PRIVILEGIUL CONTRA AUTOINCRIMINĂRII ȘI CRIPTOGRAFIA

THE PRIVILEGE AGAINST SELF-INCRIMINATION AND CRYPTOGRAPHY

George ZLATI[1]
Avocat – Baroul Cluj

Abstract

In this article the author has analised the relantionship between the privilege against self-incrimination and data encryption. Given the complexity of the subject in question, the author tried an in-depth analysis, using as starting point the European Court of Human Rights case law regarding self-incrimination.

Taken into consideration the reasoning drawn from the various cases brought before the European Court of Human Rights, the author tried to settle the issue regarding the scope of the privilege by reference to different situations such as: compelling a person to hand over the decryption key or to decrypt the information by himself and then to hand over the content in a readable format.

The conclusion was that the privilege against self-incrimination applies also in the context of computer data encryption / decryption. The author also tried to settle the issue regarding the scope of the privilege in the sense that it opposes coercion to active cooperation.

Rezumat

În acest articol autorul a analizat relația existentă între privilegiul contra autoincriminării și criptarea datelor informatice. Având în vedere complexitatea subiectului, acesta a încercat o analiză în profunzime, pornind chiar de la jurisprudența Curții Europene a Drepturilor Omului în materia privilegiului contra autoincriminării.

Având în vedere raționamentele desprinse din diversele cauze aflate pe rolul Curții, autorul a încercat să tranșeze problematica aplicării privilegiului supus analizei raportat la diverse situații concrete, ca de exemplu: atunci când o persoană este constrânsă să transmită cheia de decriptare ori să decripteze în mod nemijlocit informația și să remită ulterior conținutul într-un format lizibil.

Concluzia a fost aceea că privilegiul contra autoincriminării se aplică și contextului criptării / decriptării datelor informatice. De asemenea, autorul a încercat să tranșeze problema sferei de aplicabilitate a privilegiului în sensul că acesta se opune constrângerii la o cooperare activă.

[1] Autorul este avocat colaborator în cadrul SCPA Sergiu Bogdan & Asociații și cadru didactic asociat al Facultății de Drept din cadrul Universității Babeș-Bolyai, Cluj-Napoca, România. Domeniul de cercetare și expertiză al autorului este criminalitatea informatică. E-mail: george.zlati@law-sba.ro / george.zlati@protonmail.com.

CUPRINS

I. INTRODUCERE

În prezentul articol vom analiza câteva aspecte referitoare la criptarea și decriptarea datelor informatice cât și relația existentă între aceste activități și privilegiul contra autoincriminării.[2] Observăm sub acest aspect că **doctrina autohtonă a ignorat cu totul această problemă tehnico-juridică**, motiv pentru care vedem ca fiind necesară și oportună o incursiune doctrinară în acest domeniu. În ceea ce ne privește, ignorarea acestui subiect de către literatura de specialitate este un mare minus, în contextul în care criptarea datelor informatice este utilizată tot mai frecvent. Din moment ce problema juridică există deja, **este posibil în orice moment ca practica judiciară autohtonă să se confrunte cu aceasta**. Or, lipsa unor dezbateri juridice serioase și pertinente poate rezulta în conturarea unei practici judiciare neunitare ori chiar contrară privilegiului contra autoincriminării.

Ca o notă personală, relaţia existentă între privilegiul supus analizei și criptarea datelor informatice a reprezentat timp de ani de zile un subiect de reflecţie personală. Astfel, dincolo de relaţia existentă între privilegiul contra autoincriminării și criptografie, după un studiu aprofundat am putut să conștientizăm cu adevărat **zona gri** în care se află acest privilegiu. În consecinţă, ceea ce ne-am propus a fost de a încerca să facem cât mai multă ordine într-un domeniu în care contradicţiile și frânturile logice reprezintă regula și nicidecum excepţia.[3]

Rămâne de văzut dacă acest articol va deschide drumul unor dezbateri juridice și în doctrina autohtonă.

În ceea ce privește **structura acestui articol**, dincolo de o analiză a privilegiului contra autoincriminării, inclusiv prin raportare la jurisprudența Curții Europene a Drepturilor Omului (în continuare CtEDO sau Curtea) în materie, urmează să ne axăm pe **cinci ipoteze diferite** ale criptării / decriptării și anume:

---

[2] Uneori, în jurisprudența Curții Europene a Drepturilor Omului ori în literatura de specialitate se realizează o disociere între *dreptul la tăcere* și *privilegiul contra autoincriminării.* Chiar dacă s-ar putea realiza o diferențiere, aceasta este mai degrabă una de nuanță și nu vedem nicio relevanță practică în a ne raporta la aceste noțiuni ca la două concepte diferite deși, în esență, acoperă aspecte similare – pentru o opinie similară se poate vedea și R. Chiriță, *Dreptul la tăcere și privilegiul contra autoincriminării*, în „Caiete de drept penal", nr. 4/2006, p. 57, nota de subsol nr. 1. Teza opusă este aceea că privilegiul contra autoincriminării plasează o obligație negativă în sarcina statului și anume aceea de a nu constrânge o persoană să furnizeze probe care ar putea să ducă la incriminarea acesteia, în vreme ce dreptul la tăcere se referă la posibilitatea organelor judiciare de a extrage din tăcerea persoanei concluzii în defavoarea acesteia – vezi în acest sens M. Udroiu, O. Predescu, *Protecția europeană a drepturilor omului și procesul penal român. Tratat*, Ed. C.H. Beck, București, 2008, p. 664. Inclusiv din această perspectivă, nu vedem de ce dreptul la tăcere nu ar reprezenta o componentă a privilegiului contra autoincriminării. Dacă dreptul la tăcere ar viza doar refuzul de a da o declarație și concluziile defavorabile desprinse din acest refuz, înseamnă că refuzul de a remite un document organelor judiciare oferă posibilitatea de a trage concluzii defavorabile deoarece nu ne aflăm în prezența unui refuz de a da declarații. În ceea ce ne privește, în măsura în care cele două noțiuni se întrepătrund ori între acestea se evidențiază o legătură intrinsecă, aceste consecințe absurde sunt înlăturate ori cel puțin atenuate. Pentru o discuție privitoare la aceste două noțiuni se poate vedea și V. Pușcașu, *Prezumția de nevinovăție*, Ed. Universul Juridic, București, 2010, p. 192-193. Autorul concluzionează că dreptul la neautoincriminare (privilegiul contra autoincriminării) este categoria generică, iar dreptul la tăcere este o specie a acestuia, concluzie cu care am putea să fim de acord.

