retine ca inculpata ##### ####### #####, în seara zilei de 15.11.2018, în intervalul orar 23:54 – 23:59, fără nicio justificare, în timp ce îşi exercita atribuţiile de serviciu în sediul Poliţiei Mun.######, a accesat şi efectuat interogări în bazele de date „######## Persoanelor", ######## Paşapoarte şi ######## Auto" în interesul său personal şi al concubinului său ######## ######, cu privire la persoana vătămată #### ####### #######, după care a divulgat datele de identificare a persoanei vătămate (numele, starea civilă, anul naşterii, autoturismele deţinute, ocupaţia) numitului ######## ######, coleg de serviciu cu persoana vătămată.

7. La data de 24.11.2018, în intervalul orar 10:38 – 10:44, în urma purtării unei discuţii telefonice cu numitul ######## ######, inculpata ##### (###) ####### a accesat neautorizat (în scop personal) bazele de date ######## Persoanelor şi ######## Auto, în vederea identificării şi aflării datelor personale ale numitei ##### ##### ######### (posibil poliţistă în

cadrul ###.Mun.Beiuş), după care a comunicat concubinului său ######## ###### datele de identificare ale acesteia.

Astfel, după ce ######## ###### i-a comunicat inculpatei că a identificat-o pe facebook pe numita ##### ##### ######### (persoană pe care ######## o cunoştea), unde ar fi postat o fotografie din care ar rezulta că poartă uniformă de poliţist, lucru care numitului ######## ###### i se părea neverosimil, raportat la studiile, cel mai probabil din curiozitate, inculpata ##### a accesat cele trei baze de date, efectuând mai multe interogări în vederea identificării persoanei indicate de concubinul ei, fapt care rezultă din procesul verbal de consemnare a rezultatului verificărilor privitor la situaţia interogărilor efectuate în 18.11.2018 de utilizatorul ILECM, întocmit de lucrătorii DGA delegaţi în cauză.

În concluzie, se retine ca inculpata ##### ####### #####, în la data de 18.11.2018, în intervalul orar 10;38 – 10:45, fără nicio justificare, în timp ce îşi exercita atribuţiile de serviciu în sediul Poliţiei Mun.######, a accesat şi efectuat interogări în bazele de date „######## Persoanelor", „######## Auto" şi „######## Paşapoarte", în interesul personal al suspectei, cu privire la entitatea „##### ##### #########".

8. La datele de 20.11.2018 (intervalul orar 03:33-03:48) şi 24.11.2018 (intervalul orar 01:23-01:25), în baza aceleiaşi rezoluţiuni infracţionale, sub justificarea nereală a efectuării unor verificări operative, inculpata a accesat şi efectuat interogări în bazele de date ######## Persoanelor şi ######## Paşapoarte, privind pe numita ###### #####, colegă de serviciu cu concubinul ei, ######## ######, întrucât observase că susnumita figurează ca şi „prietenă" pe aplicaţia Facebook cu ######## ######.

La data de 20.11.2018 (intervalul orar 03:33 – 03:48), cât şi la data de 24.11.2018 (intervalul orar 01:23-01:25), inculpata ##### ####### a procedat la accesarea şi interogarea în bazele de date ######## Persoanelor şi ######## Paşapoarte a persoanei ###### #####, născută în anul 1989, fapt care rezultă din procesul verbal de consemnare a rezultatului verificărilor întocmit de lucrătorii DGA delegaţi în cauză privitor la situaţia interogărilor efectuate în 20.11.2018 şi 24.11.2018 de utilizatorul ILECM (### #######).

Din declaraţia martorului ##### ###### rezultă că nu cunoaşte absolut nimic referitor la verificările efectuate în bazele de date de către inculpată, pe care nu o cunoaşte. În schimb, îl cunoaşte pe numitul ######## ######, acesta fiind supervizorul ei la locul de muncă, fiind totodată prieteni pe facebook la un moment dat. ##### în vedere motivul audierii și fiind vorba despre colegul ei ###### ########, martorul consideră că verificarea în baza de date a fost efectuată de către inculpată din motive de gelozie.

În concluzie, se retine ca inculpata ##### ####### #####, la datele de 20.11.2018 (intervalul orar 03:33-03:48) şi 24.11.2018 (intervalul orar 01:23-01:25), în baza aceleiaşi rezoluţiuni infracţionale, sub justificarea nereală a efectuării unor verificări operative, a accesat şi efectuat interogări în bazele de date ######## Persoanelor şi ######## Paşapoarte, privind pe numita ###### #####, întrucât observase că susnumita figurează ca şi „prietenă" pe aplicaţia Facebook cu concubinul ei ######## ######.

9. La data de 19.11.2018, în intervalul orar 20:10 – 20:17, la solicitarea telefonică a suspectului ######## ######, inculpata ##### ####### a accesat neautorizat (în scop personal) bazele de date ######## Auto, în vederea identificării şi aflării datelor personale ale persoanei care posedă autoturismul cu numărul de înmatriculare ## ## ###, întrucât aceasta ar fi parcat pe

locul de parcare al susnumitului, sens în care inculpata ##### ####### a identificat-o pe numita ####### ####### ######, ale cărei date personale (profesie, adresă de domiciliu, autoturism folosit, situaţia familială, anul naşterii), pe care le-a aflat în urma accesării bazei de date ######## Persoanelor, le-a comunicat telefonic, respectiv prin intermediul aplicaţiei whattapp, suspectului ######## ######, cu scopul ca acesta să se deplaseze la locuinţa susnumitei pentru a-i reproşa modalitatea defectuoasă de parcare a autoturismului pe locul suspectului,

Din declaraţia martorului ####### ####### rezultă că, într-adevăr, deține în proprietate un autovehicul marca Toyota, de culoare roșie cu numărul de înamtriculare ######### încă din anul 2017, că are o fetiță născută în anul 2006, că este divorţată, că are ocupaţie asistent medical. În schimb, a arătat că nu îl cunoaşte pe suspectul ######## ######, nu cunoaşte să fi avut vreun conflict cu vreo persoană în legătură cu faptul că ar fi parcat neregulamentar. Martorul consideră că i-a fost adusă o atingere vieţii private prin accesarea datelor sale de identitate de către inculpată însă nu doreşte să participe la procesul penal ca şi persoană vătămată.

Din adresa Poliţiei Mun.###### din 28.04.2021, rezultă că inculpata ##### ####### a fost planificată de serviciu pentru data de 19.10.2018 (tură de noapte), în intervalul orar 19:00 (19.10.2018) - 07:00 (20.10.2018). Pe cale de consecinţă, inculpata se afla la serviciu la momentul accesării bazelor de date în intervalul orar 20.10-20:18 de pe userul ILECM (userul atribuit inculpatei – fapt comunicat de Direcţia pentru ######## Persoanelor şi Administrarea Bazelor de #### prin adresa din 03.01.2019), fiind astfel exclusă posibilitatea folosirii userului acesteia de către o altă persoană, fără acordul inculpatei.

