

ÎNCHEIERE

Ședința din camera de consiliu din data de 13.01.2015
JUDECĂTOR DE CAMERĂ PRELIMINARĂ: Liana Anișoara Cociș
GREFIER: Alina Brie

Pe rol se află examinarea competenței instanței, a legalității sesizării acesteia, a legalității administrării probelor și a efectuării actelor de către organele de urmărire penală în dosarul nr. 126/D/P/2013 al Parchetului de pe lângă Înalta Curte de Casație și Justiție – D.I.I.C.O.T. – Serviciul Teritorial Cluj, în cauza privind pe inculpatul **BORȘ SIMION TOADER**, trimis în judecată prin rechizitoriul nr. 126 D/P/2013 emis de Parchetul de pe lângă Înalta Curte de Casație și Justiție – Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism – Serviciul Teritorial Cluj pentru săvârșirea infracțiunilor de acces ilegal la un sistem informatic, prev. de art. 360 al. 1, 2, 3 din Noul Cod Penal și de operațiuni ilegale cu dispozitive sau programe informatice, în modalitatea deținerii fără drept a unor programe informatice și a unor date informatice și parole, în scopul săvârșirii uneia dintre infracțiunile prev. de art.360 – 364 din Noul Cod Penal, în formă continuată, prev. de art. 365 alin. 2 din Noul Cod Penal, cu aplicarea art. 35 alin. 1 din Noul Cod Penal.

Procedura este legal îndeplinită.

Mersul dezbaterilor și susținerile participanților au fost consemnate în încheierea ședinței camerei de consiliu din data de 17.12.2014 când s-a stabilit că pronunțarea se va face la data de 22.12.2014, când s-a amânat pronunțarea pentru data de 06.01.2015, încheieri ce fac parte integrantă din prezenta hotărâre.

JUDECĂTORUL DE CAMERĂ PRELIMINARĂ,

Prin rechizitoriul Parchetului de pe lângă Înalta Curte de Casație și Justiție – Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism – Serviciul Teritorial Cluj emis la data de 06.10.2014 în dosarul de urmărire penală nr. 126 D/P/2013, și înregistrat la Tribunalul Cluj la data de 06.10.2014 sub nr. unic de dosar 5332/117/2014, a fost trimis în judecată inculpatul **BORȘ SIMION TOADER**, pentru infracțiunile de acces ilegal la un sistem informatic, prev. de art. 360 alin.1, 2 și 3 din Noul Cod Penal și operațiuni ilegale cu dispozitive sau programe informatice, în modalitatea deținerii fără drept a unor programe informatice și a unor date informatice și parole, în scopul săvârșirii uneia dintre infracțiunile prev. de art. 360 – 364 din Noul Cod Penal, în formă continuată, prev. de art. 365 alin.2 din Noul Cod Penal, cu aplicarea art.35 alin.1 din Noul Cod Penal, cu aplicarea art. 38 alin.1 din Noul Cod Penal.

Sub aspectul stării de fapt s-a reținut prin actul de sesizare, în principal, că inculpatul, în data de 21.01.2013, în intervalul orar 11:03 – 13:26, ar fi procedat la accesarea fără drept a sistemului informatic care găzduiește server-ul www.presidency.ro, site-ul oficial al Președinției României, sistem informatic pentru care accesul era restricționat sau interzis pentru anumite categorii de utilizatori, în scopul obținerii de date informatice, de la sistemul său informatic conectat prin intermediul serviciilor de internet la adresa de IP 91.223.82.179, adresă IP atribuită sistemului informatic - server virtual privat –VPS administrat de către inculpat, server-ul virtual privat și adresa IP sus menționate fiindu-i alocate spre administrare inculpatului Borș Simion Toader contra cost de către societatea International Widespread Services, activitatea de accesare fără drept a sistemului informatic care găzduiește server-ul www.presidency.ro, site-ul oficial al Președinției României fiind efectuată de către inculpat prin atacuri informatice de tip SQL Injection care au avut ca sursă adresa IP –ul 91.223.82.179, prin folosirea fără drept a unor aplicații informatice cu ajutorul cărora s-a procedat la ocolirea mecanismului de autentificare necesar unei accesări autorizate și s-a procedat la accesarea neautorizată, în vederea obținerii de date informatice.

De asemenea se mai reține că inculpatul Borș Simion Toader, în perioada 2010 – aprilie 2014, până la intervenția organelor judiciare din data de 15.04.2014, acționând în mod repetat și în baza aceleiași rezoluții infracționale, ar fi procedat la deținerea fără drept, în sistemele sale informatice, într-un suport de stocare a datelor informatice și în adresele sale de e-mail, a următoarelor următoarele categorii de programe informatice, date informatice și parole:

a) programe informatice, deținute fără drept în sistemul său informatic identificat cu seria RC942KKN11112100733, de culoare neagră, având atașat un hard disk extern marca WD, inscripționat „My passport for MAC” și un hard extern de culoare argintiu cu negru marca Storec:

- un program informatic - bothnet de POS (Point Of Sales), care reprezintă un virus informatic care extrage datele stocate despre card-urile bancare de pe sistemul informatic la care este conectat POS-ul, sistem informatic care în prealabil este infestat cu acest virus,

- un program informatic - virus informatic ”Antrax”, care reprezintă un virus informatic care se răspândește prin e-mail și IRC – Internet Relay Chat (comunicare instantanee pe internet), după infestarea calculatorului țintă virusul informatic trimite mesaje instant la toate adresele de email din secțiunea „Adress Book” de pe sistemul informatic infestat,

- un program informatic - virus informatic ”wallet tealer”, care reprezintă un virus informatic utilizat în căutarea și copierea ”portofelelor” de monede virtuale Bitcoin stocate pe sistemul informatic infestat. Infestarea cu acest virus se poate face și prin fișiere care par a fi imagini (fișiere cu extensia JPG), dar care în realitate sunt fișiere tip program (fișiere executabile) care în momentul accesării, infectează calculatorul pe care sunt lansate în execuție,

- un program informatic "Zeus 2.0.8.9", care reprezintă un virus informatic folosit pentru a fura informații bancare de pe sistemele informatice țintă, acest virus informatic răspândindu-se în general prin activități de download,

- un program informatic "SpyEye", care reprezintă un virus informatic ce poate "fura" datele despre conturile bancare respectiv ID-ul și parola pentru accesul la contul bancar online,

- un program informatic "WinJect_1.7", care reprezintă un soft – program informatic, care se folosește în infestarea calculatoarelor țintă cu soft malițios, soft-ul " WinJect_1.7" fiind folosit pentru compromiterea conturilor utilizatorilor care au conturi la jocurile Punkbuster,

programele informatice sus menționate fiind aplicații de tip malware, respectiv programe informatice (software) - rău intenționate, proiectate intenționat pentru deteriorarea unui computer sau pentru infiltrarea în el sau în întregi rețele de calculatoare, fără consimțământul proprietarului respectiv;

- un program informatic "Acunetix Web Vulnerability Scanner", care reprezintă un program informatic folosit pentru identificarea vulnerabilităților sistemelor informatice țintă, în special a site-urilor web găzduite de acestea, vulnerabilități care ulterior pot fi exploatare.

- un program informatic "Sikandar s crypter", care reprezintă un program ce poate fi folosit pentru criptarea virusilor informatici, care în momentul copierii pe diferite calculatoare să nu fie detectați de către programul antivirus instalat.

- un program informatic "CD-konboot", care reprezintă un program folosit pentru evitarea parolelor la pornirea calculatoarelor care au ca sistem de operare Windows și Linux,

- un program informatic "PayPal-checker" care reprezintă un program ce verifică corespondența între user-ul și parola utilizatorilor site-ului PayPal, acest site fiind folosit la plăți online pe internet,

- un program informatic „AkBot”, care reprezintă un program informatic malițios care permite controlul calculatorului infestat, calculator care poate fi folosit ulterior la atacuri de tip DDOS (tip de atac care folosește o rețea de calculatoare compromise, care duc la îndeplinire atacul, din acest motiv neputându-se identifica o singură sursă),

- un program informatic „hellbot” care reprezintă un program informatic malițios care poate șterge fișierele importante de pe calculatorul infestat și poate permite controlul calculatorului infestat, precum și accesul la datele stocate pe calculatorul compromis, respectiv: informații personale și financiare,

- un program informatic „Rxbot”, care reprezintă un program informatic malițios care oferă atacatorului accesul de la distanță, neautorizat, la calculatorul infestat,

- un program informatic „Shellbot”, care reprezintă un program informatic malițios care oferă atacatorului accesul de la distanță, neautorizat la calculatorul infestat și afectează calculatoarele care au instalat sistemul de operare LINUX,

- un program informatic "Ardamax Keylogger" care reprezintă un program informatic, un soft de tip keylogger (program care rulează fără a fi sesizat de către task managerul din sistemul de operare și care înregistrează toate apăsările de taste pe care le execută utilizatorul, informațiile fiind scrise într-un fișier criptat și ulterior trimise către „destinatarul” comenzii), care este folosit pentru a monitoriza activitatea calculatorului infestat, a afla parolele de la adresele de email, ID-urile și parolele la toate conturile care sunt deschise pe calculatorul infestat,

programele informatice descrise mai sus putând fi utilizate pentru comiterea unor infracțiuni informatice de acces ilegal la un sistem informatic, interceptarea ilegală a unei transmisii de date informatice, alterarea integrității datelor informatice, perturbarea funcționării sistemelor informatice, transferul neautorizat de date informatice;

b) următoarele categorii de programe informatice deținute fără drept în sistemul său informatic identificat cu seria 9QG0TTLQ:

- programul executabil „Bandook v1.35.exe” – un program informatic care permite accesul de la distanță la un alt calculator, având caracteristici pentru efectuarea unor operațiuni de captură de ecran, logger apăsare de tastă și manager de proces,

- programul executabil „cp.exe” – un program informatic care monitorizează obiceiurile de navigare ale activității de pe un sistem informatic infestat și distribuie datele înapoi la serverele de autor pentru analiză, putând compromite securitatea computerului utilizatorului și a datelor importante,

programele informatice sus menționate fiind aplicații de tip malware, respectiv programe informatice (software) - rău intenționate, proiectate intenționat pentru deteriorarea unui computer sau pentru infiltrarea în el sau în întregi rețele de computere, fără consimțământul proprietarului respectiv, și putând fi utilizate pentru comiterea unor infracțiuni informatice de acces ilegal la un sistem informatic, transfer neautorizat de date informatice sau alterarea integrității datelor informatice;

c) următoarele categorii de programe informatice și date informatice deținute fără drept în sistemele sale informatice, respectiv: în sistemul informatic hard disk extern marca „ Western Digital”, cu seria WCASN0030932, capacitate 750 Gb, în sistemul informatic „Storex”, carcasă de culoare gri cu negru, cu seria 0710MPIX355GEOST01078, în sistemul informatic hard disk marca Seagate, capacitate 500 GB, având seria 9QG0TTLQ, în sistemul informatic hard disk Western Digital, capacitate 640 GB, cu seria WCASY0730456, în sistemele informatice cu privire la care s-a dispus măsura de acces, respectiv în sistemul informatic cu seria RC942KKN11112100733, de culoare neagră, având atașat în hard disk extern marca WD, inscripționat „ My passport for MAC” și un hard extern de culoare argintiu cu negru marca Storec, dispozitiv extern marca DS213+ cu seria D3L1N09889 cu MAC 0011321E22B9, care are cuplat un hard disk extern WD de culoare neagră, în sistemul informatic – dispozitiv „ Raspberry PI”, conectat la sistemul informatic identificat cu seria RC942KKN11112100733, sistemul

informatic cu adresa IP 91.223.82.79 conectat la sistemul informatic identificat cu seria RC942KKN1112100733, după cum urmează:

- programe informatice reprezentând aplicații care colectează datele de utilizator și numerele card-uri bancare, date informatice care ulterior sunt trimise către alte adrese de email, identificate în fișierele existente într-un număr de 9 structuri de directoare deținute în sistemele informatice utilizate de către inculpatul Borș Simion Toader,

- programe informatice reprezentând aplicații care colectează informațiile de autentificare, codurile de securitate ale utilizatorilor, ip-urile și hostname-uri, care ulterior sunt trimise către alte adrese de e-mail, identificate într-o structură de directoare deținute în sistemele informatice utilizate de către inculpatul Bors Simion Toader,

- programe informatice reprezentând aplicații care colectează informațiile de autentificare și codurile de securitate ale utilizatorilor paginilor de Internet Banking ale unor instituții bancare (43): „Poste Italiene”, „ Banco Posta”, „Barclays”, „Berliner Bank”, „Berliner Sparkasse”, „Raiffeisenbank Sparneck-Stammbranch-Zell”, „BNPPARIBAS”, „Bank of America”, „Cahoot”, „Caixa Activa”, „Caixa Penedes”, „Caixa Sabadell”, „Caja Madrid”, „Caja Madrid”, „Cajamar”, „CapitalOne”, „CCM”, „Citibank”, „Citi”, „Cooperative Bank”, „Lyonnais”, „Deutsche Bank”, „Deutsche Kreditbank”, „Dredner Bank”, „Fineco”, „VR Genossenschaftbank Fulda”, „Halifax”, „Haspa”, „HSBC”, „Lloyds”, „Banca Mediolanum”, „NatWest”, „Postbank”, „Reiffesen Bank”, „SanPaolo Bank”, „Smile”, „Sparda-Bank”, „Sparkasse Regensburg”, „Unicaja”, „Unicredit Banka”, „US Bank”, „Wells Fargo”, „Woolwich”, date care ulterior sunt trimise către alte adrese de e-mail fie sunt scrise în alte fișiere din sistemele informatice utilizate de către inculpatul Borș Simion Toader, identificate într-un număr de 46 structuri de directoare deținute în sistemele informatice utilizate de către inculpatul Borș Simion Toader

- programe informatice reprezentând aplicații care colectează informațiile referitoare la datele de acces ale utilizatorilor paginilor de Internet Banking ale instituțiilor bancare: „Desjardines”, „E-Gold”, „Suncorp”, „Deutsche-Bank”, „CUSwirl”, „Royal Bank Of Canada”, „Citibank”, „Alliance&Leicester”, „BB&T”, „Blue Ball”, „HM Revenue&Customs”, „Lloyds Bank”, „Westpac”, „Allied Irish Bank”, „Regions”, „Cooperative Bank”, „ANZ”, „Bank of Queensland”, „HSBC”, „BirminghamMidshires”, „Santander”, „Scotia Bank”, „St. George”, „Bank of Montreal” și „Netbank”, informații care sunt apoi trimise către alte adrese de e-mail, identificate într-o structură de directoare deținută în sistemele informatice utilizate de către inculpatul Bors Simion Toader.