[3] Pentru o monografie nou apărută cu privire la problematica dreptului la tăcere și a privilegiului contra autoincriminării se poate vedea V. Pușcașu, *Dreptul la tăcere și la neautoincriminare*, Ed. Universul Juridic, București, 2015. Deși lucrarea necesită a fi laudată sub aspectul documentării și analizei făcute, se observă faptul că aceasta insistă tot asupra unor probleme deja considerate ca fiind tradiționale în acest domeniu. Astfel, cu toate că nu negăm necesitatea unor asemenea apariții – în vederea clarificării unor aspecte de bază – simțim faptul că ceea ce lipsește este desprinderea la un moment dat de tradițional și ancorarea analizei în chestiuni ce cu siguranță vor deveni extrem de controversate în viitor. Apreciem sub acest aspect că e mai eficient a preîntâmpina anumite controverse ori o practică neunitară la nivelul organelor judiciare decât a încerca soluționarea acestora *post-factum.*

1. atunci când cheia de criptare / decriptare este reprezentată de o parolă care nu se regăsește pe un suport material (aceasta existând doar în memoria unei persoane);

2. atunci când cheia de criptare / decriptare este reprezentată de o parolă ce este imprimată pe un suport material (de exemplu, un înscris de mână);

3. atunci când cheia pentru decriptare este stocată pe un mijloc de stocare a datelor informatice (USB stick, SD card, CD ori DVD etc.);

4. atunci când decriptarea se realizează prin intermediul unor elemente biometrice (de exemplu, urma papilară a utilizatorului sistemului informatic ori vocea acestuia);

5. atunci când se solicită decriptarea nemijlocită a datelor informatice și remiterea acestora într-un format accesibil / lizibil.

II. IMPORTANȚA CRIPTĂRII ȘI A DECRIPTĂRII

Nu dorim să insistăm asupra aspectelor tehnice ce țin de criptarea ori decriptarea datelor informatice, analiza noastră vizând doar aspectele juridice ce țin de aplicabilitatea privilegiului contra autoincriminării în această materie. Atunci când ne vom raporta la anumite aspecte de ordin tehnic o vom face pentru a evidenția anumite elemente ce ar putea avea relevanță din perspectiva analizei juridice.

Cu toate acestea, apreciem totuși ca fiind oportună o incursiune în tematica criptării și decriptării, cel puțin din perspectiva consecințelor pe care le generează în cadrul unei anchete penale.

În primul rând, **în contra opiniei încetățenite în practica judiciară, utilizarea criptografiei nu este un element menit să sugereze *per se* o conduită infracțională.** Atunci când discutăm despre criptarea unor date informatice, **accentul trebuie pus pe *protecția datelor* și nu pe *ascunderea unor comportamente infracționale*.** Aceasta întrucât, protecția datelor informatice poate fi obținută cu succes inclusiv prin intermediul procesului de criptare. Aceasta nu înseamnă că, prin acest proces se urmărește întotdeauna ascunderea conținutului ilicit al datelor respective, conținut ce ar putea sugera o conduită infracțională, ci mai degrabă faptul că se dorește protejarea conținutului față de persoane neautorizate.

Faptul că unele persoane ajung să utilizeze acest proces în vederea ascunderii unor comportamente infracţionale nu reprezintă decât excepția. **Aceste excepții nu ar trebui să ducă la răsturnarea prezumției de nevinovăție prin instaurarea unei prezumţii relative ori absolute în sensul că ceea ce este criptat este și incriminator.** Apreciem că o asemenea prezumție este total lipsită de rezonabilitate, aspect ce ar trebui să atragă o sancţiune din perspectiva dreptului la un proces echitabil.