În concluzie, se retine ca inculpata ##### ####### #####, în seara zilei de 19.10.2018, date în intervalul orar 20.10-20:18, fiind determinată de suspectul ######## ######, fără nicio justificare, în timp ce îşi exercita atribuţiile de serviciu în sediul Poliţiei Mun.######, a accesat şi efectuat interogări în bazele de date „######## Persoanelor”, ######## Paşapoarte şi ######## Auto” în interesul său personal şi al concubinului său ######## ######, cu privire la numita ####### ####### ######, după care a divulgat datele de identificare ale acesteia (numele, starea civilă, anul naşterii, autoturismele deţinute, ocupaţia, adresa) martorului ######## ######, persoană interesată de aflarea acestor date.

10. Din procesul din procesul verbal de consemnare a rezultatului verificărilor întocmit de lucrătorii DGA privitor la situaţia interogărilor efectuate în 22.11.2018, ora 17:45, de utilizatorul ILECM (### #######), rezultă că inculpata a accesat şi efectuat o interogare în baza de date ######## Auto, în interes personal, privind pe numitul ### ######## ##### ####, sub justificarea nereală a efectuării unor verificări operative, în contextul în care dorea identificarea acestuia după autoturismul folosit, pentru a-l contacta în vederea furnizării de lemne.

Fiind audiat în calitate de martor, numitul ######## ### ##### confirmă faptul că în anul 2018 a efectuat diferite transporturi de lemne sau nisip cu autoturismele sale ######## Sprinter şi Daily Iveco şi că este posibil să fi făcut un astfel de serviciu şi inculpatei ##### #######, pe care a recunoscut o din fotografie ca fiind soţia unei persoane căreia i-a mai transportat porumb.

În concluzie, se retine ca inculpata ##### ####### #####, la data de 22.11.2018, ora 17:45, sub justificarea nereală a efectuării unor verificări operative, a accesat şi efectuat interogări în bazele de date ######## Auto, privind pe numitul ### ######## ##### ####, întrucât dorea să apeleze la serviciile acestuia pentru a-i transporta lemne.

11. Din probele administrate în cauză (proces verbal de verificări in bazele de date DEPABD din 19.02.2019, interceptări ale unor convorbiri telefonice) rezultă că în perioada 26.10.2018 – 24.11.2018, şi anume la datele de 26.10 (ora 19:21), 27.10 (ora 06:10), 30.10 (ora 23:46), 31.10 (ora 02:38) şi 24.11 (ora 01:26), în baza aceleiaşi rezoluţiuni infracţionale, în timp ce se afla la serviciu, sub justificarea nereală a efectuării unor verificări operative, inculpata a accesat şi efectuat interogări în bazele de date ######## Persoanelor şi ######## Auto, privind pe numita ######## #####, colegă de serviciu cu numitul ######## ######, (concubinul suspectei), cât şi pe fratele acesteia, ######## #### #####.

Martorul ######## ##### a declarat că îl cunoaşte pe numitul ######## ######, întrucât sunt colegi de serviciu, în schimb nu o cunoaşte pe inculpata ##### #######. Fiind întrebată dacă la nivelul anului 2018, luna noiembrie a avut vreo situație, contact cu lucrătorii de poliție care să fi determinat efectuarea de verificări în bazele de date ale M.A.I., aceasta a răspuns că nu a avut nici o astfel de situație, nu este conducător auto și nu a fost vreodată oprită pentru identificare de către lucrători de poliție. Susnumita a mai arătat că în perioada respectivă avea o relație cu un coleg de serviciu, de la care a aflat că numitul ###### ######## ar fi și el într-o relație cu o polițistă care este foarte geloasă. Martorul a menţionat că i s-a adus o atingere vieţii private prin accesarea şi interogarea bazelor de date în legătură cu persoana sa, dar nu doreşte să participe la proces în calitate de persoană vătămată, nu solicită despăgubiri de la inculpată.

În concluzie, se retine ca inculpata ##### ####### #####, în perioada 26.10.2018 – 24.11.2018, şi anume la datele de 26.10 (ora 19:21), 27.10 (ora 06:10), 30.10 (ora 23:46), 31.10 (ora 02:38) şi 24.11 (ora 01:26), în timp ce ce afla la serviciu-sediul ###.Mun.######, în baza aceleiaşi rezoluţiuni infracţionale, sub justificarea nereală a efectuării unor verificări operative, a accesat şi efectuat interogări în bazele de date ######## Persoanelor şi ######## auto, privind pe numita ######## #####, întrucât avea suspiciuni ca aceasta ar fi avut o relaţie cu concubinul ei ######## ######.

II.1.Infracţiunea de acces ilegal la un sistem informatic, prev. de art.360 alin.1,2 şi 3 cod penal (pct.1-11 din rechizitoriu)

Dispoziţii legale incidente:

Art. 360 Cod penal

”(1) Accesul, fără drept, la un sistem informatic se pedepseşte cu închisoare de la 3 luni la 3 ani sau cu amendă.

(2) Fapta prevăzută în alin. (1), săvârşită în scopul obţinerii de date informatice, se pedepseşte cu închisoarea de la 6 luni la 5 ani.

(3) #### fapta prevăzută în alin. (1) a fost săvârşită cu privire la un sistem informatic la care, prin intermediul unor proceduri, dispozitive sau programe specializate, accesul este restricţionat sau interzis pentru anumite categorii de utilizatori, pedeapsa este închisoarea de la 2 la 7 ani.”

Definiția noțiunii „fără drept” cuprinsă în conținutul constitutiv al infracțiunii de acces ilegal la un sistem informatic, deși nu este definită în partea generală a codului penal sau în norma de incriminare, se regăsește în conţinutul prevederilor art. 35 alin. (2) din Legea nr. 161/2003, respectiv, acționează fără drept persoana care se află în una dintre următoarele situații:

a) nu este autorizată, în temeiul legii sau al unui contract;

b) depășește limitele autorizării;

c) nu are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfășura cercetări științifice sau de a efectua orice altă operațiune într-un sistem informatic.

Relativ la dreptul inculpatei de a accesa şi interoga bazele de date aflate în administrarea sau la dispoziţia angajatorului, se reţine ca prin dispoziţia Inspectorului ####### al Poliţiei ###### nr.81/18.07.2018 privind aprobarea normelor metodologice privind accesul la bazele de date administrate de către D.E.P.A.B.D., care abrogă Dispoziţia IGPR 101/2017, potrivit art.3 din acel act normativ, „operaţiunile cu privire la bazele de date şi prelucrarea datelor cu caracter personal se fac cu respectarea prevederilor legale naţionale şi internaţionale în ceea ce priveşte protecţia datelor cu caracter personal şi libera circulaţie a acestor date. La art.4 se prevede că „interogarea bazelor de date de către poliţişti se efectuaează doar în scopul realizării atribuţiilor de serviciu, dacă sunt îndeplinite condiţiile prevăzute de lege privind legitimitatea prelucrării datelor cu caracter personal".