- date informatice conținând pagini de internet care seamănă/replică cu paginile de internet a unor instituții bancare: "Alliance & Leicester", "El Banco de Valencia", "Caja Navarra", "Cajamar", „Caja Madrid”, „Halifax”, "NatWest", "Banco Posta", "Regions", "Sooper”, identificate într-o structură de directoare deținută în sistemele informatice utilizate de către inculpatul Bors Simion Toader, date informatice folosite pentru crearea paginilor de phishing, în scopul

obținerii datelor bancare ale clienților băncii care accesează paginile de internet modificate.

- date informatice conținând replici ale fișierelor care alcătuiesc pagina de autentificare pe pagina de Internet Banking a unor instituții bancare: "Alliance & Leicester", "Scotiabank", „Banca Generali”, „Banca Intesa”, „Banesto”, „First Usa”, „BBVA”, „Caja Madrid”, date informatice folosite pentru crearea paginilor de phishing, în scopul obținerii datelor bancare ale clienților băncii care accesează paginile de internet modificate, identificate într-un număr de 8 structuri de directoare deținute în sistemele informatice utilizate de către inculpatul Bors Simion Toader,

- date informatice utilizate pentru ca, în momentul în care se încearcă accesarea link-ului de autentificare pe pagina web a instituției bancare „Cajamar”, să fie accesată o altă pagină web, respectiv: <http://darkgamesmovie.com>,

programele și datele sus menționate conținând funcții specifice limbajelor de programare și reprezentând coduri sursă ale unor pagini web, care replică paginile de Internet Banking, ale unor instituții bancare, având drept scop colectarea de informații referitoare la credențialele utilizatorilor și la cardurile bancare ale acestora, rezultând că permit, în urma accesării în mod neautorizat a unor sisteme informatice și a transmiterii neautorizate a datelor informatice obținute, efectuarea unor operațiuni financiare în mod fraudulos, cu consecința prejudicierii utilizatorilor reali.

d) următoarele categorii de date informatice și parole deținute fără drept:

- date informatice și parole aparținând unui număr de 54 utilizatori ai serviciului de transferuri de fonduri „PayPal”, care puteau fi folosite în vederea accesării neautorizate a unor sisteme informatice, respectiv a conturilor Paypal, în vederea obținerii de foloase în urma introducerii în mod neautorizat a datelor informatice aparținând utilizatorilor reali ai conturilor prin folosirea acestor conturi la diverse plăți online, deținute pe suportul său informatic „cd 73”,

- date informatice și parole aparținând unui număr de 101 utilizatori ai serviciului ebay, care puteau fi folosite în vederea accesării neautorizate a unor sisteme informatice în vederea obținerii de foloase în urma introducerii în mod neautorizat a datelor informatice aparținând utilizatorilor reali ai conturilor, date informatice și parole aparținând unui număr de 21 utilizatori, care puteau fi folosite în vederea accesării neautorizate a unor sisteme informatice (adrese de email) ale utilizatorilor, în vederea obținerii de foloase în urma introducerii în mod neautorizat a datelor informatice aparținând utilizatorilor reali ai conturilor, cu consecința prejudicierii acestora, date deținute în sistemele sale informatice cu privire la care s-a dispus măsura de acces, respectiv în sistemul informatic cu seria RC942KKN11112100733, de culoare neagră, având atasat în hard disk extern marca WD, inscripționat „ My passport for MAC” și un hard extern de culoare argintiu cu negru marca Storec, în sistemul informatic – dispozitiv extern marca DS213+ cu seria D3L1N09889 cu MAC 0011321E22B9, având cuplat un hard disk extern WD de culoare neagră, în sistemul informatic – dispozitiv „ Raspberry PI”, conectat la sistemul informatic identificat cu seria

RC942KKN11112100733, în sistemul informatic cu adresa IP 91.223.82.79 conectat la sistemul informatic cu seria RC942KKN11112100733;

- date informatice, respectiv adrese IP, nume utilizatori și parole aparținând unui număr de 37 utilizatori ai unor conturi pe site-ul Ebay, care puteau fi folosite în vederea accesării neautorizate a unor sisteme informatice, obținerii de foloase în urma introducerii în mod neautorizat a datelor informatice aparținând utilizatorilor reali ai conturilor, cu consecința prejudicierii acestora, inclusiv efectuarea de operațiuni financiare în mod fraudulos, deținute în sistemul său informatic hard disk extern marca Storex seria 0710MPiX355GEOST01078,

- date informatice conținând pagini de internet care seamănă cu paginile de internet a băncilor "Bank Of America" și "WellsFrago", aceste pagini de internet putând fi folosite pentru crearea paginilor de phishing, în scopul obținerii datelor bancare ale clienților băncii care accesează paginile de internet modificate, date care puteau fi utilizate pentru comiterea unor infracțiuni informatice de alterare a integrității datelor informatice, deținute în sistemul său informatic cu seria RC942KKN11112100733, de culoare neagră, având atașat un hard disk extern marca WD, inscripționat „ My passport for MAC” și un hard extern de culoare argintiu cu negru marca Storec,

e) următoarele categorii de date informatice deținute fără drept:

- date informatice conținând date ale unui număr de peste 9.000.000 card-uri bancare unice, deținute în sistemul său informatic identificat cu seria RC942KKN11112100733, de culoare neagră, având atașat un hard disk extern marca WD, inscripționat „ My passport for MAC” și un hard extern de culoare argintiu cu negru marca Storec, utilizat de inculpatul Borș Simion Toader,

- date informatice conținând date ale unui număr de 3.137 de card-uri bancare unice, deținute în adresa sa de e-mail

- date informatice conținând date ale unui număr de 119 de card-uri bancare unice, deținute în adresa sa de e-mail

- date informatice conținând date ale unui număr de 563 de card-uri bancare unice, deținute în adresa sa de e-mail

- date informatice conținând date ale unui număr de 54.622 de card-uri bancare unice, deținute în adresa sa de e-mail

- date informatice conținând date ale unui număr de 7756 de card-uri bancare unice, denumite „track data”, deținute în adresa sa de e-mail

datele informatice sus menționate, putând fi utilizate pentru accesarea în mod neautorizat a contului bancar al titularului de card – datele de identificare ale contului regăsindu-se în sistemele informatice ale băncii), iar ulterior efectuarea unei operațiuni financiare frauduloase, cardul bancar al titularului fiind compromis de la momentul când datele de identificare sunt deținute în mod ilegal,

programele informatice, datele informatice și parolele descrise mai sus, prin conținutul și scopul folosirii lor, îndeplinind aptitudinea funcțională de a fi

folosite în vederea săvârșirii uneia dintre infracțiunile informatice prev. de art. 360-364 CP.

Situația de fapt reținută în actul de sesizare a instanței are la bază următoarele mijloace de probă, structurate într-un număr de 35 de volume, după cum urmează:

VOLUMUL 1:

- adresa nr. 93080 din 25.06.2013 emisa de Serviciul de Telecomunicații Speciale si CD (f. 8-9)
- proces-verbal de investigații din data de 01.06.2013 (f.10)
- adresa nr.93390 din 03.07.2013 emisa de Serviciul de Telecomunicații Speciale si CD (f.12-13)
- proces-verbal de investigații din data de 17.07.2013 si anexa (f.14, 15-16)
- proces-verbal de verificare din data de 17.07.2013 (f.197)
- încheierea penala nr.187/18.07.2013 a Judecătoriei Cluj-Napoca (f.202-207)
- adresa nr.2718 din 26.07.2013 emisa de RDS&RCS (f.212)
- proces-verbal de analizare date din 07.03.2014 (f.213-214)
- proces-verbal de verificări din 26.03.2014 (f.215)
- proces-verbal de identificare din 26.02.2014 (f.216-217)
- procese-verbale de verificări pe internet din 26.02.2014 (f.218-220, 221-222)
- procese-verbale de verificări din 27.02.2014 si anexe (f.223, 224, 225-228)
- adresa nr.21941/27.02.2014 emisa de ITM Cluj si anexa (f.231,232)
- adresa si cerere de emitere mandate de supraveghere tehnica din 28.02.2014 (f.233, 234-240)
- încheierea penala nr.35/C/P/28.02.2014 a Judecătorului de drepturi si libertăți din cadrul Tribunalului Cluj si mandatele de supraveghere tehnica nr.48/UP/2014 si nr.49/UP/2014 (f.241-247)
- proces-verbal de constatare din 13.03.2014 (f.253)
- procese-verbale de redare a comunicărilor purtate de inculpat (f.259-263)
- proces-verbal de redare a unor imagini din 26.03.2014 (f.264-265)
- minuta și încheierea penala nr.67/C/P/27.03.2014 a Judecătorului de drepturi si libertăți din cadrul Tribunalului Cluj (f.280-288)
- încheierea penala nr.53/C/P/13.03.2014 a Judecătorului de drepturi si libertăți din cadrul Tribunalului Cluj si mandate de supraveghere tehnica nr.69/UP/2014, nr.70/UP/2014, nr.71/UP/2014 (f.302-310)
- proces-verbal de redare a comunicărilor prin e-mail purtate de inculpat (f.317-319)
- adresa către Banca Transilvania si răspunsul aferent (f.320, 321-343)
- cerere comunicare date din 04.07.2014 (f.344-356)
- încheierea penala nr.192/C/P/04.07.2014 a Judecătorului de drepturi si libertăți din cadrul Tribunalului Cluj (f.357-362)

- adrese comunicare date din 09.07.2014 (f.363-373, 376-386)
- adresa nr.1653 din 06.08.2014 emisă de ING și anexă (f.374-375)
- adresa nr.3298 din 15.07.2014 emisă de OTP Bank și anexe (f.387-394)
- procese-verbale din 30.09.2014 și 01.10.2014 privind efectuarea unor copii după sistemele informatice și suportii optici originali, reprezentând rezultatul măsurilor de supraveghere tehnică dispuse în cauză (f. 406, 423)
- procese-verbale de verificare din data de 29.09.2014 și 30.09.2014 (f.407-409, 410-411, 412-413, 414-415, 424-425)
- procese-verbale de predare grefă din 30.09.2014 și 01.10.2014 (f.416-417, 418-419, 420-421, 422, 426-427);

VOLUMUL 2:

- încheierea penală nr.40/C/P/05.03.2014 a Judecătorului de drepturi și libertăți din cadrul Tribunalului Cluj (f.10-15)
- adresa și ordonanța din 05.03.2014 privind comunicare date autorizate prin încheierea penală către Banca Transilvania (f.19, 20-22)
- adresa nr. 54899 din 05.03.2014 emisă de Banca Transilvania privind comunicare date și anexe (f.23-58, 60-70)
- proces-verbal din data de 10.03.2014 privind analiza datelor transmise de Banca Transilvania și anexe (f.71-72, 73-79)
- proces-verbal din data de 11.03.2014 privind analiza datelor transmise de Banca Transilvania și anexe (f.80-81, 82-110)
- adresa și ordonanța din 05.03.2014 privind comunicare date autorizate prin încheierea penală către BRD (f.111, 112-114)
- adresa nr.636 din 12.03.2014 emisă de BRD privind comunicare date și anexe (f.115-132)
- proces-verbal din data de 19.03.2014 privind analiza datelor transmise de BRD și anexe (f.133-135)
- adresa și ordonanța din 05.03.2014 privind comunicare date autorizate prin încheierea penală către ANAF (f.136, 137-138, 139)
- adresa nr. 504/IX/1/2014 din 31.03.2014 emisă de ANAF privind comunicare date și anexe (f.140-143)
- adresa și ordonanța din 05.03.2014 privind comunicare date autorizate prin încheierea penală către Western Union (f.144, 145-147)
- adresa din 10.03.2014 emisă de Western Union privind comunicare date și CD (f.148,149)
- cerere privind autorizare comunicare date din 14.04.2014 (f.150-181)
- minuta și încheierea penală nr.90/C/P/14.04.2014 a Judecătorului de drepturi și libertăți din cadrul Tribunalului Cluj (f.182-197, 198)
- adresa din 26.05.2014 emisă de Western Union privind comunicare date și CD (f.205,206)
- adresa și ordonanța din 14.04.2014 privind comunicare date autorizate prin încheierea penală de către Primăria Cluj (f.207-209, 210)
- adresa nr.134788/88/49 din 15.04.2014 emisă de Primăria Cluj privind comunicare date (f.211)

- adresa nr.34714 din 28.04.2014 emisă de ANAF privind comunicare date și anexe (f.216-224)
- proces-verbal de constatare din 15.04.2014 întocmit de către specialist și anexe (f.239-249)
- procese-verbale de investigații din 04.03.2014 (f.250-251, 252-253, 254, 255-256)
- proces-verbal de analiză date din 07.03.2014 și anexe (f.257-2601)
- proces-verbal de investigații din data de 11.03.2014 (f.261-262)
- proces-verbal de investigații din data de 12.03.2014 (f.263-264)
- procese-verbale de analiză date din 03.04.2014 (f.265, 266-267)
- procese-verbale de verificări din 09.04.2014 (f.268, 269)
- procese-verbale de investigații din data de 09.04.2014 (f.270, 271)
- proces-verbal de analiză date din 10.04.2014 și anexa (f.272-273, 274)
- proces-verbal de analiză date din 13.05.2014 și anexa (f.275, 276-277)
- raport de analiză întocmit de B.C.C.O Cluj din 15.04.2014, CD și hartă relațională (f.281-284, 285, 286)
- proces-verbal din data de 30.09.2014 privind analiză date Western Union (f.287-291);
- VOLUMUL 3:
- încheierea penală nr.39/C/P/05.03.2014 a Judecătorului de drepturi și libertăți din cadrul Tribunalului Cluj (f.9-12)
- adresa și ordonanța din 05.03.2014 privind comunicare date autorizate prin încheierea penală de către RCS&RDS (f.13, 14-18)
- adrese către RCS&RDS (f.19, 20-21,22,)
- adresa nr.1149 din 11.03.2014 și nr. 2315/23.05.2014 emise de RCS&RDS privind comunicare date și anexe (f.23-24, 25-42, 43-44)
- adresa și ordonanța din 13.03.2014 privind comunicare date autorizate prin încheierea penală de către RCS&RDS (f.45, 46-48)
- minuta și încheierea penală nr.91/C/P/14.04.2014 a Judecătorului de drepturi și libertăți din cadrul Tribunalului Cluj (f.75-88)
- adresă către B.C.C.O București (f.105)
- adresa din 07.08.2014 emisă de B.C.C.O București și CD (f.106, 107)
- proces-verbal de copiere date din 12.08.2014 (f.108)
- adrese către Oficiul Național de Prevenire și Combatere a Spălării Banilor București (f.124-125, 126-127)
- adresa nr. C/XIV/1088 din 09.07.2014 emis de Oficiul Național de Prevenire și Combatere a Spălării Banilor București și CD (f.128-133, 134)
- adrese și ordonanța de instituire a măsurii asiguratorii din 16.04.2014 (f.135, 136-148, 151,153, 156)
- adresa nr.56101 din 18.04.2014 emisă de BRD (f.152)
- adresa nr.99481 din 17.04.2014 emisă de BRD (f.154)
- proces-verbal predare grefă din 09.05.2014 (f.155)
- adresa emisă de BCCO Cluj din 17.04.2014 (f.157)
- proces-verbal din 16.04.2014 privind depunerea banilor confiscați în bancă și recipisele de consemnare (f.158-159, 159-175)

- procese-verbale de sechestrul din data de 10.03.2014 (f.176-178, 184-186)
- proces-verbal de predare grea din 01.07.2014 (f.179)
- proces-verbal de aplicare a măsurii asiguratorii a sechestrului din 18.04.2014 (f.180-182)
 - copie carte de identificare a autoturismului (f.183)
 - adrese de la Tribunalul Cluj (f.187, 188, 190)
 - adresă către Tribunalul Cluj (f.189)
 - încheierea penală nr.96/JDL/30.04.2014 (f.191)
- procese-verbale de analiza datelor din 26.03.2014 și anexe (f.192, 193-199, 200, 201-213)
 - proces-verbal de analiza datelor din 09.04.2014 și anexa (f.214, 215)
 - procese-verbale de verificări din 03.07.2014 (f.216, 217, 218-225)
 - adresă către Ambasada SUA din 08.05.2014 (f.226-234)
 - adresă către D.I.I.C.O.T.- Structura Centrală și răspunsul aferent (f.235-236, 237)
 - adresă către ANCPI anexe și răspunsul aferent (f.238-239, 240-249)
 - adrese emise de BCCO Cluj (f.250, 253-269)
 - adresa către Banca Transilvania și răspunsul aferent (f.251, 252)
 - adrese de la BRD, BCR, ING, GarantiBank, Citi, Unicredit Tiriace Bank (f. 270-274, 280, 281)
 - adresă către ORDA și răspunsul aferent (f.275-277, 278-279)
 - adresă emisă de BCCO București din 08.09.2014 (f.282)
 - proces-verbal de analiză site-uri din 28.09.2014 și anexa (f.283-285)
 - adresă DCCO răspuns Ambasada SUA și suport optic (f. 286-287)
 - proces-verbal analiză date 30.09.2014 (f. 288-289);
- VOLUMUL 4:
 - mandat de percheziție domiciliară nr.35 din 14.04.2014 (f.341-342)
 - minuta încheierii penale nr.88/C/P/14.04.2014 a Judecătorului de drepturi și libertăți din cadrul Tribunalului Cluj (f.34)
 - proces-verbal de punere în executare a mandatului de aducere din data de 16.04.2014 (f.43)
 - proces-verbal de percheziție domiciliară din data de 15.04.2014 (f.44-77)
 - procese-verbale de efectuare a activităților premergătoare a percheziției domiciliare din data de 15.04.2014 (f.82-84)
 - procese-verbale privind accesul în sisteme informatice din data de 16.04.2014 (f.112,113)
 - minuta și încheierea penală nr.103/C/P/18.04.2014 a Judecătorului de drepturi și libertăți din cadrul Tribunalului Cluj (f.139-152)
 - procese-verbale privind accesul în sistem informatic din data de 23.04.2014 și 28.04.2014 (f.157-158, 159)
 - proces-verbal de analiză parțială a datelor din sistemul informatic și CD din data de 04.06.2014 (f.161-163)

- procese-verbale privind accesul în sistem informatic din data de 01.08.2014, 09.05.2014, 07.05.2014, 02.06.2014, 06.06.2014 (f.164, 166-167, 169, 170-179, 180-181)

- proces-verbal privind analiză date carduri din data de 10.07.2014 și CD (f.182-184)

- proces-verbal din data de 10.07.2014 privind imprimarea pe hârtie a unor numere de carduri deținute de inculpat în sistemele sale informatice (f.185-417)

- mandat de percheziție domiciliară (f. 418-419)

- adresă Tribunalul Cluj (f. 420-421);

VOLUMUL 5:

- încheierea penală nr.104/C/P/18.04.2014 a Judecătorului de drepturi și libertăți din cadrul Tribunalului Cluj (f.23-41)

- adresa și cerere privind efectuarea unei percheziții informatice din 03.06.2014 (f.63, 64-91)

- minuta și încheierea penală nr.161/C/P/03.06.2014 a Judecătorului de drepturi și libertăți din cadrul Tribunalului Cluj (f.92-109, 113-114)

- mandat de percheziție informatică nr.62/C/P/2014 din 03.06.2014 (f.110-112, 115-117)

- ordonanța din 03.06.2014 privind efectuare copii sisteme informatice (f.121-126)

- proces-verbal de efectuare a percheziției informatice din 13.05.2014 (f.132-136)

- proces-verbal de copiere sistem informatic din 14.05.2014 (f.139-147)

- procese-verbale de copiere și sigilare din 13.05.2014, 14.05.2014, 15.05.2014, 16.05.2014, 17.05.2014, 19.05.2014, 20.05.2014, 05.06.2014, 06.06.2014, 10.06.2014, 11.06.2014, 12.06.2014, 13.06.2014, 16.06.2014, 17.06.2014, 18.06.2014, 19.06.2014, 20.06.2014, 24.06.2014, 25.06.2014, 26.06.2014, 27.06.2014, 01.07.2014, 02.07.2014, 03.07.2014, 04.07.2014 (f. 137, 138, 148, 149, 157, 158, 159, 160, 161, 162, 163, 176, 177, 180,181, 189, 190, 191, 205, 207, 223, 224, 225, 235,236, 237, 238, 239, 240, 241, 242, 243, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 294, 295)

- proces-verbal de efectuare a percheziției informatice din 16.05.2014 (f.150-156)

- proces-verbal de copiere sisteme informatice din 19.05.2014 (f.164-174)

- proces-verbal de constatare din 20.05.2014 (f.178-179)

- proces-verbal de efectuare a percheziției informatice din 22.05.2014 (f.182-186)

- proces-verbal de constatare din 23.05.2014 (f.187-188)

- procese-verbale de copiere sistem informatic și efectuare percheziții informatice din 05.06.2014, 10.06.2014, 12.06.2014, 16.06.2014, 23.06.2014, 24.06.2014 (f.192-197 198-203, 209-222, 226-234, 244-250, 251-262,)

- proces-verbal de percheziție informatică din 25.06.2014 (f.273-279),

- proces-verbal de copiere sistem informatic din 02.07.2014 (f.280-284)

- proces-verbal de percheziție informatică din 03.07.2014 (f.285-293), cu precizarea că rezultatele perchezițiilor informatice au fost stocate pe un număr de 2 (două) hard disk-uri, unul marca Verbatim – seria 530293423502221 și unul marca Seagate, seria NA498BK7, acestea urmând a fi înaintate instanței de judecată împreună cu prezentul act de sesizare,

- proces-verbal de constatare din 10.07.2014 (f.296-297)
- proces-verbal de analiza a sistemului informatic din 29.07.2014 (f.298-299)

- adrese către INC București (f.300-301, 310)
- notă de constatare din 28.05.2014 (f.309, 318, 319)
- adresa și raportul de constatare criminalistică nr.63483 din 02.06.2014 (f.320-332)

- adresa și raportul de constatare tehnico-științifică din 28.08.2014 și CD (f.347-355)

- procese-verbale de analiza datelor din 30.07.2014 (f.356-392, 393-401, 402-409, 410-418)

- proces-verbal de analiza datelor din 14.07.2014 (f.419-430)
- proces-verbal de analiza datelor din 01.08.2014 și CD (f.356-392, 431-439, 440)

- proces-verbal de analiza datelor din 11.08.2014 (f.441-442)
- proces-verbal de analiza datelor din 12.08.2014 (f.443-450)
- procese-verbale de analiza datelor din 22.08.2014, anexa și CD (f.451-463, 464-469)

- proces-verbal de analiza datelor din 23.08.2014 (f.470-490)
- procese-verbale de analiza datelor din 29.08.2014, anexa și CD (f.494-518, 519-520, 558-561)

- procese-verbale de analiza datelor din 30.08.2014 și anexe (f.519-520, 521-557)

- proces-verbal analiză date carduri și un suport optic (f. 558-561)

- proces-verbal termeni informatici (f. 562-566);

VOLUMUL 6:

- procese-verbale de verificare și constatare din 01.07.2013, 02.07.2013, 26.07.2013, 22.07.2013 (f.1-4, 16)

- Încheierea penală nr. 182 din 03.07.2013 a Judecătoriei Cluj-Napoca (f.8)

- adrese către SC Telemobil Romania (f.12-15, 28-30)

- adresele nr.187/23.07.2013, nr.189/31.07.2013, 191/02.08.2013 și 192/07.08.2013, nr.197/09.08.2014, nr.202/17.09.2014 emise de Telemobil și CD (f.17, 31, 32-34, 36, 37, 41, 43,44, 46)

- Încheierea penală nr.197 din 29.07.2013 a Judecătoriei Cluj-Napoca (f.22-24)

- proces-verbal din 23.09.2013 de analiza a răspunsurilor primite de la SC Telemobil Romania (f.47-51)

- proces-verbal de analiza a datelor in sistemele informatice din 20.08.2014 și CD (f.52-58)