Criptarea este așadar un mijloc adecvat pentru stocarea datelor informatice într-un mediu securizat. Multe persoane ar putea chiar să folosească criptarea fără să cunoască acest aspect – de exemplu, prin folosirea protocolului **https** (de exemplu, https://www.google.ro) în loc de **http** în momentul accesării unor pagini web. Orice persoană ce ajunge să pună sub semnul întrebării această concluzie trebuie să realizeze faptul că în această eră a tehnologiei, viața privată a fiecărui individ nu este stocată doar în memoria acestuia ori a celor apropiați lui ci și într-o sumedie de sisteme informatice ori mijloace de stocare a datelor informatice. De asemenea, necesită acceptat faptul că nu sunt stocate în format digital doar aspecte legate de viața privată (imagini personale, jurnale etc.), fiind de asemenea notoriu faptul că o analiză atentă asupra mijlocului de stocare a datelor informatice poate rezulta în identificarea unor date precum coduri de acces la diferite platforme ori servicii online (E-mail, magazine virtuale, Internet Banking etc.), generându-se astfel riscul conturării unor pagube patrimoniale semnificative, furturi de identitate, spionaj economic etc.[4]

Nu în ultimul rând, în mediul virtual nu sunt stocate doar date informatice legate de viața privată, fiind des întâlnit ca anumite persoane să stocheze date informatice ce țin de activitatea profesională inclusiv pe sistemele informatice deținute în nume ori interes personal. Este de asemenea posibil ca datele informatice stocate să fie de interes național – de exemplu, în cazul unui administrator ori lichidator judiciar. Pentru protecția acestor date, criptarea este o soluție care nu poate fi ignorată. Altfel, furtul unui sistem informatic ori a unui mijloc de stocare implică nu doar o pierdere patrimonială ci și pierderea controlului asupra unor date informatice importante din perspectiva personală, profesională ori chiar a siguranței naționale.

[4] Vezi și S.M. Oltmann, *Encryption and Incrimination: The Evolving Status of Ecrypted Drives*, în „Bulletin of the Association for Information Science and Technology", nr. 2, vol. 40, 2014, p. 22.

Din acest punct de vedere, **criptarea datelor informatice este benefică oricărui individ ori entități juridice.** Cu titlu de exemplu, în Legea nr. 11/1991 privind combaterea concurenţei neloiale *secretul comercial* este definit în art. 1 ind. 1 lit. b) ca fiind "*informatia care, în totalitate sau în conexarea exactă a elementelor acesteia, nu este în general cunoscută sau nu este ușor accesibilă persoanelor din mediul care se ocupă în mod obișnuit cu acest gen de informație și care dobândește o valoare comercială prin faptul că este secretă,* ***iar deținătorul a luat măsuri rezonabile, ținând seama de circumstanțe, pentru a fi menținută în regim de secret;*** *protecția secretului comercial operează atâta timp cât condițiile enunțate anterior sunt îndeplinite*".

În măsura în care informaţia supusă analizei nu se pliază pe definiţia secretului comercial, infracţiunile prevăzute la art. 5 din Legea nr. 11/1991 nu își pot găsi aplicabilitatea. Definiţia secretului comercial devine așadar elementul central în ceea ce privește sfera de aplicabilitate a textelor de incriminare privitoare la concurența neloială avută în vedere de această lege. Or, așa cum se poate observa, **o condiţie pozitivă pentru calificarea informaţiei ca fiind un secret comercial este ca deţinătorul acesteia să ia măsuri rezonabile, ţinând seama de circumstanţe, pentru a fi menţinută în regim de secret.**

Aceeași problemă poate fi identificată în contextul transmiterii secretelor comerciale prin intermediul unei reţele wireless, fie că aceasta este una securizată ori nesecurizată. Având în vedere posibilitatea interceptării datelor informatice se pune întrebarea în ce măsură deţinătorul secretului comercial are sau nu obligaţia pozitivă de a transmite datele informatice într-un format criptat.

Dincolo de faptul că, la nivel de claritate și previzibilitate, această condiţie pozitivă impusă de legiuitor lasă de dorit, se poate pune problema în ce măsură, în anumite circumstanţe, deţinătorul informaţiei nu ar avea îndatorirea de a utiliza criptarea în vederea menţinerii regimului secret a conţinutului datelor informatice.

Ne putem imagina un exemplu în care secretele comerciale au fost stocate pe sisteme informatice ce urmează a fi înlocuite cu altele mai performante. În măsura în care aceste sisteme ies din sfera de control a deţinătorului secretului comercial se pune problema în ce măsură era necesară criptarea înainte de formatarea partiţiilor existente pe mijloacele de stocare aferente sistemului informatic. În măsura în care se apelează doar la o ștergere logică ori la o formatare este posibilă recuperarea datelor informatice prin mijloace și proceduri tehnice specifice. Apare așadar problema măsurilor rezonabile ce necesitau a fi luate în context pentru păstrarea regimul secret a secretelor comerciale.

Am făcut trimitere la aceste exemple pentru a întări teza conform căreia criptarea este în primul rând un mijloc de protecţie. Observăm chiar faptul că, **în contextul Legii nr. 11/1991, dacă am accepta faptul că în anumite circumstanţe criptarea reprezintă o măsură rezonabilă de protecţie devine *o obligaţie legală*.**

Acceptăm însă faptul că dincolo de aceste aspecte pozitive, criptarea reprezintă de asemenea **un mecanism *anti-forensic*[5] eficient**, susceptibil să îngreuneze o anchetă penală ori chiar să o împiedice întru totul. Având în vedere faptul că procesul de criptare este la îndemâna oricui, fără a fi necesare cunoștințe tehnice avansate, este posibil ca unele persoane să utilizeze acest proces în vederea ascunderii propriei conduite infracționale.