Interogarea bazelor de date se face fie direct, personal de către lucrătorul de poliţie ce are drept de acces la baza de date, prin utilizarea unui cod de identificare şi a unei parole de acces ori indirect, prin solicitarea informaţiilor de la un lucrător de poliţie care drept de acces direct la bazele de date (art.5).

Potrivit art.6 alin.2, se interzice accesul poliţiştilor la bazele de date prin utilizarea codului de identificare şi a parolei de acces aparţinând altor poliţişti. Potrivit art.16 alin.1, pentru respectarea principiul responsabilităţii, se interzice efectuarea de interogări a bazelor de date administrate de DEPABD la solicitarea personalului aparţinând altor unităţi ce nu fac parte din structura organizatorică a M.A.I. Iar alin.2 preve de că „în situaţia în care o instituţie, o persoană juridică sau fizică adresează o cerere privitor la furnizarea unor date de cu caracter personal din bazele de date administrate de DEPABD, această cerere va fi înaintată spre soluţionare DEPABD, respectiv serviciilor publice comunitare locale de evidenţă a persoanelor."

Consideraţii teoretice, jurisprudenţa, decizii CCR, decizii ICCJ, doctrina.

Pentru a verifica incidenta incriminării la cazul concret, instanta este nevoită să expună câteva consideraţii teoretice cu privire la momentul consumării infracţiunii prev. de art.360 Cod penal, având în vedere că exista o divergentă de opinii intre Ministerul ###### şi inculpat din această perspectivă, după cum există şi pentru ipoteza înţelegerii noţiunii de „exploaterea unui sistem, cu depăşirea limitelor autorizării".

Astfel, instanta apreciază că accesul la un sistem informatic se consumă la momentul autentificării într-o bază de date și obținerea informațiilor existente în acea bază de date, care nu reprezintă decât o accesare a unor date informatice, nu implica un acces separat.

În acest sens, instanta amintește și considerentele Deciziei nr. ##/2021 a înaltei #####-Completul pentru Dezlegarea unor chestiuni de drept, în cuprinsul cărora s-a arătat că accesul fără drept la un sistem informatic, prevăzută de art. 360 alin. (1) din Codul penal, se consumă în momentul realizării elementului material al laturii obiective, respectiv al accesului, când autorul, interacţionând la nivel logic cu sistemul informatic, beneficiază dc resursele ori/și de funcțiile lui și când se produce urmarea imediată constând în lezarea relațiilor sociale privind siguranța/securitatea sistemelor și datelor informatice prin asigurarea confidențialității, integrității și accesibilității acestora.

În cazul accesării unei baze de date, accesul la un sistem informatic are loc la momentul autentificării.

După cum s-a arătat în doctrină, “autentificarea reprezintă procesul prin care un utilizator este identificat în cadrul unui sistem informatic prin nume utilizator, parolă, cod de acces, cod de verificare sau alte asemenea date - denumite ”credențiale de acces” - care probează existența unei accepțiuni formale acordată respectivului utilizator de a interacționa cu sistemul. Pe de altă parte, utilizarea credențialelor de acces presupune mai înainte existența unui "cont de utilizator” cont care se creează în sistem de către un responsabil 1T sau dc către orice altă persoană desemnată, în baza dispoziției unei persoane competente sau apte să dea o astfel de decizie.(...) Odată autentificarea realizată, funcționarul este plasat virtual în spațiul denumit generic ”cont de utilizator”, căruia îi sunt alocate (în baza permisiunilor formale acordate) mai multe operațiuni logice (de comandă și control) asupra sistemului de operare, mijloacelor de stocare ori asupra unuia sau mai multor seturi de date informatice, operațiuni care, la nivelul sistemului informatic, reprezintă execuția unor instrucțiuni de prelucrare de date ”(M. #########. Considerații tehnice și juridice privind reținerea infracțiunii de acces ilegal la un sistem informatic în situația interogării unei baze de date prin depășirea limitelor autorizări. în Pcnalmenle Relevant, nr. 1/2021, p. 74).

Odată accesat sistemul informatic, odată ce autorul, interacționând la nivel logic cu sistemul informatic, beneficiază de resursele ori/și de funcțiile lui, conduita sa ulterioară (care are loc uneori chiar și după câteva ore) de a interoga baza de date, în opinia instanţei si in acord cu apararile formulate de inculpata, excedează normei de incriminare prev. de art. 360 C.pen.

În același sens, s-a arătat că “din punct de vedere procedural, în baza fișei de post și a atribuțiilor funcționale cuprinse în regulamentele, ordinele sau dispozițiile interne ale organizației deținătoare a informațiilor vizate, funcționarul ori persoană anume desemnată poate avea (primi) permisiunea (dreptul) de a interacționa cu una sau mai multe colecții de informații. Aceste colecții de informații în format electronic reprezintă "date informatice" în sensul art. 35 alin. (l) lit. d) din Legea nr. 161/20033, adică "orice reprezentare a unor fapte, informații sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic". Legea mai arată și că "în această categorie se include și orice program informatic care poate determina realizarea unei funcții de către un sistem informatic". Definiția a fost preluată parțial în Noul Cod Penal și o regăsim în cuprinsul art. 181 alin. (2) astfel: "orice reprezentare a unor fapte, informații sau concepte înlr-o formă care poate fi prelucrată printr-un sistem informatic". ##### în vedere că bazele de date se construiesc cu ajutorul unor programe informatice, care reprezintă tot date informatice, rezultă că în situația analizată, acțiunea prezumtivilor făptuitori se îndreaptă doar asupra unor date informatice’ (M. #########. op.cil., p. 71).

În condițiile în care legiuitorul nu a incriminat folosirea fără drept a unui sistem informatic sau accesarea fără drept a datelor informatice, conduita inculpatului nu se circumscrie acțiunii incriminate de art. 360 C.pen.

Bazele de date (colecțiile de informații, evidențele electronice) reprezintă seturi de date informatice care, însă, nu se circumscriu programelor informatice indispensabile existenței și funcționării unui sistem informatic. Drept urmare, o eventuală interacțiune "neautorizată" a unui utilizator cu aceste seturi structurate de dale nu este de natură să atragă, în opinia noastră, din

punct de vedere tehnic și obiectiv, tipicilatea infracțiunii prevăzute la art. 360 C.pen.” (M. #########, op.cât., p. 73).