- procese-verbale de desigilare plicuri din data de 14.05.2014, 13.05.2014 (f.59, 61)
 - proces-verbal de efectuare a percheziției corporale din 16.04.2014 (f.60)
 - proces-verbal de efectuare copii xerox după înscrisurile ridicate cu ocazia percheziției domiciliare din 19.05.2014 și 24.09.2014 (f.62-63, 64-70, 190)
 - înscrisurile ridicate cu ocazia percheziției domiciliare (f.71-76, 82-94, 104-127, 130-150, 155-189)
 - proces-verbal de analiza chitanțe din 19.05.2014 (f.77-78)
 - plic conținând chitanțe retrageri ATM-uri (f.79)
 - procese-verbale de identificare înscrisuri din 19.05.2014, 21.05.2014 (f.80-81, 102-103, 128-129, 151-154)
 - proces-verbal de identificare bonuri fiscale din 19.05.2014 (f.95)
 - bonuri fiscale schimb valutar, plic (f.96-101)
 - proces-verbal analiza înscrisuri (f. 102-103)
 - înscrisuri ridicate de la percheziția domiciliară și plic (f. 104-189)
 - proces-verbal efectuare copii(f. 190)
 - proces-verbal de predare grefă (f. 191);
- VOLUMUL 7:
- Încheierea penală nr.89/C/17.04.2014, dosar nr. 2411/117/2014 al Tribunalului Cluj – Secția penală, privind arestarea preventivă a inculpatului Borș Simion Toader pentru o perioadă de 30 de zile (f. 57-79)
 - adresa și Încheierea penală nr.106/JDL/13.05.2014, dosar nr. 2770/117/2014 al Tribunalului Cluj – Secția penală, prin care s-a dispus prelungirea duratei arestării preventive a inculpatului Borș Simion Toader (f. 140, 141-157)
 - Încheierea penală nr.134/JDL/12.06.2014, dosar nr. 3386/117/2014 al Tribunalului Cluj – Secția penală, s-a dispus prelungirea duratei arestării preventive a inculpatului Borș Simion Toader pentru o perioadă de 30 de zile (f. 234-250)
 - Încheierea penală nr.173/JDL/14.07.2014, dosar nr. 3971/117/2014 al Tribunalului Cluj – Secția penală, s-a dispus prelungirea duratei arestării preventive a inculpatului Borș Simion Toader pentru o perioadă de 30 de (f. 332-352)
 - Încheierea penală nr.104/17.07.2014 a Curții de Apel Cluj, (f. 353-369)
 - Încheierea penală nr. 200/C/06.08.2014, dosar nr. 4377/117/2014 al Tribunalului Cluj – Secția penală, s-a dispus prelungirea duratei arestării preventive a inculpatului Borș Simion Toader pentru o perioadă de 30 de zile (f. 463-502)
 - adresă către Tribunalul Cluj din 01.09.2014 (f.503)
 - adresa, minuta și Încheierea penală nr. 218/04.09.2014 a Curții de Apel Cluj (f. 504-508)
 - adresa, minuta și Încheierea penală nr. 224/JDL/10.09.2014, dosar nr. 4912/117/2014 al Tribunalului Cluj – Secția penală, s-a dispus prelungirea

duratei arestării preventive a inculpatului Borș Simion Toader pentru o perioadă de 30 de zile (f. 611-651)

- minuta Încheierii penale nr.137/22.09.2014 a Curții de Apel Cluj, (f. 652)

- adrese Tribunalul Cluj (f. 351-353)

- comunicare și minuta încheierii penale nr. 275/C/02.10.2014 a Tribunalului Cluj (f. 354-355);

VOLUMUL 8:

- minuta și Încheierea penală nr. 89/C/14.04.2014, ale Tribunalului Cluj – Secția penală (f. 12-19)

- proces-verbal de executare a mandatului de aducere din 16.04.2014 (f.20)

- fișa de cazier judiciar (f.32-33, 202)

- declarațiile în calitate de suspect și inculpat ale lui Borș Simion Toader (f.34-41, 83-93, 97-122, 135-147, 166-173)

- cereri formulate de inculpat prin apărătorii aleși (f.150, 229-230, 247-248, 259, 261-263, 276-294, 296-297, 300, 302-303, 314-315, 336, 337-339, 342)

- declarația suspectei Uifălean Alexandra (f.203-207)

- declarația martorului Uifălean Bogdan Vasile (f.224-228)

- adresa nr. 1156/II/7/2014 din 22.08.2014 emisă de D.I.I.C.O.T. – Biroul Teritorial Bistrița Năsăud (f.299)

- adresa din 26.09.2014 privind comunicarea unei copii de pe declarația inculpatului (f.318)

- solicitare depunere suporturi optice (f. 336)

- solicitare inculpat din data de 26.09.2014 (f. 337-338)

- solicitări apărător ales (f. 339-340)

- adresa din 29.09.2014 privind restituirea de CD-uri (f.341)

- solicitare apărător ales (f. 342)

- proces-verbal consultare dosar (f. 343-344)

- procese-verbale consultare dosar (f. 354, 355, 356-357)

- cerere formulată de inculpat prin apărătorii săi aleși din 03.10.2014 (f.373-375)

- proces-verbal consultare dosar (f. 376-377)

- proces-verbal verificări (f. 378);

VOLUMUL 9:

- proces-verbal din 11.04.2014 de identificare numere carduri din adresele de e-mail aparținând inculpatului Borș Simion Toader precum și anexa reprezentând un număr de 448 file (f.1-449);

VOLUMUL 10:

- proces-verbal din 26.03.2014 privind redarea conversațiilor purtate de inculpat pe adresele sale de e-mail în limba engleză și traduceriile acestora în limba româna (f.1-660);

VOLUMUL 11:

- proces-verbal din 28.03.2014 privind redarea conversațiilor purtate de inculpat pe adresele sale de e-mail în limba engleză și în limba română (f.1-255)

- proces-verbal din 01.04.2014 privind redarea conversațiilor purtate de inculpat pe adresele sale de e-mail în limba engleză și în limba română (f.256-421);

VOLUMUL 12:

- proces-verbal din 26.04.2014 de identificare IP-uri aparținând inculpatului Borș Simion Toader, corespondența purtată de acesta, precum și anexa reprezentând două e-mail-uri identificate (f.1-390)

- proces-verbal de redare a convorbirilor purtate de inculpat din 29.09.2014 (f.391-392)

- proces-verbal date VPS (Virtual Private Server) din 30.09.2014 (f.393)

- proces-verbal descriere site Warez-host din 02.10.2014 (f. 294-295)

- proces-verbal identificare fragmente care conțin cuvântul „alex asimov” (f. 296-298);

VOLUMUL 13:

- procese-verbale de redare a convorbirilor și comunicărilor purtate de inculpat prin intermediul adreselor de e-mail în limba engleză și traducerea în limba română a acestora (f.1-327);

VOLUMUL 14:

- procese-verbale din 03.04.2014 de analiza datelor de pe suportul optic tip DVS marca COPYME (f.1-150, 258-260, 261-301, 302-348)

- proces-verbal de redare a convorbirilor purtate de inculpat (f.151-257);

VOLUMUL 15:

- procese-verbale de redare a convorbirilor purtate de inculpat de pe adresele sale de e-mail în limba engleză și traducerea acestora în limba română (copie) (f.1-496);

VOLUMUL 16:

- procese-verbale de redare a convorbirilor purtate de inculpat de pe adresele sale de e-mail în limba engleză și traducerea acestora în limba română (copie) (f.1-335);

VOLUMUL 17:

- proces-verbal din 03.04.2014 privind identificarea de numere de carduri existente în adresele de e-mail ale inculpatului (f.1-212)

- proces-verbal din 09.04.2014 privind identificarea de numere de carduri existente în adresele de e-mail ale inculpatului (f.213-224)

- proces-verbal din 09.04.2014 privind identificarea de numere de carduri existente în adresele de e-mail ale inculpatului (f.225-341);

VOLUMUL 18:

- procese-verbale de redare a convorbirilor purtate de inculpat de pe adresele sale de e-mail în limba engleză și traducerea acestora în limba română (copie) (f.1-436);

VOLUMUL 19:

- Încheierea penală nr.194/C/P/04.07.2014 a Judecătorului de Drepturi și Libertăți din cadrul Tribunalului Cluj (f.29-51);

VOLUMUL 20:

- proces-verbal din data de 18.04.2014 privind copiere sistem informatic (f.1-2)

- proces-verbal privind analiza date informatice (f.4)

- date de carduri bancare (f.4-464);

VOLUMUL 21:

- continuare date de carduri bancare de la volumul 20 (f.4-459);

VOLUMUL 22:

- continuare date de carduri bancare de la volumul 21 (f.1-531);

VOLUMUL 23

- continuare date de carduri bancare de la volumul 22 (f.1-515);

VOLUMUL 24:

- adrese către AMERICAN EXPRESS (f.1-2, 3, 5-6, 9, 34-35)

- proces-verbal de analiza date informatice din 29.07.2014 (f.4)

- adrese de la American Express (f.7-8, 10-11,36-37)

- anexa 1, American Express – lista tranzacții frauduloase (f.12-33)

- anexa 1, American Express – lista tranzacții frauduloase (f.38-597);

VOLUMUL 25:

- anexa 1, American Express – lista tranzacții frauduloase, continuare de la volumul 24 (f.1-539);

VOLUMUL 26:

- anexa 1, American Express – lista tranzacții frauduloase, continuare de la volumul 25(f.1-630);

VOLUMUL 27:

- anexa 1, American Express – lista tranzacții frauduloase, continuare de la volumul 26 (f.1-675);

VOLUMUL 28:

- anexa 2, American Express – lista tranzacții frauduloase, continuare de la volumul 27 (f.1-450);

VOLUMUL 29:

- anexa 2, American Express – lista tranzacții frauduloase, continuare de la volumul 28 (f.1-451);

VOLUMUL 30:

- anexa 2, American Express – lista tranzacții frauduloase, continuare de la volumul 29 (f.1-452);

VOLUMUL 31:

- anexa 2, American Express – lista tranzacții frauduloase, continuare de la volumul 30 (f.1-540);

VOLUMUL 32:

- anexa 2, American Express – lista tranzacții frauduloase, continuare de la volumul 31 (f.1-538);

VOLUMUL 33:

- anexa 2, American Express – lista tranzacții frauduloase, continuare de la volumul 32 (f.1-450);

VOLUMUL 34:

- anexa 2, American Express – lista tranzacții frauduloase, continuare de la volumul 33 (f.1-451);

VOLUMUL 35:

- anexa 2, American Express – lista tranzacții frauduloase, continuare de la volumul 34 (f.1-416).

Potrivit art. 342 Cod de Procedură Penală obiectul procedurii în cameră preliminară îl constituie verificarea, după trimiterea în judecată, a competenței și a legalității sesizării instanței, precum și verificarea legalității administrării probelor și a efectuării actelor de către organele de urmărire penală.

În cadrul acestei etape se verifică, așadar, legalitatea sesizării instanței, competența acesteia, legalitatea administrării probelor și a efectuării actelor de urmărire penală.

În cadrul procedurii camerei preliminare, inculpatul, prin apărătorul său și în termenul prevăzut de art. 344 alin.2 Cod de Procedură Penală, a depus o serie excepții și cereri cu privire la legalitatea sesizării instanței și a efectuării actelor de către organul de urmărire penală, iar Parchetul de pe lângă Înalta Curte de Casație și Justiție – D.I.I.C.O.T. – Serviciul Teritorial Cluj, căruia i-a fost comunicat memoriul, a răspuns în termenul prev. de art.344 alin.4 Cod de Procedură Penală.

Apreciem că excepțiile invocate sunt, în parte fondate, însă cele mai multe nu sunt fondate, din următoarele considerente:

Prin memoriul depus la dosar (filele 11-78), apărătorul ales al inculpatului Borș Simion Toader a solicitat excluderea tuturor probelor administrate cu încălcarea prevederilor legale, invocându-se nelegalitatea punerii în executare a mandatelor nr. 48/UP/2014 și 49/UP/2014 emise în dosarul 1152/117/2014 al Tribunalului Cluj, precum și a mandatului nr. 69/UP/2014, emis în dosarul nr. 1430/117/2014 al Tribunalului Cluj.

În cele ce urmează ne vom referi la mandatul nr. 69/UP/2014 și la modalitatea în care acesta a fost pus în executare, apreciind că cu această ocazie au fost încălcate norme procedural penale, după cum vom arăta în cele ce urmează.

Mandatul 69/UP/2014 emis în dosarul 1450/117/2014 al Tribunalului Cluj, ca urmare a pronunțării în același dosar a încheierii penale nr. 53/JDL/2014, la data de 13.03.2014, autorizează, pentru o perioadă de 30 de zile, începând cu data de 14.03.2014, supravegherea tehnică constând în interceptarea comunicațiilor sau a oricărui tip de comunicare de la distanță, purtate prin intermediul următoarelor adrese de email: |

, mandatul fiind valabil până la data de 12.04.2014.