Aceasta este de altfel și **premisa ce sprijină necesitatea unei dezbateri serioase privitoare la posibilitatea obligării / constrângerii unei persoane să decripteze datele informatice pentru ca acestea să fie accesibile organelor judiciare.** Deși există mijloace tehnice prin care se poate depăși acest mecanism de protecție (utilizarea unor atacuri de tip *brute force* ori de tip *dicționar*), acestea sunt în general nefezabile în măsura în care cheia de criptare / decriptare este puternică iar criptarea a fost una de tipul *full disk encryption* (vezi *infra*).[6] În măsura în care procesul de criptare a vizat doar anumite fișiere (*file encryption*), recuperarea conținutului este posibilă prin identificarea unor fragmente din respectivele fișiere într-o formă necriptată (de exemplu, este posibilă crearea unor fișiere temporare care nu sunt supuse procesului de criptare).[7]

---

[5] Conceptul de *anti-forensic*, așa cum sugerează și denumirea, înglobează acele tehnici ori proceduri ce îngreunează ori fac imposibilă activitatea de cercetare, identificare și obținere a urmelor ori a probelor digitale.

[6] S. Lowman, *The Effect of File and Disk Encryption on Computer Forensics*, 2010, p. 7, articol disponibil pe site-ul http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf (ultima accesare în data de 21.09.2015).

[7] A se vedea o analiză în acest sens în E. Casey ș.a., *The growing impact of full disk encryption on digital forensics*, în „Digital Investigation", vol. 8, 2011, p. 129 și urm.

III. CÂTEVA ASPECTE TEHNICE REFERITOARE LA CRIPTARE ȘI DECRIPTARE

Criptarea reprezintă un proces prin care un conținut lizibil (*plaintext*) este transformat prin intermediul unui algoritm de criptare într-unul ilizibil (*cyphertext / codat*). Decriptarea reprezintă mecanismul în sens invers, prin care conținutul ilizibil devine unul lizibil.[8]

Algoritmul de criptare / decriptare are la bază o cheie (*key*) ce se poate regăsi sub forma unei parole, a unui memory stick, urmă papilară etc. De multe ori se utilizează sintagma „*parola pentru decriptare*" în locul sintagmei „*cheia pentru decriptare*". Cu toate acestea, necesită reținut că o astfel de cheie nu este în mod necesar o parolă formată dintr-un șir de caractere, ea putând fi reprezentată inclusiv de un element tangibil (un dispozitiv fizic ori o urmă papilară), vocea persoanei etc.

Fără a insista foarte mult, precizăm faptul că procesul de criptare poate să fie unul *simetric* ori *asimetric*. În cazul *criptării simetrice* există o singură cheie folosită atât pentru criptare, cât și pentru decriptare. Vulnerabilitatea este aceea că, în măsura în care datele informatice trebuie transmise de la o persoană la o altă persoană, ambele persoane trebuie să cunoască această cheie de criptare / decriptare, ceea ce implică uneori necesitatea transmiterii acesteia.

În cazul *criptării asimetrice* discutăm despre un proces mai complex în care există o cheie publică (*public encryption key*) și două chei private – una pentru criptare și alta pentru decriptare. Astfel, expeditorul va cripta datele informatice folosind cheia sa privată pentru criptarea acestora și le va transmite expeditorului împreună cu cheia publică (ce nu este necesar să fie ţinută în secret). Destinatarul, va putea decripta datele informatice folosind cheia sa privată, fără a cunoaște însă și cheia privată a expeditorului. Folosind criptarea asimetrică dispare problema transmiterii cheii pentru criptarea / decriptarea datelor informatice, singura cheie transmisă fiind cea publică. Or, aceasta din urmă nu poate duce *per se* la decriptarea datelor informatice, fiind necesară utilizarea unei chei private care este cunoscută doar de către destinatar. Exemplele folosite în prezentul articol vor viza îndeosebi *criptarea simetrică*, dar concluziile ce urmează a fi conturate rămân valabile și în ceea ce privește criptarea datelor informatice în general.

Problema criptării din perspectiva dreptului penal este aceea că algoritmii moderni de criptare (de exemplu, AES-256) fac nefezabilă decriptarea în lipsa cheii folosite la decriptare.[9] Cu alte cuvinte, fără accesul la cheia pentru decriptare, informația criptată nu va putea fi accesibilă / lizibilă. Mai mult decât atât, informația criptată ajunge să fie – *în principiu* – de nediferențiat față de o succesiune aleatorie de biți[10], aspect ce ridică dificultăți inclusiv la nivelul identificării procesului de criptare. Cu alte cuvinte, dacă nu se cunoaște din alte surse faptul că datele informatice au fost criptate, analiza acestora îl va pune pe specialist în dificultatea de a aprecia în ce măsură datele sunt ori nu criptate.

Datorită importanţei cheii pentru criptarea și decriptarea datelor informatice, **se susține faptul că, de multe ori criptarea este pe atât de puternică pe cât este cheia de decriptare din structura algoritmului de criptare.** De exemplu, în măsura în care această cheie este o parolă cu conținutul „1234", fiabilitatea algoritmului de criptare devine aproape irelevantă. Aceasta deoarece se vor putea utiliza procedee precum *brute force atack* (când se încearcă toate combinaţiile posibile) ori atacuri tip *dicționar* (când se folosesc combinaţii, cuvinte, fraze etc. cunoscute) prin care să se reușească identificarea conținutului cheii de decriptare. În măsura în care parola este formată dintr-un șir lung de caractere (cc. 20-25) relativ aleatorii (pentru a se evita atacurile de tip dicționar), criptarea reprezintă un impediment serios pentru orice entitate care dorește să acceseze conținutul datelor informatice într-un format lizibil / accesibil.[11] Oricum, indiferent de cheia folosită, în măsura în ca algoritmul de criptare este unul vulnerabil, criptarea va putea fi depășită. În contextul actual, un „atac" asupra algoritmilor actuali de criptare (de exemplu, AES 256) este nefezabil, motiv pentru care modalitatea uzuală de a depăși procesul de criptare este reprezentată de un „atac" asupra cheii în baza căreia se realizează criptare / decriptarea.