În acest sens, instanta reaminteşte și considerentele Deciziei nr. ##/2021 a înaltei #####-Completul pentru Dezlegarea unor chestiuni de drept, în cuprinsul cărora s-a arătat că nu are nicio relevanță în ceea ce privește caracterizarea faptei ca infracțiune conduita ulterioară a agentului în raport cu informațiile obținute prin accesarea sistemului informatic, sub aspectul folosirii sau nefolosirii lor ori al scopului în care au fost efectiv utilizate (în cadrul activității de serviciu sau fără legătură cu aceasta), deoarece aceasta intervine după momentul consumării infracțiunii.

În concret, orice acțiune ulterioară (de exemplu, divulgarea unor informații) va fi sancționată doar dacă este incriminată de legiuitor ca o infracțiune de sine stătătoare, de exemplu, favorizarea făptuitorului, compromiterea intereselor justiției sau cum este cazul în speţă de fată, divulgarea informațiilor secrete de serviciu sau nepublice, faptă prev. și ped. de art. 304 alin. 1 C.p.

Contrar opiniei Ministerului ######, în speţa analizată, lipsa autorizării sau depăşirea limitelor autorizării nu vizează accesul, ci folosirea datelor informatice, fiind fără importanță modul sau scopul în care informațiile obținute prin această acțiune au fost utilizate ulterior consumării accesului sau dacă nu au fost folosite în cadrul unei anumite activități, motiv pentru care orice analiză sub acest aspect excedează operațiunii de stabilire a tipicității infracțiunii reglementate de art. 360 alin 1 Codul penal.

Chiar dacă se coroborează dispozițiile art. 360 CP cu dispozițiile art 35 alin. (2) lit. b) din Legea nr. 161/2003, necesită observat faptul că definiția legală a noțiunii „fără drept" reprezintă o normă incompletă, astfel cum a indicat si avocatul inculpatei.

Astfel, teza depășirii limitelor autorizării avută în vedere de către legiuitor la art. 35 alin. (2) lit. b) din Legea nr. 161/2003 trebuie raportată la dispozițiile art. 35 alin. (2) lit. a) din lege, ce fac vorbire despre lipsa unei autorizări legale ori contractuale. Rezultă așadar că teza depășirii limitelor autorizării nu are autonomie, fiind esențială identificarea unor dispoziții legale ori contractuale care au fost încălcate de către inculpata, exclusiv la momentul consumării accesului. Depășirea limitelor autorizării prin raportare la existența unui alt scop decât cel pentru care s-a conferit autorizarea nu este prevăzută de legea penală.

Drept urmare, noțiunea „fără drept” din cuprinsul normei de incriminare trebuie raportat la la existența unei autorizări legale sau contractuale în ceea ce privește accesarea sistemului informatic, nu la exploatarea accesului în alte scopuri.

Practic, a accepta susținerile Parchetului, ar însemna că ori de câte ori un judecător accesează sistemul informatic EMAP pentru a vedea din curiozitate o soluție sau pentru a căuta jurisprudență în interes personal pentru o cauză în care este implicat şi în cuprinsul căreia exista atenţionarea că exploatarea sistemului se realizează numai în interes de serviciu, ar însemna că acesta ar comite infracțiunea de acces la un sistem informatic, deși în mod evident o astfel de faptă nu poate atrage decât o răspundere disciplinară.

După cum arată și considerentele Deciziei nr. ##/2021 a Inaltei #####-Completul pentru Dezlegarea unor chestiuni de drept, existența infracțiunii prev. de art. 360 C.pen. nu poate depinde de conduita ulterioară a autorului, respectiv de scopul în care urmează a fi utilizate informațiile obținute.

De altfel, instanta observa ca toate trimiterile legale expuse de Ministerul ###### în cuprinsul rechizitoriului se referă la confidențialitatea, procesarea și dezvăluirea sau accesarea datelor cu caracter personal. Or, toate aceste aspecte vizează conduite ulterioare autentificării la bazele de date, fiind necesară o interogare a bazelor de date ce nu poate fi subsumată unui acces.

De altfel, chiar în Dispozițiile inspectorului general al Poliției ###### nr. 101/2007 și nr. 81/2018 se face vorbire despre „interogarea bazei de date". De asemenea, se face chiar o distincție între interogarea bazelor de date (art. 4) și accesarea acestora prin utilizarea contului de identificare și a parolei (art. 6). Or, în ceea ce privește accesarea bazelor de date se precizează doar faptul că autentificarea nu se poate realiza prin folosirea parolei de acces aparținând altor polițiști, aceasta din urmă fiind ipoteza în care s-ar pune problema unui acces ilegal la un sistem informatic.

Scopul ilicit reprezintă doar o circumstanță de calificare prin raportare la prevederile art. 360 alin. (2) CP, fără a fi un element constitutiv al formei de bază. Prin urmare, înainte de analiza scopului special, constând în obținerea de date informatice, este necesară identificarea unui acces propriu-zis care să se realizeze fără drept, respectiv cu depășirea limitelor autorizării. Cum ar fi, de exemplu, existenţa unei autorizări de logare într-o parte a unui sistem informatic (partiţia C), urmat de accesarea şi a altei părţi a sistemului informatic (partiţia D), fara a fi existat o autorizare in acest ultim caz.

Conceptual, autorizarea (sau dreptul) are natură juridică a unei cauze justificative. Chiar dacă în ceea ce privește art. 360 CP, acest element a fost inclus în tipicitatea faptei, analiza conceptuală prezintă în continuare importanță deoarece analiza referitoare la existența ori inexistența unei autorizări trebuie analizată în raportul cu elementul material al infracțiunii (accesul), nu cu o conduită ulterioară consumării infracțiunii.

autorizării trebuie așadar să fie în legătură cu un comportament inclus în latura obiectivă a infracțiunii. Or, accesarea datelor informatice prin interogarea unei baze de date excedează sferei de aplicabile a art. 360 CP.

Faptul că lipsa autorizării trebuie raportată în mod exclusiv la acces, fiind exclusă orice conduită ulterioară consumării accesului, rezultă fără echivoc inclusiv din considerentele ICCJ (HPnr. 68/2021) redate anterior.

Relativ la agravanta reţinută în cauza prev. de art.360 alin.3 Cod penal, instanta nu reţine că accesul la sistemul informatic s-a realizat prin depășirea unor măsuri de securitate în primul rând, pentru faptul că fapta nu este tipică în forma ei de bază şi analiza cu privire la tipicitatea unei variante agravate este lipsită de obiect.

Cu toate acestea, analiza art. 360 alin. (3) CP prezintă relevanță în prezența cauză deoarece trimiterea în judecată inclusiv cu privire la această variantă agravată evidențiază din nou confuzia pe care a făcut-o acuzarea între accesarea unui sistem informatic și exploatarea unui acces consumat anterior.