Apărarea a invocat că, cu ocazia punerii în executare a acestui mandat, organele de poliție au efectuat activități neautorizate specifice accesului la un sistem informatic și conservarea datelor obținute, ulterior procedând la așa zise

analize fără solicitarea vreunei autorizații de percheziție informatică, fără înștiințarea inculpatului și cu îngrădirea implicită a dreptului său la apărare.

Cert este că potrivit unor procese verbale încheiate de către organele de urmărire penală cu ocazia punerii în executare a mandatului nr. 69/UP/2014, reiese că organele de urmărire penală au accesat comunicările purtate de inculpat prin intermediul celor trei adrese de e-mail,

(), într-o perioadă mult anterioară datei de la care organele de urmărire penală au fost autorizate să intercepteze comunicările purtate de inculpat prin intermediul adreselor de e-mail mai sus arătate, evidențiindu-se în cadrul acelor procese verbale comunicări ce ar fi avut loc în cursul anilor 2012, sau chiar 2011.

În sensul celor de mai sus apărarea invocă nulitatea proceselor verbale de la filele 265, 266, vol. II, a procesului verbal de la fila 317 din vol. II, a procesului verbal de la filele 214-215 din volumul III, a procesului verbal de la filele 192-200 vol. III, a procesului verbal existent la filele 200-214 și a procesului verbal de la filele 214-215 din vol. III, a procesului verbal de la fila 257 din vol. II, a procesului verbal de la fila 275 din vol. II.

Cu privire la aceste excepții, Parchetul de pe lângă Înalta Curte de Casație și Justiție – Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism – Serviciul Teritorial Cluj a arătat că mandatul de supraveghere tehnică nr. 69/UP/13.03.2014 a fost emis în cauză în baza încheierii penale nr. 53/C/P/13.03.2014 emisă de judecătorul de drepturi și libertăți din cadrul Tribunalului Cluj în dosarul nr. 1450/117/2014, pentru autorizarea măsurii de supraveghere tehnică constând în interceptarea comunicațiilor sau a oricărui tip de comunicare de la distanță purtate prin intermediul următoarelor adrese de e-mail:

: , utilizate de inculpatul Borș Simion Toader.

Potrivit disp. art. 138 al.2 NCPP, prin interceptarea comunicațiilor ori a oricărui tip de comunicare se înțelege interceptarea, accesul, monitorizarea, colectarea sau înregistrarea comunicărilor efectuate prin telefon, sistem informatic ori prin orice alt mijloc de comunicare.

Adresa de e-mail reprezintă un mod de comunicare în mediul virtual, cu ajutorul unor sisteme informatice, prin intermediul cărora utilizatorul se conectează, utilizând un sistem informatic având conexiune internet, la serverul, respectiv sistemul informatic care găzduiește adresa sa de e-mail. Rezultă astfel că modalitatea prin care poate fi realizată o interceptare a comunicațiilor purtate prin intermediul unei adrese de e-mail a utilizatorului o reprezintă în concret activitatea tehnică realizată cu privire la comunicările efectuate prin sistemul informatic care găzduiește adresa de e-mail.

De asemenea, din interpretarea termenilor rezultați din definiția măsurii de supraveghere tehnică de interceptare a comunicațiilor rezultă faptul că această măsură de supraveghere tehnică poate implica, pentru a fi pusă în executare, efectuarea unor activități tehnice diferite, nu doar strict de interceptare, ci și activități tehnice anterioare sau concomitente realizării efective a măsurii de interceptare, constând în accesul la comunicațiile efectuate

prin intermediul sistemului informatic care face obiectul măsurii, de monitorizare a comunicațiilor purtate prin intermediul sistemului informatic, de colectare sau înregistrare a comunicărilor efectuate printr-un sistem informatic.

Rezultă astfel că măsura de supraveghere tehnică de interceptare a comunicațiilor, pentru a putea fi realizată, poate implica efectuarea uneia sau mai multor activități tehnice fie de interceptare, de acces, de monitorizare, de colectare sau de înregistrare a comunicărilor efectuate printr-un sistem informatic, aceste activități putând fi utilizate integral sau alternativ, în funcție de natura mijlocului de comunicare care face obiectul măsurii de supraveghere tehnică. Astfel, s-a apreciat de către procuror că modalitatea de ordin tehnic prin care poate fi pusă în executare măsura de supraveghere tehnică de interceptare a comunicațiilor diferă în funcție de mijlocul prin care se realizează comunicările, legiuitorul urmărind prin enumerarea modalităților integrale sau alternative care pot fi utilizate pentru această măsură de supraveghere să însumeze totalitatea procedeele tehnice care pot fi utilizate pentru a pune în executare și valorifica o astfel de măsură de supraveghere.

Din analiza dispozițiilor legale sus menționate rezultă în mod implicit faptul că o măsură de supraveghere tehnică de interceptare a comunicațiilor poate implica, pentru a fi pusă în executare, activități de acces, de monitorizare, de colectare sau înregistrare a comunicărilor efectuate printr-un sistem informatic, modalitatea tehnică de realizare a acestor activități vizând sistemul informatic prin intermediul căruia se efectuează comunicările. Rezultă astfel că măsura de supraveghere tehnică de interceptare a comunicațiilor purtate prin intermediul unei adrese de e-mail poate fi realizată prin accesarea prealabilă a comunicărilor efectuate prin intermediul sistemului informatic care găzduiește adresa de e-mail, prin colectarea și înregistrarea comunicărilor efectuate prin acest mijloc de comunicare, reprezentând o măsură de supraveghere tehnică complexă care poate include în conținutul ei și măsura de acces într-un sistem informatic.

Potrivit disp. art. 139 al.3 NCPP, accesul într-un sistem informatic reprezintă pătrunderea într-un sistem informatic sau mijloc de stocare a datelor informatice, fie direct, fie de la distanță, prin intermediul unor programe specializate ori prin intermediul unei rețele, în scopul de a identifica probe.

Termenul de „monitorizare” a comunicărilor se referă la activitatea de supraveghere a comunicărilor, termenul de „colectare” reprezintă activitatea de a aduna la un loc comunicările, termenul de înregistrare reprezintă activitatea de reținere și imprimare a comunicărilor, în vederea păstrării lor și a redării ulterioare.

Rezultă astfel că măsura de interceptare a comunicațiilor reprezintă o măsură complexă din punct de vedere al activităților de ordin tehnic care implică materializarea rezultatelor obținute.

Referitor la obiectul măsurii de supraveghere tehnică de interceptare a comunicațiilor, tot din cuprinsul disp. art. 139 al. 2 NCPP, rezultă faptul că această măsură se referă la comunicările efectuate prin telefon, sistem informatic sau orice alt mijloc de comunicare, nefiind prevăzut în mod expres că activitatea

de interceptare ar privi exclusiv doar comunicările viitoare care vor fi efectuate prin intermediul unui sistem informatic și implicit nerezultând din textul legal amintit mai sus că utilizarea acestei metode ar privi doar strict comunicările care vor fi efectuate în viitor, pe durata dispunerii măsurii de supraveghere tehnică, durata pentru care este dispusă măsura reprezentând intervalul de timp în care sunt autorizate activitățile tehnice care implică punerea în executare a acestei măsuri. Procurorul a considerat că obiectul unei măsuri de supraveghere tehnică de interceptare a comunicațiilor poate privi atât comunicările care au fost efectuate sau care urmează a fi efectuate, raportat la mijlocul prin care sunt realizate și stocate aceste comunicări, neputând fi pus semnul egalității între modalitățile tehnice prin care se realizează interceptarea unor comunicări efectuate prin telefon, caz care exclude un acces în telefonul utilizatorului și cele care se realizează prin intermediul unui sistem informatic, mijloc care, datorită caracteristicilor tehnice, permite accesul și colectarea datelor referitoare la comunicațiile efectuate.

Tot în susținerea acestei argumentații s-a apreciat de către acuzare că trebuie analizate și disp. art. 138 al.1 lit. e rap. la art. 138 al.9 NCPP, referitoare la măsura de supraveghere tehnică de obținere a datelor privind tranzacțiile financiare ale unei persoane, în acest caz punerea în executare a acestei măsuri de supraveghere referindu-se expres atât la tranzacțiile efectuate, deci cele anterioare dispunerii măsurii de supraveghere, cât și la tranzacțiile viitoare, care urmează a fi efectuate.

Astfel Parchetul de pe lângă Înalta Curte de Casație și Justiție – Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism – Serviciul Teritorial Cluj a apreciat că modalitatea prin care a fost pusă în executare măsura de supraveghere tehnică a interceptării comunicațiilor purtate prin intermediul adreselor de e-mail utilizate de inculpatul Borș Simion Toader a fost realizată cu respectarea dispozițiilor legale, iar rezultatele obținute în urma punerii în executare, constând în identificarea și analizarea conținutului adreselor de e-mail care au făcut obiectul interceptării au reprezentat modalitatea legală prin care datele obținute au fost valorificate ca mijloace de probă în soluționarea prezentei cauze. S-a mai arătat că a interpreta conținutul dispozițiilor referitoare la interceptarea comunicațiilor purtate prin intermediul unui sistem informatic, în sensul că această măsură ar privi în mod exclusiv doar comunicările care vor fi efectuate pe viitor, pe perioada autorizării mandatului de supraveghere tehnică, ar reprezenta o adăugare nejustificată la prevederile legale care reglementează această instituție, întrucât din analiza dispozițiilor legale sus menționate rezultă că este folosit termenul de comunicări efectuate, și nu în mod expres termenul de comunicări care vor fi efectuate, astfel cum legiuitorul a precizat în cazul definiției date măsurii de supraveghere tehnică de obținere a datelor privind tranzacțiile financiare ale unei persoane.

S-a apreciat de către Parchet că susținerile din cuprinsul memoriului depus de inculpat prin apărătorii săi, referitoare la efectuarea de activități neautorizate, specific accesului la un sistem informatic, sunt nefondate, întrucât măsura de interceptare a comunicațiilor permite efectuarea de activități de acces

a sistemului informatic prin care sunt efectuate comunicările, precum și colectarea comunicărilor efectuate, astfel încât s-a considerat că modalitatea de punere în executare și valorificare a datelor rezultate din mandatul de supraveghere tehnică emis pentru interceptarea comunicațiilor purtate prin intermediul adreselor de e-mail utilizate de către inculpat a fost realizată cu respectarea dispozițiilor legale, iar rezultatul punerii în executare a acestei măsuri de supraveghere, materializat în întocmirea proceselor-verbale de redare a comunicărilor efectuate și de analizare a datelor rezultate în urma punerii în executare a acestei măsuri reprezintă modalitatea legală și concretă de valorificare a rezultatelor obținute.

Nu putem îmbrățișa acest punct de vedere, întrucât potrivit art. 138 al. (2) din Noul Cod de Procedură Penală, prin interceptarea comunicațiilor ori a oricărui tip de comunicare se înțelege interceptarea, accesul, monitorizarea, colectarea sau înregistrarea comunicărilor efectuate prin telefon, sistem informatic ori prin orice alt mijloc de comunicare, activitate valabilă pentru viitor începând cu momentul autorizării.

În acest sens Tribunalul Cluj are o practică constată în a considera că este vorba despre *comunicările viitoare*, indiferent de mijlocul tehnic prin care acestea se realizează, fie telefon mobil, sistem informatic sau alt mijloc de comunicare. Este real că textul de lege mai sus amintit utilizează adjectivul efectuate, fără a distinge dacă este vorba despre comunicări trecute sau viitoare, însă, așa cum am mai arătat, dacă în privința comunicărilor realizate prin intermediul telefonului mobil nu există nici umbră de îndoială că este posibilă doar interceptarea comunicărilor viitoare, pe durata menționată în mandatul de autorizare a măsurii, aspect pe care Parchetul nu l-a contestat niciodată, și a pus întocmai în executare mandatele aferente, nu înțelegem de ce ar fi necesară crearea acestei distincții atunci când vine vorba despre comunicările realizate prin intermediul unui sistem informatic.

Mai mult noțiunea de „acces” utilizată de dispozițiile art. 138 al. 2 Cod de Procedură Penală nu se referă la accesul la sistemul informatic prin intermediul căruia s-a realizat comunicarea ci se referă la însăși comunicarea în cauză.

În acest sens s-a exprimat și doctrina de specialitate (*a se vedea Mihail Udriș: „Procedură Penală, Partea Generală”, editura C.H. Beck, București 2014, paginile 303-304*), unde se arată că accesul la un sistem informatic este utilizat în practică pentru pătrunderea în sisteme informatice în care sunt stocate e-mail-uri, așadar după interceptarea email-ului, interceptare ce se realizează la momentul la care se realizează comunicarea, se poate pătrunde în sistemul informatic pentru analizarea mail-urilor transmise și înainte de perioada în care acestea au fost interceptate.