---

[8] Vezi S. Lowman, *op. cit.*, p. 1.

[9] S. Lowman, *op. cit.*, p. 2; S.M. Oltmann, *op. cit.*, p. 22; D. Terzian, *The Fifth Amendment, Encryption, and the Forgotten State Interest*, în „UCLA Law Review Discourse", vol. 61, 2014, p. 300; N. Soares, *The Right to Remain Encrypted: The Self-Incrimination Doctrine in the Digital Age*, în „American Criminal Law Review", vol. 49, 2012, p. 2008.

[10] S. Lowman, *op. cit.*, p. 1.

[11] D. Terzian, *op. cit.*, p. 302.

Criptarea poate viza date informatice specifice (anumite fișiere text, imagini, fișiere video etc.), **o întreagă partiție** (volum) sau chiar **un întreg mijloc de stocare** (criptarea în întregime a unui hard-disk, a unui CD, a unui memory stick etc.). Criptarea individuală poartă denumirea de *file encryption,* în vreme ce criptarea „globală" poartă denumirea de *full disk encryption* (*FDE*). Acest proces poate avea loc fie **la nivel *software*** (prin utilizarea unor programe informatice specifice – de exemplu BitLocker, TrueCrypt, VeraCrypt etc.), fie **la nivel *hardware*** (de exemplu, modele de hard-disk-uri Hitachi ori Seagate).[12]

După criptarea datelor informatice, **activitatea de percheziționare în mediul informatic în conformitate cu art. 168 C. proc. pen. devine lipsită de obiect.** Obținerea unei copii fidele (clonă / imagine *bit-stream*) după mediul / mijlocul de stocare al datelor informatice, activitate ce necesită a avea loc în mod obligatoriu anterior efectuării precheziției informatice efective, devine irelevantă deoarece copia obținută va avea același conținut ilizibil precum sursa originară a datelor informatice. Or, specialistul desemnat pentru efectuarea percheziției informatice se va afla în imposibilitatea obiectivă de a continua percheziția informatică, procesul de cercetare, identificare și obținere a probelor cu relevanță în cauză fiind imposibil de realizat fără decriptarea datelor informatice. Cu alte cuvinte, **ceea ce este criptat nu poate fi supus procesului de analiză, fiind așadar imposibilă cercetarea, identificarea și obținerea unor urme digitale relevante sub aspect probator.**[13]

IV. IMPORTANȚA DISCUȚIEI PRIVIND APLICATIVITATEA PRIVILEGIULUI CONTRA AUTOINCRIMINĂRII

1. Legislația din Regatul Unit al Marii Britanii și Irlandei

Începând cu anul 2007, **în Regatul Unit constituie infracțiune fapta de a nu oferi autorităților conținutul decriptat al datelor informatice ori cheia pentru decriptarea acestora**, în măsura în care a existat o notificare oficială din partea acestora (a se vedea secțiunea 49-53 din *Regulation of Investigatory Powers* Act[14]). Cadrul normativ ce legitimează practic o **formă de constrângere la cooperare** prin permiterea accesului la conținutul unor informații protejate este extrem de complex, motiv pentru care analiza acestuia nu va face obiectul prezentului articol. Este însă de reținut faptul că acest cadru normativ face **inaplicabil privilegiul contra autoincriminării inclusiv pentru persoanele acuzate în mod oficial de comiterea unei infracțiuni**, motiv pentru care este posibil să apară cât de curând o jurisprudență a CtEDO exact pe acest subiect ce va tranșa problema într-un sens sau altul.

Legislația din Regatul Unit cu privire la acest subiect este extrem de relevantă din două perspective. În primul rând, fenomenul criptării se regăsește îndeosebi în domeniul criminalității informatice, iar aceasta a fost cunoscută ca având un caracter predominant transfrontalier. Este așadar posibil ca un cetățean român să fie supus unei astfel de forme de contrângere la cooperare, fapt ce va pune în discuție aplicabilitatea privilegiului fie pe teritoriul Regatului Unit, fie pe teritoriul României, prin intermediul cooperării judiciare în materie penală.

Nu în ultimul rând, modelul folosit în Regatul Unit ar putea reprezenta la un moment dat o sursă de inspirație pentru legiuitorul național. În măsura în care practica judiciară se va confrunta tot mai des cu această problemă, suntem ferm convinși că se va încerca la un moment dat restrângerea sferei de aplicabilitate a privilegiului contra autoincriminării folosindu-se drept justificare interesul public în contracararea acestui mecanism *anti-forensic* extrem de eficient.

2. Legislația din România

2.1. Din perspectiva dreptului procesual penal

Legiuitorul român nu a avut deocamdată tentația de a urma modelul existent în Regatul Unit, privilegiul contra autoincriminării beneficiind în dreptul intern, cel puțin din punct de vedere formal, de un **nivel sporit de protecție**. Astfel, conform art. 83 lit. a) din C. proc. pen., inculpatul are **dreptul**[15] **de a refuza să dea declarație fără riscul de a suferi vreo consecință defavorabilă ca urmare a acestui refuz.** Din acest punct

[12] Vezi și E. Casey ș.a., *op. cit.*, p. 130.