Atât potrivit Deciziei CCR nr. 27/2021 și nr. 183/2018, cât și potrivit HP nr. 68/2021, forma agravată prevăzută la art. 360 alin. (3) CP se poate reține doar atunci când făptuitorul utilizează „mijloace calificate" de acces, apte să depășească ori să eludeze protecția sporită instituită prin măsurile de securitate.

Cu alte cuvinte, nu este suficient ca sistemul informatic să fie unul securizat, fiind necesar ca făptuitorul să depășească, eludeze sau înlăture o măsură de securitate.

Din consideretentele expuse prin Decizia CCR nr. 27/2021, relevante sunt următoarele:” forma agravată a infracțiunii prevăzută de art.360 alin. (3) din Codul penal există atunci când făptuitorul utilizează „mijloace calificate" de acces, apte să depășească ori să eludeze protecția sporită instituită prin măsurile de securitate. S-a reținut că textul de lege criticat nu prevede nicio condiție cu privire la modul concret în care restricția este nesocotită, motiv pentru care își menține actualitatea jurisprudența care, anterior Codului penal, a reținut incidența art.42 alin.(3) din Legea nr.161/2003”.

Curtea a reținut că forma agravată subzistă și atunci când nesocotirea restricției este facilitată de disfuncțiile sau carențele sistemului de protecție, care permit înlăturarea sau ocolirea/eludarea facilă a protecției.

Din consideretentele expuse prin Decizia nr. CCR nr. 183/2018, rezulta că forma agravată a infracțiunii prevăzută de art.360 alin. (3) din Codul penal există atunci când făptuitorul utilizează „mijloace calificate" de acces, apte să depășească ori să eludeze protecția sporită instituită prin măsurile de securitate.

Astfel agravanta prevăzută la alin. (3) sancționează o formă calificată de acces echivalentă efracției - făptuitorul încalcă sau eludează măsurile de securitate în vederea consumării accesului. Or, în mod evident, în prezenţa cauză, accesul a fost consumat anterior efectuării tuturor interogărilor bazelor de date.

De altfel, în alte situații în care s-a dispus trimiterea în judecată a unui polițist pentru interogarea bazelor de date în interes personal, instanta reţine ca încadrarea juridică a fost făcută exclusiv prin raportare la prevederile art. 360 alin. (1) și (2) CP - a se vedea în acest sens C.A. București, secția I penală, decizia nr. ###/A/2023 (depusă la dosarul cauzei).

Prin urmare, în prezenta cauză, nu este incidenta o depășire sau eludare a măsurilor de securitate, deoarece procesul de autentificare s-a consumat anterior interogării bazelor de date. De altfel, autentificarea la bazele de date nu s-a realizat fără drept deoarece inculpata ##### a folosit propriul cont de utilizator și chiar a efectuat interogări ale bazelor de date ce nu au făcut obiectul acuzației în materie penală.

Diferențele la nivel de formă între art. 42 alin. (3) din Legea nr. 161/2003 și art. 360 alin. (3) CP nu ar trebui să se transpună într-o extindere a sferei de aplicabilitate a art. 360 alin. (3) CP. Sub acest aspect, nu se identifica o modificare de substanță a acestei circumstanțe de calificare, îndeosebi raportat la DCCR nr. 27/2021, DCCR nr. 183/2018 și potrivit HP nr. 68/2021. Ambele decizii ale Curții Constituționale au avut în vedere prevederile art. 360 alin. (3) CP, Curtea respingând criticile de neconstituționalitate prin clarificarea modului în care trebuie interpretată această variantă agravată a infracțiunii.

A susține că alin. (3) se reține de fiecare dată când este incident un sistem informatic securizat, fără să prezinte relevanță în ce măsură au fost eludate sau nu măsurile de securitate implementate la nivelul acestuia (adică, identificarea unei forme calificate de acces), ar conduce la imposibilitatea reținerii art. 360 CP în formă de bază. Aceasta întrucât, este aproape imposibil de imaginat un sistem informatic care să nu aibă implementate „din fabrică" diverse măsuri de securitate, independent de activarea sau dezactivarea unor opțiuni suplimentare (e.g. cu privire la setarea unei parole, activarea sistemului de autentifica re în doi pași etc.) de către utilizator.

Continuând spre norma de incriminare în formă de bază, instanta reţine ca fiind relevanta și jurisprudență americană în cauza ### Buren vs. Statele Unite ale Americii, soluționată la data

de 3 iunie 2023 de Curtea Supremă a SUA, cauza în care fostul agent de poliție ###### ### Buren a fost trimis în judecată pentru că a accesat (de la computerul din mașina de patrulare) baza de date a poliției pentru a verifica un număr de înmatriculare al unui vehicul, dar nu pentru îndeplinirea atribuțiilor de serviciu, ci pentru a comunica respectivele informații, contra cost, unei alte persoane (martor denunțător, aflat sub controlul Biroului Federal de Investigații în cadrul unei operațiuni de documentare operativă a presupuselor ilegalități săvârșite de polițist), fiind condamnat într-o primă instanță la 18 luni de închisoare pentru săvârșirea infracțiunii de "acces intenționat la un computer, iara drept sau prin depășirea limitelor autorizării" (cuprinsă în Legea privind fraudele și abuzul asupra sistemelor informatice - din 1986. prin raportare la secțiunea 1030 (a)(2) din Titlul 18 al Codului penal al SUA).

de condițiile și împrejurările concrete de săvârșire a faptei de către fostul polițist, prin raportare la normele penale aplicabile și ținând cont inclusiv de opiniile separate formulate de anumiți judecători în caz, Curtea Supremă a SUA a statuat că o persoană se consideră că depășește limitele de autorizare a accesului la un sistem informatic în situația în care acea persoană realizează un acces legal, permis, dar apoi obține informații aflate în anumite zone ale sistemului informatic - cum ar fi fișiere, foldere sau baze de date - care îi sunt interzise. Curtea a mai arătat că, în calitatea sa de polițist, ### Buren a accesat legal, cu drept, sistemul informatic al poliției și, mai mult, acesta era îndreptățit să prelucreze (inclusiv prin consultare) informațiile despre înmatricularea vehiculelor, nefiind în postura de a încălca legea penală privind accesul neautorizat la un sistem informatic chiar dacă scopul prelucrării datelor din evidențele poliției a fost unul necorespunzător (în afara atribuțiilor de serviciu ale acestuia).