Este necesar să observăm că prin mandatul 69/UP/2014, judecătorul de drepturi și libertăți de la Tribunalul Cluj a autorizat **numai interceptarea** comunicărilor efectuate de către inculpat prin intermediul celor trei adrese de e-mail. Ori potrivit Dicționarului Explicativ al Limbii Române interceptat înseamnă prins, reținut, surprins, controlat, sesizat, ori nu poate fi prins și reținut

decât ceva în mișcare, în derulare, așa cum este o comunicare ce tocmai se desfășoară, și nu una ce deja a avut loc.

Consecința acestei neregularități este nulitatea relativă parțială a următoarelor probe, urmând ca acestea să fie excluse în măsura în care conțin interceptări ale unor comunicări efectuate de inculpat, prin sistem informatic, aferente adreselor de e-mail

, anterior datei de 14.03.2014, dată începând cu care a fost autorizată măsura supravegherii tehnice a interceptării comunicărilor efectuate de către inculpat prin intermediul sistemelor informatice, potrivit încheierii penale nr. 53/2014, pronunțată în dosarul nr. 1450/117/2014, și în baza căreia au fost emise mandatele de interceptare nr. 69/UP/2014 și 70/UP/2014, aici interesând mandatul 69/UP/2014, și anume ne referim la procesul verbal existent la fila 265, vol. II din dosarul de urmărire penală, procesul verbal existent la fila 266 din vol. II al dosarului de urmărire penală, procesul verbal existent la filele 214-215 din vol. III de urmărire penală, procesul verbal existent la filele 192-199 din vol. III de urmărire penală și procesul verbal existent la filele 200-213 din vol. III al dosarului de urmărire penală, precum și la actele subsecvente acestora.

Cu toate că apărarea a cerut și excluderea procesului verbal încheiat la data de 07.03.2014, și aflat la – fila 257 din vol. II din dosarul de urmărire penală, apreciem că acest proces verbal nu reprezintă o probă rezultată din punerea în executare a mandatului nr. 69/UP/2014, practic nu are legătură cu acest mandat de supraveghere tehnică, așa încât judecătorul de cameră preliminară nu va proceda la excluderea lui. Situația este identică și pentru procesul verbal din 13.05.2014, care se află la fila 275 vol. II, nici acesta neavând vreo legătură cu mandatul de supraveghere tehnică mai sus amintit, astfel că nu va fi exclus deși apărarea a solicitat aceasta.

Așa cum am arătat, celelalte excepții invocate de către apărare urmează să fie respinse, după cum vom arăta în cele ce urmează:

1). S-a solicitat restituirea cauzei la parchet având în vedere neregularitatea actului de sesizare a instanței, ca urmare a omisiunii descrierii faptelor reținute în sarcina inculpatului într-un mod susceptibil de a produce consecințe juridice și a omisiunii analizării detaliate a probelor administrate în cuprinsul rechizitoriului, de manieră a susține acuzațiile.

Această excepție nu este fundamentată în condițiile în care rechizitoriul prin care inculpatul a fost trimis în judecată cuprinde, la capitolul descrierea stării de fapt nu mai puțin de 65 de pagini. Este adevărat că infracțiunile pentru care inculpatul a fost trimis în judecată au un specific tehnic evident, motiv pentru care și descrierea stării de fapt conține multe date tehnice, cu prea puține elemente narrative, dat fiind specificul infracțiunilor cercetate.

Astfel, trebuie să evidențiem că prin rechizitoriul emis la data de 06.10.2014 a fost trimis în judecată inculpatul Borș Simion Toader, pentru săvârșirea infracțiunilor de acces ilegal la un sistem informatic, prev. de art.360 alin.1, 2 și 3 din CP și operațiuni ilegale cu dispozitive sau programe informatice, în modalitatea deținerii fără drept a unor programe informatice și a

unor date informatice și parole, în scopul săvârșirii uneia dintre infracțiunile prev. de art. 360 – 364 NCP, în formă continuată, prev. de art. 365 alin. 2 NCP, cu aplic. art. 35 alin. 1 NCP, cu aplic. art. 38 alin. 1 NCP.

Din lecturarea rechizitoriului amintit reiese că acesta a fost întocmit cu respectarea dispozițiilor prev. de art. 328 – art. 330 NCPP, actul de sesizare conținând în mod complet și integral *date referitoare la faptele reținute* în sarcina inculpatului, și care au fost descrise și expuse în mod detaliat în cuprinsul stării de fapt, cu indicarea perioadei săvârșirii acestora, a modalității de comitere și a descrierii complete a activității infracționale reținute, *date referitoare la încadrarea juridică* corespunzătoare activității infracționale reținute în sarcina inculpatului, potrivit descrierii cuprinsă la capitolul starea de fapt, *date referitoare la probele și mijloacele de probă* care au condus la adoptarea soluției de trimitere în judecată a inculpatului. Prin urmare apreciem că au fost indicate și descrise în cuprinsul rechizitoriului probele pe care se fundamentează acuzația, cu expunerea conținutului acestora și cu indicarea filelor și volumelor unde acestea se regăsesc.

Drept consecință, considerăm că actul de sesizare a instanței cuprinde toate mențiunile obligatorii, faptele fiind descrise pe larg, cu indicarea infracțiunilor și a actelor normative care le reglementează, nerezultând vreo situație care să conducă la o vătămare a drepturilor inculpatului, actul de sesizare al instanței îndeplinind cerințele legale, rezultând din conținutul acestuia învinuirea adusă inculpatului, denumirea și descrierea faptelor imputate și încadrarea juridică corespunzătoare.

Se mai critică rechizitoriul arătându-se că la capitolul soluții de disjungere se arată că în cauza disjunsă se apreciază că sunt incidente prev. art. 142. al. 5 NCPP referitoare la datele rezultate în urma punerii în aplicare a măsurilor de supraveghere care au fost autorizate în prezenta cauză date ce urmează a fi folosite în cauza disjunsă. Ori inculpatul fiind trimis în judecată pentru infracțiuni informatice, dosar în care toate probele atât în acuzare cât și în apărare se regăsesc pe sistemele informatice: hard-uri, cd-uri, etc., ridicate sau cele formate în urma măsurilor de supraveghere tehnică, este evident că acesta este restricționat să-și exercite dreptul la apărare datorită netrimiterii mijloacelor materiale de probă o dată cu rechizitoriul cu atât mai mult cu cât acestea sunt contestate. Se mai arată de către apărare că inclusiv instanța de judecată, în lipsa trimiterii probelor și a mijloacelor de probă la care se face trimitere în cuprinsul rechizitoriului, nu poate verifica conținutul proceselor verbale, ce teoretic reprezintă materializarea unor proceduri de analiză, procese verbale întocmite de către organul de cercetare. În aceste condiții inculpatul nu poate să beneficieze de respectarea dreptului la apărare.

Apreciem că și aceste excepții sunt nefondate. Astfel, este de remarcat în primul rând că soluția de disjungere emisă de Parchetul de pe lângă Înalta Curte de Casație și Justiție – Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism – Serviciul Teritorial Cluj, prin rechizitoriul criticat, nu face obiectul analizei în această etapă procesuală și în acest cadru procesual,

soluția de disjungere putând fi atacată cu plângere la procurorul ierarhic superior celui ce a dispus-o.

În privința lipsei mijloacelor de probă din dosarul cauzei trebuie să observăm că potrivit adresei de înaintare a rechizitoriului și a dosarului de urmărire penală către instanța de judecată, datată 06.10.2014, au fost trimise instanței următoarele mijloace materiale de probă:

- un plic sigilat conținând un proces-verbal, în original, încheiat în baza dispozițiilor art. 143 NCPP, referitor la punerea în executare a măsurilor de supraveghere tehnică de acces în sisteme informatice dispuse în baza ordonanțelor procurorului din data de 15.04.2014, în dosar nr. 126 D/P/2013 al D.I.I.C.O.T. – S.T. Cluj, măsuri confirmate de judecătorul de drepturi și libertăți din cadrul Tribunalului Cluj, în baza încheierii penale nr. 103/C/P/18.04.2014 – dosar nr. 2429/117/2014, o cutie, sigilată cu sigiliul MI seria 36264 unde se află un hard disk marca Western Digital de capacitate 500 Gb, cu seria WXD1A2445619, și o cutie sigilată cu sigiliul MI seria 36264 unde se află un hard disk marca Western Digital de capacitate 500 Gb, cu seria WXD1A24D3573, care conțin copii după datele rezultate în urma punerii în aplicare a măsurilor de supraveghere sus menționate, care sunt atașate la procesul-verbal sus menționat.

În conformitate cu art. 141 al. 5 lit. a NCPP, în cazul datelor informatice identificate prin accesul la un sistem informatic, procurorul poate dispune prin ordonanță realizarea și conservarea de copii, ori prin ordonanțele prin care s-a dispus autorizarea acestei măsuri de supraveghere de către procuror, s-a dispus și efectuarea de copii ale datelor informatice care s-au regăsit pe sistemele informatice cu privire la care s-a efectuat accesul.

- un plic sigilat conținând un proces-verbal, în original, încheiat în baza disp. art. 143 NCPP, referitor la punerea în executare a măsurii de supraveghere tehnică constând în interceptarea comunicațiilor sau a oricărui tip de comunicare de la distanță, măsură autorizată de către judecătorul de drepturi și libertăți din cadrul Tribunalului Cluj, în baza încheierii penale nr. 53/C/P/13.03.2014 – dosar nr. 1450/117/2014, și un plic sigilat cu sigiliul MI 36264, conținând un suport optic, reprezentând copie după suportul optic original care conține rezultatul activității de supraveghere tehnică sus menționată, suport optic care este atașat procesului-verbal sus menționat; precum și un proces-verbal, în original, încheiat în baza disp. art. 143 NCPP, referitor la punerea în executare a măsurii de supraveghere tehnică constând în supravegherea video, audio sau prin fotografiere autorizată de către judecătorul de drepturi și libertăți din cadrul Tribunalului Cluj, în baza încheierii penale nr. 35/C/P/28.02.2014 – dosar nr. 1152/117/2014, și prelungită în baza încheierii penale nr. 67/C/P/27.03.2014 – dosar nr. 1765/117/2014, și un suport CD, sigilat cu sigiliul MI 36264, care are în interior un număr de 28 suporturi optice conținând copii după suportii optici originali care conțin rezultatul activității de supraveghere tehnică sus menționată, atașati procesului-verbal sus menționat.

Suportii optici sus menționați, reprezentând copii ai suporturilor care conțin rezultatul activității de supraveghere tehnică, au fost înaintați

Tribunalului Cluj, în conformitate cu disp. art. 143 al.2 NCPP, din conținutul acestor dispoziții legale rezultând faptul că se înaintează instanței copia suportului care conține activitățile de supraveghere tehnică, suportul original fiind păstrat la sediul parchetului, putând fi pus la dispoziția instanței, la solicitarea acesteia.

De asemenea, din cuprinsul proceselor verbale încheiate în cursul urmăririi penale, referitoare la datele obținute în urma punerii în executare a măsurilor de supraveghere tehnică de interceptare a comunicațiilor sau a oricărui tip de comunicare de la distanță, precum și de supraveghere video, audio sau prin fotografiere existenți, rezultă faptul că suportii optici originali, au fost predați în vederea păstrării, la sediul parchetului, în locuri speciale, potrivit disp. art. 143 al. 2 NCPP.

- un număr de 2 (două) hard disk-uri, unul marca Verbatim – seria 530293423502221 și unul marca Seagate, seria NA498BK7, care conțin rezultatul perchezițiilor informatice.

Așadar susținerile din cuprinsul memoriului cuprinzând excepțiile referitoare la obiectul camerei preliminare, prin care se invocă lipsa mijloacelor de probă reprezentând rezultatul măsurilor de supraveghere tehnică utilizate în cauză și al perchezițiilor informatice efectuate în cauză sunt neîntemeiate, întrucât toate rezultatele activităților sus menționate au fost înaintate instanței de judecată, în conformitate cu dispozițiile legale în materie, care au fost respectate întocmai.

2). S-a mai invocat de către inculpat nerespectarea dreptului la apărare a acestuia față de împrejurarea că toate solicitările în probațiune formulate de către inculpat au fost respinse cu o motivare sumară. Se arată în acest sens că în volumul 8 începând cu filele 276, fila 355, fila 375, etc., se regăsesc o parte din cererile inculpatului în probațiune, toate fiind respinse, iar pe parcursul celor 6 luni de anchetă, organele de urmărire penală nu au administrat nicio probă în favoarea inculpatului.

Apreciem că această excepție ține de temeinicia acuzațiilor și nu de legalitatea administrării probelor ori a efectuării actelor de urmărire penală, în condițiile în care ordonanțele de soluționare a cererilor în probațiune, aflate în vol. 8, au fost întocmite cu respectarea dispozițiilor legale prevăzute de art. 100 al. 3 NCPP, fiind motivate în fapt și în drept. Din cuprinsul acestor acte de urmărire penală rezultă în mod explicit și clar modalitatea de soluționare a fiecăreia dintre cererile formulate de către inculpat, și considerentele care au condus la adoptarea fiecăreia dintre soluțiile dispuse.