[13] În legătură cu problema criptării din perspectiva percheziției informatice, a se vedea și G. Zlati, *Percheziția sistemelor informatice și a mijloacelor de stocare a datelor informatice (I)*, în „Caiete de drept penal", nr. 3/2014, p. 27-28.

[14] A se vedea http://www.legislation.gov.uk/ukpga/2000/23/part/III/data.pdf (ultima accesare în data de 20.09.2015).

[15] Conform art. 78 din C. proc. pen., suspectul având exact aceleași drepturi pe care le are și inculpatul.

de vedere, dreptul intern se detașează semnificativ de legislaţia Regatului Unit prin care, odată cu hotărârea CtEDO în cauza *Murray c. Regatul Unit,* a fost legitimată tragerea unor concluzii defavorabile din tăcerea persoanei acuzate dacă împrejurările concrete în care s-a invocat dreptul la tăcere permit acest lucru. În dreptul intern dreptul la tăcere, și implicit privilegiul contra autoincriminării, pare să aibă din acest punct de vedere un **caracter absolut.**

Necesită însă făcute două precizări. În primul rând, art. 83 din C. proc. pen. face trimitere doar la **refuzul de a da declaraţii**, rămânând sub semnul întrebării dacă toate aspectele legate de criptarea / decriptarea datelor informatice sunt acoperite de această prevedere. Dacă dreptul la tăcere se suprapune peste privilegiul contra autoincriminării ori viceversa, poate ar fi fost mai adecvat ca legiuitorul să nu se refere la refuzul de a da declaraţii ci la dreptul la tăcere în ansamblul său. Dacă admitem însă că privilegiul contra autoincriminării este mai larg decât dreptul la tăcere, nu ne rămâne decât să facem aplicare directă a art. 6 din Convenţie acolo unde dreptul intern oferă o protecţie inferioară celei Convenţionale. Dincolo de această posibilitate, necesită totuși remarcat faptul că privilegiul contra autoincriminării nu este cu totul uitat în dreptul intern, art. 99 alin. (2) C. proc. pen. făcând vorbire despre „*dreptul de a nu contribui la propria acuzare*". După cum este lesne de observat, această formulare este una extrem de generoasă ce poate oferi o sferă largă de aplicabilitatea privilegiului supus analizei.

Cu toate acestea, **de prevederile art. 83 și art. 99 alin. (2) C. proc. pen. beneficiază doar suspectul ori inculpatul.** În ceea ce îi privește pe martori, aceștia pot refuza să dea declaraţie doar prin raportare la privilegiul conferit de art. 117 C. proc. pen., ce nu are însă nimic în comun cu privilegiul contra autoincriminării. Acesta este doar *un privilegiu al soțului, ascendenților și descendeților în linie directă, precum și a fraților și surorilor suspectului ori inculpatului.*[16] În literatura de specialitate se vorbește în acest caz despre o protecție de ordin moral, prin trimitere la cauza *Hummer c. Germania*.[17] Cert este faptul că, în vreme ce privilegiul contra autoincriminării derivă din prevederile art. 6 din Convenție, acest privilegiu se află într-o strânsă legătură cu art. 8 din Convenție.[18]

În ceea ce privește art. 118 C. proc. pen., deși acesta poartă o denumire marginală ce se referă la „*dreptul martorului de a nu se acuza*", apreciem că **legislația națională nu permite aplicarea privilegiului contra autoincriminării într-o manieră identică precum în cazul suspectului ori inculpatului.**[19]

În realitate, prin raportare la dispoziţiile din dreptul intern, martorul nu are posibilitatea de a refuza să dea declaraţie prin invocarea privilegiului contra autoincriminării, el beneficiind doar de **o anumită formă de imunitate.** Cu alte cuvinte, martorul este obligat să declare tot ceea ce cunoaște, sub sancţiunea săvârșirii infracţiunii de mărturie mincinoasă, chiar dacă prin declaraţia acestuia se autoincriminează. S-a mers așadar pe ideea că privilegiul contra autoincriminării (*self-incrimnation*) îl protejează doar pe cel care colaborează nu și pe celelalte persoane care urmează să aibă de suferit de pe urma acestei colaborări cu organele judiciare.

În consecință, „dreptul" martorului reprezintă în realitate o obligaţie pozitivă de a colabora cu organele judiciare, ce are drept corelativ obligaţia acestora de a nu utiliza declaraţia împotriva martorului. Doar la o analiză superficială s-ar putea susține însă că martorul beneficiază de același nivel de protecție de care beneficiază suspectul ori inculpatul. Susținem acest lucru deoarece imunitatea de care beneficiază martorul în dreptul intern poartă denumirea de *use immunity*, aceasta implicând doar faptul că **declaraţia nu poate fi**

---

[16] Pentru o discuție în acest sens, a se vedea G. Zlati, *Refuzul concubinului de a da declarație în calitate de martor* – articol disponibil pe site-ul http://www.penalmente.eu/2015/04/09/refuzul-concubinului-de-a-da-declaratie-in-calitate-de-martor/ (ultima accesare la data de 20.09.2015).

[17] A se vedea în acest sens N. Volonciu, A. Vasiliu, R. Gheorghe, *Noul Cod de procedură penală adnotat. Partea generală*, Ed. Universul Juridic, București, 2014, p. 201.