Răspunderea penală

Drept consecinţă, constatând că nu este realizată tipicitatea obiectivă a infracţiunii de acces ilegal la un sistem informatic, prev. de art.360 alin.1,2 şi 3 cod penal, instanţa, în temeiul art.396 alin.5 raportat la art.16 alin.1 lit.b) teza a I-a Cod procedura penală, va pronunţă o soluţie de achitare pentru toate cele 11 infracţiuni prezentate în cuprinsul rechizitoriului şi care vor fi enunţate, separat, prin dispozitivul prezentei hotărâri.

II.2 Infracţiunea de divulgarea informațiilor secrete de serviciu sau nepublice ,prev. de art. 304 alin. 1 C.p, pct. 5, 6 şi 9 din rechizitoriu.

Potrivit art. 304 alin. (1) CP, constituie infracțiune „fapta de a divulga, fără drept, informații secrete de serviciu sau care nu sunt destinate publicității. Potrivit art. 304 alin. (2) CP, divulgarea constituie infracțiune dacă fapta este săvârșită de persoana care ia cunoștință de informațiile secrete de serviciu sau care nu sunt destinate publicității.”

Dat fiind situaţia de fapt reţinută de instanţă, contrar argumentelor prezentate de inculpata, prin avocat, se apreciază că s-a realizat, partial, tipicitatea obiectivă şi subiectiva a infracţiunii din discuţie.

Astfel, în mod cert informațiile ce au făcut obiectul interogării bazelor de date şi dezvăluite de inculpata unor terţi care nu aveau acces la acestea, nu au natura unor secrete de serviciu, având în vedere că nu s-a făcut dovada că au intrat în această categorie potrivit legii speciale, respectiv potrivit Legii nr.182/2002.

Cu toate acestea, instanta constata că informaţiile în cauză nu sunt destinate publicităţii, acestea intrând în categoria informaţiilor cu caracter personal.

În context, nu poate fi reţinută ipoteza apărării, expusa în sensul că faptele din discuţie ar atrage o posibilă răspundere contravenţională în temeiul art. 12 din Legea nr. 190/2018, care prevede că „ constituie contravenție procesarea nelegală a datelor cu caracter personal.”

Potrivit art.4 din Regulamentul ######## prin "prelucrare" se înţelege „orice operaţiune sau set de operaţiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziţie în orice alt mod, alinierea sau combinarea, restricţionarea, ştergerea sau distrugerea.”

Mai departe, „prin operator” se înţelege „persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile şi mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern”.

În fine, prin "persoană împuternicită de operator" se înţelege „persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care prelucrează datele cu caracter personal în numele operatorului”.

Subiectul activ al faptei contravenţionale prev. de art.12 din Legea nr.190/2018 poate fi atât persoana juridică, deţinătorul bazei de date confidenţiale, cât şi persoana fizică, împuternicită de operator, pentru a prelucra datele cu caracter personal.

Cu toate acestea, distincţia dintre cele două fapte este dată de urmarea produsă, fapta contravenţională fiind una de pericol, în timp ce infracţiunea prev.de art.304 Cod penal, este una de rezultat, respectiv în cazul celei din urmă fiind necesar sa se producă o afectare a intereselor unor persoane, de regulă, a persoanelor a căror date personale au fost divulgate.

Or, în cauză, instanta reţine că interesele persoanelor #### ####### ####### (pct.6 rechizitoriu), ####### ####### (pct.9 din rechizitoriu), au fost afectate, astfel cum rezultă din declaraţiile acestora, chiar dacă persoanele vătămate nu s-au constituit părţi civile. Abordarea expusă de inculpat, prin avocat, în sensul că domeniul de incidenta al „intereselor lezate”, ar trebui să se situeze în sfera altor valori sociale decât cele protejate de GDPR, nu poate fi primită de instanţă, având în vedere că norma de incriminare nu expune o atare distincţie. În context, delimitarea dintre răspunderea penală şi răspunderea contravenţională se realizează doar prin raportare la urmarea produsă, astfel cum s-a arătat anterior.

În continuare, în privinţa faptei descrise la pct.5 din rechizitoriu, instanta constata că Parchetul nici măcar nu a făcut dovada că „entităţile” aşa cum sunt denumite prin actul de sesizare, „##### ####, ##### ##### #######, ##### ######## şi ##### ###” sunt persoane care exista in realitate şi, mai mult, că interesele acestora ar fi fost vătămate.

Pe cale de consecinţă, instanta reţine ca pentru faptele descrise la pct.6 şi 9 din rechizitoriu este realizată tipicitatea obiectivă şi subiectiva a infracţiunii prev. de art.304 Cod penal, în timp ce pentru fapta descrisă la pct.5 din rechizitoriu nu este realizată tipicitatea obiectivă a infracţiunii în discuţie, motiv pentru care în această ultimă situaţie, instanţă, în temeiul art.396 alin.6 rap.la art.16 alin.1 lit.b) teza a I-a Cod procedura penală va pronunţă o soluţie de achitare.

În schimb, pentru faptele descrise la pct.6 şi 9 din rechizitoriu, instanţa va reţine ca a intervenit prescripţia răspunderii penale.

Potrivit disp.art.153 alin.1 Cod penal „Prescripţia înlătură răspunderea penală.”

Potrivit disp.art.154 Cod penal,

”(1) Termenele de prescripţie a răspunderii penale sunt:

a) 15 ani, când legea prevede pentru infracţiunea săvârşită pedeapsa detenţiunii pe viaţă sau pedeapsa închisorii mai mare de 20 de ani;

b) 10 ani, când legea prevede pentru infracţiunea săvârşită pedeapsa închisorii mai mare de 10 ani, dar care nu depăşeşte 20 de ani;

c) 8 ani, când legea prevede pentru infracţiunea săvârşită pedeapsa închisorii mai mare de 5 ani, dar care nu depăşeşte 10 ani;

d) 5 ani, când legea prevede pentru infracţiunea săvârşită pedeapsa închisorii mai mare de un an, dar care nu depăşeşte 5 ani;

e) 3 ani, când legea prevede pentru infracţiunea săvârşită pedeapsa închisorii care nu depăşeşte un an sau amendă.

(2) Termenele prevăzute în prezentul articol încep să curgă de la data săvârşirii infracţiunii. În cazul infracţiunilor continue termenul curge de la data încetării acţiunii sau inacţiunii, în cazul infracţiunilor continuate, de la data săvârşirii ultimei acţiuni sau inacţiuni, iar în cazul infracţiunilor de obicei, de la data săvârşirii ultimului act.”