Prin urmare, câtă vreme cererile în probațiune au fost respinse ca neîntemeiate, nimic nu-l împiedică pe inculpatul să le reitereze în fața instanței de judecată, care poate să manifeste altă opinie juridică și să aprecieze că cererile sunt fondate și să procedeze la administrarea lor. Deci, așa cum am arătat excepția de mai sus are legătură cu temeinicia cererilor de administrare a unor probe, cereri respinse, și nu cu legalitatea lor.

3). De asemenea, inculpatul, prin apărătorii săi, invocă excluderea probelor obținute în baza mandatele de supraveghere tehnică emise sub numerele 48 și 49, în dosarul nr. 1152/117/2014 al Tribunalului Cluj.

Se arată, în susținerea acestei excepții că la data de 28.02.2014 Tribunalul Cluj, prin încheierea nr. 35/C/P/2014 pronunțată în dosarul nr. 1152/117/2014 a dispus admiterea în parte a solicitărilor parchetului, respectiv a dispus autorizarea măsurii supravegherii tehnice constând în accesul la sistemul informatic utilizat de inculpat, existent la adresa din Cluj-Napoca, str. Ion Mester nr. 3 ap. 59 și totodată a dispus autorizarea supravegherii tehnice constând în supravegherea video, audio sau prin fotografiere a inculpatului pentru o perioadă de 30 de zile, din data de 29.02.2014 până la data de 29.03.2014.

În baza mandatului 49 s-a autorizat supravegherea tehnică constând în supravegherea video, audio sau prin fotografiere a inculpatului, sens în care s-au întocmit mai multe procese verbale conform art. 143 din Noul Cod de Procedură Penală, unele dintre ele, apreciindu-se de către apărare, cu încălcarea prevederilor legale. Inculpatul consideră că acesta este cazul procesului verbal încheiat la data de 26.03.2014, fila 264 Vol. I din dos. de u.p., întrucât la dosarul de urmărire penală sunt depuse fotografiile ale sistemelor informatice teoretic utilizate de inculpat, în condițiile în care măsura dispusă viza supravegherea video, audio și fotografierea persoanei inculpatului, nu a imobilului său ori a bunurilor despre care s-ar considera că îi aparțin, judecătorul de drepturi și libertăți de la Tribunalul Cluj specificând expres persoana inculpatului, cu atât mai mult cu cât în imobilul respectiv posibil să fi locuit și alte persoane, altele decât numita Uifălean Alexandra, prietena inculpatului.

Considerăm că și această excepție este nefondată. Așa fiind, trebuie să remarcăm că mandatul de supraveghere tehnică nr. 49/UP/28.02.2014 a fost emis în cauză în baza încheierii penale nr. 35/C/P/28.02.2014 pronunțată de judecătorul de drepturi și libertăți din cadrul Tribunalului Cluj în dosarul nr. 1152/117/2014, pentru autorizarea măsurii de supraveghere tehnică a supravegherii video, audio sau prin fotografiere a numitului Borș Simion Toader. Totodată, prin mandatul respectiv a fost autorizată încuviințarea pătrunderii în spațiul privat, respectiv în locuința inculpatului, pentru activarea/dezactivarea mijloacelor de supraveghere tehnică ce urmau a fi folosite pentru executarea acestei măsuri de supraveghere. Deci, una dintre componentele punerii în executare a acestei măsuri de supraveghere o reprezintă surprinderea activității desfășurate de către Borș Simion Toader în locuința sa, în legătură cu obiectul cauzei pentru care se efectuau cercetările, în concret infracțiuni informatice, comise prin intermediul sistemelor informatice.

În conformitate cu prevederile art. 138 al. 6 din Noul Cod de Procedură Penală, prin supraveghere video, audio sau prin fotografiere se înțelege fotografierea persoanelor, observarea sau înregistrarea conversațiilor, mișcărilor ori a altor activități ale acestora. Ori fotografiile efectuate asupra sistemelor informatice deținute la locuința inculpatului Borș Simion Toader reprezintă un rezultat valabil al punerii în executare a măsurii de supraveghere tehnică de

supraveghere video, audio sau prin fotografiere, modalitate de punere în executare a acestui procedeu probator, fiind vorba despre înregistrări de imagini din spații private. În prezenta cauză sistemele informatice de la domiciliul inculpatului au reprezentat un mijloc de realizare a modalității de comitere a activității infracționale identificate în cazul inculpatului Borș Simion Toader, iar fotografierea acestora, în baza mandatului de supraveghere sus menționat, reprezintă o componentă a modalității de realizare a acestei măsuri de supraveghere tehnică, care poate fi materializată și prin înregistrarea de imagini. De altfel, fotografierea sistemelor informatice găsite la domiciliul inculpatului, reprezintă fixarea mijloacelor tehnice utilizate de către inculpat în cadrul activităților sale, presupus infracționale, opri aceste mijloace tehnice sunt indisolubil legate de activitatea persoanei supuse măsurii de supraveghere.

Așa cum a subliniat și Parchetul de pe lângă Înalta Curte de Casație și Justiție – Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism – Serviciul Teritorial Cluj în memoriul depus la dosar, măsura de supraveghere tehnică constând în supravegherea video, audio sau prin fotografiere a inculpatului Borș Simion Toader a fost pusă în executare cu respectarea dispozițiilor legale, fotografierea sistemelor informatice de la locuința inculpatului reprezentând o modalitate de materializare în plan probator a activității presupus infracționale desfășurate de către acesta, prin intermediul sistemelor informatice de la locuința sa, măsura fiind impusă de necesitatea identificării sistemelor informatice utilizate în activitatea de care era bănuț inculpatul că o desfășoară.

4). De asemenea apărarea mai solicită să se constate nulitatea tuturor proceselor verbale întocmite în urma analizelor efectuate de către lucrătorii BCCO asupra informațiilor și datelor existente pe sistemul SEAGATE cu seria NA4KFJ03 ulterior copiate pe un hard extern marca WESTERN DIGITAL de capacitate 1 TB având seria WCC3F2934060, întrucât au fost întocmite cu încălcarea mai multor prevederi legale.

Apreciem că nici aceste excepții nu sunt întemeiate. Astfel, așa cum reiese din actele de la dosar, cu ocazia efectuării percheziției domiciliare la locuința inculpatului la data de 15.04.2014, au fost identificate mai multe sisteme informatice aflate în legătură funcțională, respectiv un sistem informatic cu seria RC942KKN1112100733, de culoare neagră, având atașat un hard disk extern marca WD, inscripționat „My passport for MAC” și un hard extern de culoare argintiu cu negru marca Storec, în stare de funcționare iar pe sistemul informatic cu seria RC942KKN1112100733, un sistem informatic - dispozitiv extern marca DS213+ cu seria D3L1N09889 cu MAC 0011321E22B9, care are cuplat un hard disk extern WD (f. 82-83 vol.4).

Prin ordonanța procurorului din data de 15.04.2014, ora 16:30, s-a dispus autorizarea, cu titlu provizoriu, pe o durată de 48 ore, de la data de 15.04.2014, ora 17:00, până la data de 17.04.2014, ora 17:00, a măsurii de supraveghere tehnică constând în accesul în sistemul informatic identificat cu seria RC942KKN1112100733, de culoare neagră, având atașat un hard disk extern marca WD, inscripționat „My passport for MAC” și un hard extern de culoare

argintiu cu negru marca Storec, în stare de funcționare, identificat cu ocazia efectuării percheziției domiciliare sus menționate, precum și autorizarea, cu titlu provizoriu, pe o durată de 48 ore, de la data de 15.04.2014, ora 17:00, până la data de 17.04.2014, ora 17:00, a măsurii de supraveghere tehnică constând în accesul în sistemul informatic - dispozitiv extern marca DS213+ cu seria D3L1N09889 cu MAC 0011321E22B9, care are cuplat un hard disk extern WD de culoare neagră fără alte date de identificare, identificat cu ocazia efectuării percheziției domiciliare, realizarea și conservarea de copii ale datelor informatice identificate prin accesul la sistemele informatice cu privire la care s-a dispus în mod provizoriu prin ordonanța sus menționată măsura de supraveghere tehnică constând în accesul la sistemul informatic, măsura sus menționată fiind confirmată de către judecătorul de drepturi și libertăți de la Tribunalul Cluj, conform încheierii penale nr. 103/C/P/18.04.2014, pronunțată în dosarul nr. 2429/117/2014.

În urma punerii în executare a ordonanței provizorii de acces în sistem informatic, menționată mai sus, ar fi rezultat faptul că, în taskbar-ul (bara de activități din sistemul de operare, afișată pe ecranul computerului), aferent sistemului informatic identificat cu seria RC 942 KKN 11112100733, au fost identificate, printre programele care ar fi rulat, două programe Putty, din care unul ar fi conectat la sistemul „Rasberry Pi”, iar celălalt la un sistem informatic având IP 91.223.82.179, aceeași adresă de IP de la care ar fi fost accesat în data de 21.01.2013 serverul care găzduiește site-ul Președenției României. De asemenea, ar fi rezultat faptul că, sistemele informatice identificate de către organele de poliție cu ocazia efectuării percheziției domiciliare se aflau în legătură funcțională.

Acest aspect ar demonstra faptul că, întrucât unul dintre sistemele informatice de la domiciliul inculpatului, ar fi fost conectat la sistemul informatic cu IP-ul sus menționat, iar inculpatul ar fi administrat un server virtual care i-ar fi fost alocat cu aceeași adresă de IP, inculpatul ar fi fost utilizatorul sistemului informatic identificat cu adresa de IP 91.223.82.179, aflat în legătură cu sistemul informatic de la domiciliul său.

Referitor la sistemul informatic cu adresa IP 91.223.82.179, cu privire la care ar fi rezultat că se află în legătură funcțională cu sistemul informatic identificat cu seria RC 942 KKN 11112100733, astfel cum a rezultat din cercetările efectuate, s-a stabilit faptul că această adresă de IP aparține inculpatului Borș Simion Toader, și că i-ar fi fost alocată acestuia de reprezentanții International Widespread Services Limited, de la această adresă IP fiind, se pare, inițiate în data de 21.01.2013 în intervalul 11:03-13:26, atacuri informatice asupra serverului www.presidency.ro.

Prin ordonanța din data de 15.04.2014, ora 20:45, s-a dispus autorizarea, cu titlu provizoriu, pe o durată de 48 ore, de la data de 15.04.2014, ora 21:00, până la data de 17.04.2014, ora 21:00 a măsurii de supraveghere tehnică constând în accesul în sistemul informatic - dispozitiv „Rasberry Pi”, conectat la sistemul informatic identificat cu seria RC942KKN11112100733, cu privire la care s-a dispus prin ordonanța procurorului din data de 15.04.2014 autorizarea

provizorie a accesului în acest sistem informatic; autorizarea, cu titlu provizoriu, pe o durată de 48 ore, de la data de 15.04.2014, ora 21:00, până la data de 17.04.2014, ora 21:00 a măsurii de supraveghere tehnică constând în accesul în sistemul informatic cu adresa IP 91.223.82.179, conectat la sistemul informatic identificat cu seria RC942KKN11112100733, cu privire la care s-a dispus prin ordonanța procurorului din data de 15.04.2014 autorizarea provizorie a accesului în acest sistem informatic, precum și realizarea și conservarea de copii ale datelor informatice identificate prin accesul la sistemele informatice cu privire la care s-a dispus în mod provizoriu măsura de supraveghere tehnică constând în accesul la sistemul informatic, măsura sus menționată fiind confirmată de către Tribunalul Cluj – dosar nr. 2429/117/2014, în baza încheierii penale nr. 103/C/P/18.04.2014, rezultând faptul că sistemul informatic conectat la adresa IP 91.223.82.179 era funcțional și ar fi fost utilizat și administrat de către inculpat.

Nu există la dosar nici o dovadă din care să rezulte că datele informatice accesate ar fi fost alterate în vreun fel, câtă vreme au fost copiate în condiții tehnice apte să asigure integritatea informațiilor conținute în sistemele informatice, fiind întocmite de către organele de poliție, cu privire la fiecare activitate tehnică realizată, procese-verbale de consemnare a activităților efectuate și a modalității tehnice prin care s-a realizat fiecare activitate.

5). Apărarea a mai susținut că la momentul punerii în executare a ordonanței procurorului din 15.04.2014, ora 20:45, prin care s-a autorizat provizoriu accesul la sistemele informatice deținute la domiciliul inculpatului, ofițerii de poliție au accesat prin intermediul internetului serverul cu IP 91.223.82.179 și au copiat din Olanda date prin intermediul calculatorului inculpatului, iar în plus, ofițerii de poliție nu au folosit programul ENCASE sau alt program pentru a nu se altera datele din calculatorul inculpatului, fapt ce rezultă inclusiv din procesele verbale încheiate și din procesele verbale de efectuare a percheziției domiciliare.