[18] A se vedea și V. Constantinescu, Comentariu în M. Udroiu (coord.), *Codul de procedură penală. Comentariu pe articole*, Ed. C.H. Beck, București, 2015, p. 387-388.

[19] Poate ar fi necesar a se preciza faptul că în Proiectul noului Cod de procedură penală art. 116 stabilea un veritabil drept al martorului de a nu se autoincrimina, fapt ce implica dreptul acestuia de a nu da nicio declarație. Mai mult decât atât, art. 116 alin. (2) stabilea faptul că atunci când organul judiciar constată că prin declarația sa martorul s-ar expune unei investigații penale, acesta are obligația de a-i comunica martorului faptul că în urma acestor declarații se pot declanșa investigații penale împotriva sa și că are dreptul de a nu da nicio declarație cu privire la aspectele care l-ar putea expune unei investigații penale, precum și dreptul de a fi asistat de un avocat. Așadar, este lesne de observat că prevederea actuală este un veritabil regres față de forma inițială.

folosită în mod direct împotriva sa.[20] De exemplu, martorul nu poate fi condamnat prin raportare la cele statuate de acesta în conţinutul declaraţiei de martor (de exemplu: *„da, l-am ajutat pe X să intre în locuinţa părţii vătămate*"). *Per a contrario*, **declaraţia poate fi folosită indirect împotriva martorului prin utilizarea acesteia în vederea obţinerii unor altor mijloace de probă.** De exemplu, martorul declară unde a ascuns arma crimei ori persoanele cu care s-a aflat la locul comiterii infracţiunii, organele de urmărire penală urmând a utiliza aceste informaţii în vederea strângerii de probe (ridicarea armei, audieri persoane etc.).

Astfel, cu toate că declaraţia nu va putea fi folosită împotriva martorului, probele materiale ori declaraţiile celorlalte persoane obţinute ori / și administrate ca urmare a celor consemnate în declaraţia de martor vor putea fi folosite în vederea obţinerii unei soluţii de condamnare. Este discutabil inclusiv în ce măsură art. 102 alin. (4) C. proc. pen. și-ar putea găsi aplicabilitatea în acest context din moment ce art. 118 C. proc. pen. legitimează o anumită formă de constrângere.

În dreptul intern nu se recunoaște așadar imunitatea derivativă (*derivative-use immunity*) în contextul autoincriminării martorilor[21]**, ceea ce pune în discuţie din punctul nostru de vedere conformitatea dreptului intern cu jurisprudenţa CtEDO în materie.**[22] Sub acest aspect, deosebit de importante sunt cauzele *Shabelnik c. Ucraina* (parag. 57 din hot.) și *Loutsenko c. Ucraina* (parag. 50 și urm. din hot.), unde CtEDO a criticat poziția vulnerabilă a martorilor aflați în situația de a fi constrânși să declare tot ceea ce cunosc chiar cu riscul de a se autoincrimina.[23]

Una este ca declaraţia martorului ori probele obţinute indirect prin declaraţia acestuia să fie folosite împotriva altor persoane și alta este ca martorul să fie contrâns să colaboreze cu organele judiciare inclusiv în situaţia în care există riscul de a se incrimina indirect prin declaraţia dată. Ar necesita a fi menționat, că inclusiv această ipoteză a fost criticată de CtEDO în cauza *Loutsenko c.* Ucraina (parag. 51 din hot.).[24] Oferirea unei imunităţi veritabile nu ar avea decât efectul de a-l plasa pe martor în postura de a beneficia de o protecţie similară celei conferite de privilegiul contra autoincriminării.

Având așadar în vedere existenţa unei imunităţi parţiale (*use immunity*), opinăm în sensul că **martorul va putea invoca privilegiul contra autoincriminării raportat la prevederile art. 6 din Convenţie, refuzând să dea declaraţie atunci când există riscul de a se autoincrimina – fie direct, fie indirect.**[25] Este adevărat faptul că, procedând astfel, acesta se supune riscului de a răspunde penal prin raportare la infracțiunea de mărturie mincinoasă (art. 273 Cod pen.) ori obstrucționare a justiției (art. 271 Cod pen.). Diferența este aceea că, în ceea ce ne privește, textul de la mărturie mincinoasă devine incident **doar după** ce persoana a dobândit calitatea de martor **și** a depus jurământul prevăzut de lege. Fără depunerea acestui jurământ, nu pot fi adresate întrebări, motiv pentru care nu se poate identifica o acțiune ori omisiune care să se plieze pe latura obiectivă a infracțiunii. În acest sens, necesită observat faptul că **martorul trebuie să fie întrebat** iar declarația sa trebuie **să atingă împrejurări esențiale cauzei** cu privire la care a fost întrebat. Prin urmare, în lipsa unor întrebări ce necesită răspuns, datorită faptului că se refuză depunerea jurământului ori chiar prezența în fața organelor judiciare, este imposibil să discutăm despre potențialitatea îndeplinirii elementelor constitutive ale infracțiunii. În acest context, singura posibilitate este de a face aplicare textului de incriminare prev. la art. 271 Cod pen. Pentru aceasta, este însă necesar să se realizeze o avertizare oficială cu privire la consecințele faptului de a refuza să se prezinte ori de a depune jurământul cerut de lege. În lipsa acestei notificări, inclusiv infracțiunea prev. de art. 271 Cod pen. devine inaplicabilă. În literatura de specialitate s-a susţinut faptul că martorul are dreptul de

---

[20] M. Redmayne, *op. cit.,* p. 212.