Prin Decizia nr. ### din 26 aprilie 2018 a Curții Constituționale a României, instanța de contencios constituțional a admis excepția de neconstituționalitate referitoare la art. 155 alin. (1) Cod penal, care statua faptul că întreruperea cursului prescripției a răspunderii penale se întrerupe prin orice act procedură în cauză, diferențiindu-se astfel de reglementarea din Vechiul cod penal (art. 123: „Cursul termenului prescripției… se întrerupe prin îndeplinirea oricărui act care, potrivit legii, trebuie comunicat învinuitului sau inculpatului în desfășurarea procesului penal.”). ##### în vedere că deciziile CCR sunt obligatorii și, prin aceasta, textul de lege în cauză își încetează efectele juridice în termen de 45 de zile de la publicarea deciziei în Monitorul Oficial, conform art. 147 alin. (1) din Constituție, legiuitorul a avut la dispoziție acest interval de timp pentru a pune în acord textul de lege cu decizia Curții, fapt care nu s-a întâmplat în cazul de față. Ca urmare, în cvasi majoritatea jurisprudenţei, instanțele au făcut aplicarea deciziei CCR, în discuţie, în mod interpretativ.

Prin Decizia nr. ### din 26 mai 2022 a CCR, s-a statuat că „deși Curtea Constituțională a făcut trimitere la vechea reglementare, evidențiind reperele unui comportament constituțional pe care legiuitorul avea obligația să și-l însușească, aplicând cele statuate de #####, acest fapt nu poate fi interpretat ca o permisiune acordată de către instanța de contencios constituțional organelor judiciare de a stabili ele însele cazurile de întrerupere a prescripției răspunderii penale”, stabilind astfel natura restrictivă a deciziei, și, prin urmare, creându-se un gol legislativ în perioada dintre cele două decizii, chiar dacă de această dată legiuitorul a modificat conținutul art. 155 alin. (1) al Codului penal, prin O.U.G. nr. 71 din 30 mai 2022.

Cu privire la mecanismul de aplicare a legii penale mai favorabile, Curtea Constituţională, sesizată cu excepţia de neconstituţionalitate a dispoziţiilor art. 5 Cod penal a pronunţat Decizia nr. ### din 6 mai 2014, publicată în Monitorul Oficial al României nr. 372 din 20 mai 2014, prin care a statuat aplicarea globală a legii penale mai favorabile.

Determinarea legii penale mai favorabile şi alegerea acesteia dintre legile succesive implică, în prealabil, evaluarea, prin comparare, a dispoziţiilor penale din legi succesive care îşi găsesc aplicarea în cauză, utilizând criteriul aprecierii în concreto.

Pentru a deveni aplicabile dispoziţiile mai favorabile din legile succesive, în afara condiţiei de existenţă a unei situaţii tranzitorii, care a fost anterior constatată în cuprinsul acestor considerente, mai este necesar ca fapta ce face obiectul acuzaţiei să fie infracţiune atât potrivit legii sub imperiul căreia a fost comisă, cât şi conform legii în vigoare la data judecării cauzei, iar dintre legile penale succesive una să fie mai favorabilă.

Unul dintre criteriile prin care se determină în concret legea penală mai favorabilă până la soluționarea definitivă a cauzei este cel al condițiilor de tragere la răspundere penală. Aşa cum s-a reţinut în doctrină, în aplicarea concretă a acestui criteriu, va fi mai favorabilă legea care prevede un termen de prescripție mai scurt sau permite împlinirea mai rapidă a termenului de prescripție (spre exemplu, nu prevede o anumită cauză de întrerupere.

De altfel, prin Decizia nr. ## din 25 octombrie 2022 a Înaltei ##### de Casaţie şi Justiţie pronunţată pe calea dezlegării unor chestiuni de drept în materie penală s-a stabilit că „Normele referitoare la întreruperea cursului prescripţiei sunt norme de drept penal material (substanţial) supuse din perspectiva aplicării lor în timp principiului activităţii legii penale prevăzut de art. 3 din Codul penal, cu excepţia dispoziţiilor mai favorabile, potrivit principiului mitior lex prevăzut de art. 15 alin. (2) din Constituţie şi art. 5 din Codul penal.”

Instanţa opinează că, faţă de considerentele obligatorii ale deciziei nr. ###/2022 a Curţii Constituţionale, decizia nr. ###/2018 este o decizie simplă non-textuală care alterează activitatea substanțială a normei unice pe care textul o conține, în sensul că, până la data modificării prevederilor art. 155 alin. (1) Cod penal prin Ordonanța de urgență a Guvernului nr. 71/2022, respectivul text normativ nu a reglementat un caz de întrerupere a prescripției răspunderii penale, deoarece unica soluție legislativă pe care textul a reglementat-o de la intrarea sa în vigoare la data de 01 februarie 2014 intră sub puterea general obligatorie a declarației de neconstituționalitate exprimate ca atare prin actul de jurisdicție constituțională.

Astfel, până la data de 30 mai 2022, data intrării în vigoare a Ordonanței de urgență a Guvernului nr. 71/2022 [prin care a articolul 155 din Legea nr. 286/2009 privind Codul penal, publicată în Monitorul Oficial al României, Partea I, nr. 510 din 24 iulie 2009, cu modificările şi completările ulterioare, alineatul (1) au fost modificate şi au următorul cuprins: "(1) Cursul termenului prescripţiei răspunderii penale se întrerupe prin îndeplinirea oricărui act de procedură în cauză care, potrivit legii, trebuie comunicat suspectului sau inculpatului."], în materie penală nu a funcționat întreruperea cursului termenelor de prescripție a răspunderii penale, situație juridică care va produce efecte în condițiile legii penale mai favorabile în cauzele pendinte. Ipotezele de întrerupere a cursului prescripției răspunderii penale în condițiile Ordonanței de urgență a Guvernului nr. 71/2022 se vor aplica numai cu privire la faptele comise începând cu data de 30 mai 2022, acestea neputând fi aplicate retroactiv în cauzele pendinte, neavând natura unei legi penale mai favorabile.

Instanţa apreciază că, în aplicarea mitior lex, deciziile nr. 297/2018 şi nr. 358/2018 ale Curţii Constituţionale se aplică tuturor cauzelor penale care erau pendinte în data de 25 iunie 2018 - data publicării în Monitorul Oficial al României a deciziei nr. ###/2018 şi că niciun act efectuat în prezenţa cauză până în data de 25 iunie 2018, nu poate produce efecte întreruptive de

prescripție a răspunderii penale în baza unei prevederi legale care, încă de la intrarea sa în vigoare, a configurat o unică soluţie normativă neconstituţională, sancţionată ca atare prin aceste două decizii ale instanţei de contencios constituţional, aplicabile raporturilor juridice de conflict pendinte.

În speță, instanţă reține că legea penală mai favorabilă în cauză o reprezintă Noul Cod penal în forma în vigoare la data de 25.06.2018, respectiv după publicarea Deciziei Curții Constituționale nr. 297/2018, legislație care nu mai prevedea cazuri de întrerupere a prescripției speciale.