Considerăm că și aceste aspecte invocate de către inculpat țin de temeinicia acuzațiilor, în condițiile în care în procesele verbale încheiate cu ocazia punerii în aplicare a ordonanțelor procurorului de acces la sistemele informatice descoperite la domiciliul inculpatului s-a consemnat că aceste sisteme erau în legătură funcțională cu serverul cu IP-ul mai sus indicat. Ori evident că numai în cadrul cercetării judecătorești se va putea stabili dacă erau sau nu erau într-o asemenea legătură, dacă se va putea face distincție între datele informatice conținute de sistemele informatice aflate la domiciliul inculpatului și cele ce ar fi fost copiate de pe serverul din Olanda, cunoscut fiind că orice dubiu este de natură a-i profita inculpatului. Însă așa cum am arătat toate cele invocate de către apărare țin de temeinicia acuzațiilor și nu de legalitatea efectuării actelor de urmărire penală sau a administrării probelor.

6). Inculpatul, prin apărătorii săi, mai invocă nulitatea relativă a proceselor verbale aflate la filele 161, 170-179 și 180, din vol. IV de urmărire penală, precum și nulitatea actelor subsecvente, arătându-se că s-a procedat la o analiză a rezultatelor autorizării provizorii a accesului la sistemele informatice

deținute de către inculpat, fără a se autoriza de către judecătorul de drepturi și libertăți percheziția informatică.

Judecătorul de cameră preliminară de la Tribunalul Cluj apreciază că și aceste excepții sunt nefondate, având în vedere că dispozițiile legale care reglementează modalitatea de valorificare a datelor obținute în urma accesului autorizat la un sistem informatic sunt cuprinse în art.142-143 NCPP, procesele-verbale de consemnare a activităților de supraveghere tehnică efectuate reprezentând mijlocul de probă obținut prin utilizarea acestui procedeu probator, normele procedurale necondiționând valabilitatea acestui mijloc de probă de obligativitatea efectuării unei percheziții informatice.

Ori putem observa că procesele-verbale conținând aspectele constatate cu privire la sistemele informatice identificate cu ocazia efectuării percheziției domiciliare, precum și cele întocmite în urma punerii în executare a măsurii de supraveghere tehnică de acces în sistemele informatice utilizate de inculpat, au fost întocmite cu respectarea dispozițiilor legale și reprezintă mijloace de probă legal administrate în prezenta cauză.

Este real că literatura de specialitate și practica judiciară nu a consacrat încă o distincție clară și precisă între cele două procedee probatorii, și anume accesul la un sistem informatic și percheziția informatică, când anume trebuie folosit unul sau altul din cele două. Personal opinăm că accesul la un sistem informatic este de preferat a se utiliza în faza incipientă a cercetărilor penale, și când urmărirea penală este începută doar *in rem*, așa cum s-a procedat și în speța de față, iar percheziția informatică se poate dispune atât în faza incipientă cât și după ce în cauză există un suspect.

Pe de altă parte apreciem că distincția dintre cele două procedee probatorii este dată și de oportunități de anchetă penală, în condițiile în care, potrivit Ghidului Introductiv pentru Aplicarea Dispozițiilor Legale Referitoare la Criminalitatea Informatică elaborat de Ministerul Telecomunicațiilor și Tehnologia Informației, cu ocazia efectuării percheziției informatice se impune ridicarea sistemelor informatice, ceea ce presupune, în primul rând, închiderea sistemelor găsite. Ori în speța de față, la momentul pătrunderii în domiciliul inculpatului, cu ocazia efectuării percheziției domiciliare, sistemele informatice au fost găsite în funcțiune, iar datele cauzei conduceau spre presupunerea că închiderea sistemelor ar putea implica pierderea unor date informatice, motiv pentru care s-a preferat, în speța de față, aplicarea procedurii probatorii al accesului în sistemul informatic, în scopul de a identifica probe.

7). Apărarea a solicitat și constatarea nulității relative a raportului de constatare tehnico-științific efectuat în cauza de către I.T.A. și aflat în dosarul de urmărire penală începând cu fila 347 din vol. V al dosarului de urmărire penală, având în vedere ca acesta a avut la bază analiza unor date obținute nelegal de către organele de poliție cu încălcarea drepturilor inculpatului, fără a fi urmată procedura percheziției informatice.

Considerăm că și această cerere este nefondată având în vedere faptul că raportul de constatare tehnico-științifică întocmit de către Institutul pentru Tehnologii Avansate București a avut ca obiectiv cercetarea și analizarea unor

fișiere și foldere, care ar fi fost identificate ca fiind deținute în sistemele informatice utilizate de inculpatul Borș Simion Toader, potrivit procesului-verbal întocmit de către organele de poliție din data de 29.07.2014 și aflat la filele 298-299 din vol. V al dosarului de urmărire penală. În cuprinsul acestui proces-verbal sunt exemplificate date informatice care au rezultat fie în urma efectuării perchezițiilor informatice asupra sistemelor informatice utilizate de către inculpatul Borș Simion Toader, fie în urma punerii în executare a ordonanțelor procurorului prin care s-a autorizat, în mod provizoriu, accesul în sistemele informatice utilizate de către inculpat, în acest din urmă caz, procesele-verbale de consemnare a activităților de supraveghere tehnică efectuate reprezentând mijloace de probă legale, normele procedural-penale necondiționând valabilitatea lor de obligativitatea efectuării unei percheziții informatice.

Prin urmare datele analizate de către Institutul pentru Tehnologii Avansate au fost legal obținute, astfel încât procesul-verbal cuprinzând datele informatice transmise spre analiză Institutului pentru Tehnologii Avansate, a fost întocmit cu respectarea dispozițiilor legale și reprezintă un mijloc de probă legal administrat, sens în care atât acesta cât și actul subsecvent, respectiv raportul de constatare tehnico-științifică întocmit de către institutul mai sus amintit se impun a fi menținute ca mijloace de probă în prezenta cauză.

8). Cu privire la nulitatea proceselor verbale încheiate la datele de 20.08.2014 și respectiv 22.08.2014, aflate la filele 52 din vol. VI și 470-490 din vol. V, considerentele exprimate sub punctul 6), în sensul respingerii acestei cereri sunt valabile și în situația de față. Pe de altă parte, este de observat că unele argumente invocate de către apărare în raport de procesul verbal din 22.08.2014, din vol. V (paginile 55-59 din memoriul de pus de către inculpat conținând cererile și excepțiile invocate cu privire la obiectul camerei preliminare) se plasează pe tărâmul temeiniciei acuzațiilor și nicidecum pe cel al legalității efectuării actelor de urmărire penală sau al administrării probelor.

9). S-a solicitat de către apărare excluderea tuturor actelor efectuate în cauză anterior începerii urmăririi penale, în lipsa consemnării acestora într-un proces verbal de constatare a efectuării actelor premergătoare, respectiv a adresei din 25.06.2013 (f. 8-9), a procesului verbal de investigații din 01.06.2013 (f. 10), a procesului verbal de investigații (filele 14-16), a adresei de la filele 12-13, a proceselor-verbale de verificare și constatare din 01.07.2013, 02.07.2013, 26.07.2013, 22.07.2013 (filele 1-4, 16), a adreselor și ordonanțelor de delegare (filele 9, 10-11, 25, 26-27, 38, 39-40), a adreselor către SC Telemobil România (filele 12-15, 28-30), a adreselor nr. 187/23.07.2013, nr. 189/31.07.2013, nr. 191/02.08.2013 și nr. 192/07.08.2013, nr. 197/09.08.2014, nr. 202/17.09.2014 emise de Telemobil și CD (filele 17, 31, 32-34, 36, 37, 41, 43, 44, 46), a procesului-verbal din 23.09.2013 de analiza a răspunsurilor primite de la SC Telemobil România (filele 47-51).

Apreciem că nici această cerere nu este fondată având în vedere că normele procedural penale actuale, în vigoare începând cu data de 01.02.2014, nu mai prevăd etapa actelor premergătoare, ca etapă distinctă a urmăririi penale.

Ori la momentul intrării în vigoare a Noului Cod de Procedură Penală, etapa actelor premergătoare nu era încheiată, ca să se poată consemna actele premergătoare efectuate într-un proces verbal, conform art. 224 al. 3 din Codul de Procedură Penală din 1968, iar după data mai sus menționată, noile norme procedural penale fiind de imediată aplicare, nu a mai fost posibilă încheierea unui proces verbal de acte premergătoare. Potrivit art. 4 al. 1 din L. 255/2013 privind punerea în aplicare a Legii 135/2010 privind Cod de Procedură Penală, actele de procedură îndeplinite înainte de intrarea în vigoare a Noului Cod de Procedură Penală, cu respectarea dispozițiilor legale în vigoare îndeplinirii lor, rămân valabile, cu excepțiile prevăzute de legea 255/2013. Ori în cauza de față, actele efectuate înainte de începerea urmăririi penale, în etapa actelor premergătoare, etapă ce nu fusese finalizată până la momentul intrării în vigoare a Noului Cod de Procedură Penală, au fost efectuate cu respectarea normelor ce guvernau la vremea respectivă desfășurarea procesului penal.

Sintetizând cele mai sus expuse, judecătorul de cameră preliminară de la Tribunalul Cluj va admite în parte cererile formulată de către inculpatul **BORȘ Simion Toader**, și în consecință, în baza art. 345 al. 2 rap. la art. 282 al. 1-3, al. 4 lit. a Cod de Procedură Penală va constata nulitatea relativă parțială a următoarelor probe, urmând ca acestea să fie excluse în măsura în care conțin interceptări ale unor comunicări efectuate de inculpat, prin sistem informatic, aferente adreselor de e-mail _____

_____, anterior datei de 14.03.2014, dată începând cu care a fost autorizată măsura supravegherii tehnice a interceptării comunicărilor efectuate de către inculpat prin intermediul sistemelor informatice, potrivit încheierii penale nr. 53/2014, pronunțată în dosarul nr. 1450/117/2014, și în baza căreia au fost emise mandatele de interceptate nr. 69/UP/2014 și 70/UP/2014, aici interesând mandatul 69/UP/2014, respectiv procesul verbal existent la fila 265, procesul verbal existent la fila 266 din vol. II, procesul verbal existent la filele 214-215 din vol. III, procesul verbal existent la filele 192-199 din vol. III și procesul verbal existent la filele 200-213 din vol. III, precum și actele subsecvente acestora.

Va dispune comunicarea prezentei încheieri Parchetului de pe lângă Înalta Curte de Casație și Justiție – Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism – Serviciul Teritorial Cluj, în vederea remedierii neregularităților constatate în actul de sesizare, procurorul urmând a comunica judecătorului de cameră preliminară dacă menține dispoziția de trimitere în judecată ori solicită restituirea cauzei.

Vor fi respinse toate celelalte cereri și excepții formulate de către inculpatul Borș Simion Toader, prin apărătorul său.

**PENTRU ACESTE MOTIVE,
ÎN NUMELE LEGII,
DISPUNE:**

Admite în parte cererile formulată de către inculpatul **BORȘ SIMION TOADER**,

, în prezent arestat la domiciliul său din , prin apărătorul său și în consecință:

În baza art. 345 al. 2 rap. la art. 282 al. 1-3, al. 4 lit. a Cod de Procedură Penală constată nulitatea relativă parțială a următoarelor probe, urmând ca acestea să fie excluse în măsura în care conțin interceptări ale unor comunicări efectuate de inculpat, prin sistem informatic, aferente adreselor de e-mail

anterior datei de 14.03.2014, dată începând cu care a fost autorizată măsura supravegherii tehnice a interceptării comunicărilor efectuate de către inculpat prin intermediul sistemelor informatice, potrivit încheierii penale nr. 53/2014, pronunțată în dosarul nr. 1450/117/2014, și în baza căreia au fost emise mandatele de interceptate nr. 69/UP/2014 și 70/UP/2014, aici interesând mandatul 69/UP/2014, respectiv procesul verbal existent la fila 265, procesul verbal existent la fila 266 din vol. II, procesul verbal existent la filele 214-215 din vol. III, procesul verbal existent la filele 192-199 din vol. III și procesul verbal existent la filele 200-213 din vol. III, precum și actele subsecvente acestora.

Dispune comunicarea prezentei încheieri Parchetului de pe lângă Înalta Curte de Casație și Justiție – Direcția de Investigare a Infrațiunilor de Criminalitate Organizată și Terorism – Serviciul Teritorial Cluj, în vederea remedierii neregularităților constatate în actul de sesizare, procurorul urmând a comunica judecătorului de cameră preliminară dacă menține dispoziția de trimitere în judecată ori solicită restituirea cauzei.

Respinge celelalte cereri și excepții formulate de către inculpatul Borș Simion Toader, prin apărătorul său.

Definitivă.

Pronunțată în camera de consiliu, azi, 13 ianuarie 2015.

**JUDECĂTOR DE CAMERĂ PRELIMINARĂ,
LIANA ANIȘOARA COCIȘ**

**GREFIER
ALINA BRIE**