Aplicând aceste norme de drept substanţial la situaţia de fapt reţinută în cauză, instanţa constata că cele două infracţiuni descrise la pct.6 şi 9 din rechizitoriu, s-au consumat la data de 15.11.2018, respectiv 19.10.2018 (în lipsa unor alte date certe), moment de la care începe să curgă termenul de prescripţie generală de 5 ani, calculat în conformitate cu disp.art.154 alin.1 lit.d) Cod penal, prin raportare la limitele de pedeapsa prevăzute pentru infracţiunea în discuţie, respectiv de la 3 luni la 3 ani sau amenda.

######## că legea penală mai favorabilă este Legea nr. 286/2009 privind Codul penal cu referire la intervalul cuprins între publicarea în Monitorul oficial al Deciziei Curţii Constituţionale nr. 297/2018 – şi momentul intrării în vigoare a O.U.G. nr. 71/2022 (perioada 25.06.2018-30.05.2022).

În consecinţă, instanţa constata că a intervenit prescripţia răspunderii penale prin aplicarea dispoziţiilor art.5 Cod penal referitoare la legea mai favorabilă, termenul de prescripţie de 5 ani fiind împlinit la datele de 14.11.2023 şi 18.10.2023.

Drept urmare, în baza art.396 alin.6 rap.la art.16 alin.1 lit.f) Cod procedura penală, cu aplicarea art.154 alin.1 lit.d) Cod penal şi art.5 Cod penal, cu referire la art. 155 alin.1 Cod Penal şi în aplicarea Deciziilor Curţii Constituţionale nr.297/2018 şi nr.358/2022, instanţa va dispune încetarea procesului penala, in raport infracţiunea de divulgarea informațiilor secrete de serviciu sau nepublice, faptă prev. de art. 304 alin. 1 C.p. (pct.6 şi 9 din rechizitoriu).

Cheltuieli judiciare

În baza art.275 alin.6 Cod procedura penală, onorariul parţial al avocatului din oficiu ####### #######, în cuantum de 434 lei, conform delegatiei nr. 4092/03.11.2021, va fi suportat din fondurile Ministerului Justitiei.

În baza art.275 alin.1 pct.1 şi alin.1 pct.2 Cod procedura penală, cheltuielile judiciare rămân în sarcina statului.

PENTRU ACESTE MOTIVE
ÎN NUMELE LEGII
HOTĂRĂŞTE:

În temeiul art.396 alin.5 raportat la art.16 alin.1 lit.b) teza a I-a Cod procedura penală dispune achitarea inculpatei ##### (###) ####### #####, CNP ##############, cetăţean român, cu dom. în sat #######, nr.163, agent de poliţie în cadrul I.P.J. Bihor-###.Mun.######-Biroul de Ordine #######, în raport de infracţiunile:

- acces ilegal la un sistem informatic, prev. de art.360 alin.1,2 şi 3 cod penal (fapta descrisă la pct.1 din rechizitoriu)

- acces ilegal la un sistem informatic, prev. de art.360 alin.1,2 şi 3 cod penal (fapta descrisă la pct.2 din rechizitoriu)

- acces ilegal la un sistem informatic, prev. de art.360 alin.1,2 şi 3 cod penal, (fapta descrisă la pct.3 din rechizitoriu)

- acces ilegal la un sistem informatic, prev. de art.360 alin.1,2 şi 3 cod penal, (fapta descrisă la pct.4 din rechizitoriu)

- acces ilegal la un sistem informatic, prev. de art.360 alin.1,2 şi 3 cod penal, (faptă descrisă la pct.5 din rechizitoriu);

- acces ilegal la un sistem informatic, prev. de art.360 alin.1,2 şi 3 cod penal, (fapta descrisă la pct. 6 din rechizitoriu);

- acces ilegal la un sistem informatic, prev. de art.360 alin.1,2 şi 3 cod penal (faptă descrisă la pct.7 din rechizitoriu)

- acces ilegal la un sistem informatic în formă continuată (două acte materiale), prev. de art.360 alin.1,2 şi 3 cod penal, cu aplic. art.35 c.pen. (faptă descrisă la pct.8 din rechizitoriu),

- acces ilegal la un sistem informatic, prev. de art.360 alin.1,2 şi 3 cod penal (fapta descrisă la pct.9 din rechizitoriu)

- acces ilegal la un sistem informatic, prev. de art.360 alin.1,2 şi 3 cod penal (faptă descrisă la pct.10 din rechizitoriu)

- acces ilegal la un sistem informatic în formă continuată (5 acte materiale), prev. de art.360 alin.1,2 şi 3 cod penal, cu aplic. art.35 c.pen. (fapte descrise la pct.11 din rechizitoriu).

În temeiul art.396 alin.6 rap.la art.16 alin.1 lit.b) teza a I-a Cod procedura penală dispune achitarea inculpatei ##### (###) ####### #####, CNP ##############, cetăţean român, cu dom. în sat #######, nr.163, agent de poliţie în cadrul I.P.J. Bihor-###.Mun.######-Biroul de Ordine #######, în raport de infracţiunea de divulgarea informațiilor secrete de serviciu sau nepublice, faptă prev. de art. 304 alin. 1 C.p. (pct.5 din rechizitoriu).

În temeiul art.396 alin.6 rap.la art.16 alin.1 lit.f) Cod procedura penală, cu aplicarea art.154 alin.1 lit.d) Cod penal şi art.5 Cod penal, cu referire la art. 155 alin.1 Cod Penal şi în aplicarea Deciziilor Curţii Constituţionale nr.297/2018 şi nr.358/2022, dispune încetarea procesului penal fata de inculpata ##### (###) ####### #####, CNP ##############, cetăţean român, cu dom. în sat #######, nr.163, agent de poliţie în cadrul I.P.J. Bihor-###.Mun.######-Biroul de Ordine #######, în raport de infracţiunea de divulgarea informațiilor secrete de serviciu sau nepublice, faptă prev. de art. 304 alin. 1 C.p. (pct.6 şi 9 din rechizitoriu).

În baza art.275 alin.6 Cod procedura penală, onorariul parţial al avocatului din oficiu ####### #######, în cuantum de 434 lei, conform delegatiei nr. 4092/03.11.2021, va fi suportat din fondurile Ministerului Justitiei.

În baza art.275 alin.1 pct.1 şi alin.1 pct.2 Cod procedura penală, cheltuielile judiciare rămân în sarcina statului.

Cu drept de apel în termen de 10 zile de la comunicarea hotărârii.

Pronunţată prin punerea hotărârii redactate la dispoziţia procurorului şi inculpatei, prin intermediul grefei instanţei la data de 17.09.2024.

Preşedinte,
######## #######

Grefier,
####

Red.: Jud. ####/17.09.2024
Tehnored.: ####. ######## / 31.05.2024
4 ex. / 17.09.2024 / 2 #### – inc., P.T.BH.