[21] A se vedea în acest sens *Kastigar c. US (1972)* citată în M. Berger, *Self-incrimination and the European Court of Human Rights: Procedural Issues in the Enforcement of the Right to Silence*, în „European Human Rights Law Review", nr. 5, 2007, p. 521.

[22] Ar fi de menționat faptul că în dreptul australian ori cel american există o astfel de imunitate derivativă. De asemenea, deși în dreptul canadian există o prevedere similară celei din dreptul intern, jurisprudența a extins protecția martorilor înspre o imunitate derivativă. Mai multe detalii în A. Choo, *The Privilege against self-incrimination and Criminal Justice*, Hart Publishing, Oxford, 2013, p. 63 și urm.

[23] A se vedea în acest sens și V. Pușcașu, *Dreptul la tăcere... precit.*, p. 144 și urm.

[24] Este adevărat că în această cauză CtEDO a ținut cont de împrejurările concrete ale cauzei. Cu toate acestea, în ceea ce ne privește, prin hot. dată CtEDO a statuat implict faptul că încălcarea privilegiului contra autoincriminării nu este necesar a fi invocată neapărat de către persoana ce a făcut obiectul constrângerii la cooperare.

[25] Pentru o opinie similară, a se vedea V. Constantinescu, Comentariu în M. Udroiu, *Codul de procedură... precit.*, p. 392-393. A se vedea și V. Pușcașu, *Dreptul la tăcere..., precit.*, p. 149-150.

a nu se autoincrimina, însă nu prin raportare la prevederile Convenţiei, ci printr-o interpretare eronată – *din punctul nostru de vedere* – a art. 118 C. proc. pen..[26]

S-a mai susținut că prevederile art. 118 C. proc. pen. sunt în acord cu jurisprudența CtEDO (cauza *Serves c. Franța*),[27] fapt cu care nu suntem de acord, din moment ce **în cauza citată Curtea a insistat pe ideea că martorul nu are dreptul de a refuza să depună jurământul în calitate de martor dar ulterior depunerii acestuia are dreptul de a refuza să participe la propria incriminare** (a se vedea analiza de la parag. 47 din hotărâre).[28]

O opinie mai nuanțată este aceea că art. 118 C. proc. pen. nu reprezintă decât o garanție pe care legea o conferă martorului cu privire la eventuala punere sub acuzare, aceasta fiind catalogată ca fiind o veritabilă alternativă la situația în care suspectul ori inculpatul are dreptul de a păstra tăcerea.[29] Deși suntem de acord că suntem în prezența unei garanții ce ia forma unei imunități, rămâne de văzut în ce măsură aceasta este suficientă din perspectiva respectării prevederilor art. 6 din Convenție. Ne este totuși greu să acceptăm că o asemenea garanţie este o **veritabilă alternativă** la situaţia în care suspectul ori inculpatul are dreptul de a păstra tăcerea. Căci tăcerea nu poate fi întoarsă împotriva acestora, în vreme ce declaraţia poate fi utilizată în mod indirect în vederea obţinerii unei soluţii de condamnare.

În consecinţă, este rezonabil a conchide faptul că **imunitatea conferită martorilor nu reprezintă o garanție suficientă deoarece aceștia pot ajunge să contribuie indirect la propria lor incriminare.**[30] Nu putem decât să ne întrebăm în context care este diferența între a participa direct ori indirect la propria ta incriminare atâta vreme cât, în esență, organele judiciare ajung să folosească – *într-o formă sau alta* – declarația luată ca urmare a unei constrângeri la cooperare împotriva ta? Dacă de esenţa privilegiului contra autoincriminării este inclusiv respectarea prezumţiei de nevinovăţie, ce implică faptul că organele de urmărire penale sunt cele care trebuie să probeze vinovăţia persoanei acuzate și nu aceasta din urmă, constrângerea la o autoincriminare indirectă nu duce decât la ignorarea acestei raţiuni.

Aplicabilitatea directă a art. 6 din Convenţie ar putea duce la acoperirea lacunelor art. 118 C. proc. pen. și oferirea cadrului legal în vederea aplicării sancţiunii prevăzute de art. 102 alin. (4) C. proc. pen., fapt ce ar produce efecte similare cu cele ale imunităţii derivative.

2.2.Din perspectiva dreptului penal substanţial

În context, relevantă este infracțiunea de obstrucționare a justiției prevăzută la art. 271 Cod pen. Astfel, deși alin. 2 al art. 271 Cod pen. exclude din sfera subiecților activi persoanele urmărite sau judecate pentru infracțiunea care formează obiectul procesului penal se pune problema în ce măsură art. 271 alin. 1 lit. b) Cod pen. își poate găsi aplicabilitatea în ceea ce îi privește pe martori.

De exemplu, se efectuează o percheziție informatică asupra unui mijloc de stocare în vederea identificării unor materiale pornografice cu minori, dar se observă faptul că datele informatice sunt criptate iar suspectul refuză să comunice cheia pentru decriptarea acestora. Având în vedere acest aspect, organele de urmărire penală

---

[26] A se vedea în acest sens M. Oprea, *Infracțiuni contra înfăptuirii justiției*, Ed. Universul Juridic, București, 2015, p. 213. Autorul susține că martorul nu va putea răspunde pentru infracțiunea prevăzută de art. 271 Cod pen. (obstrucționarea justiției) decât în situația în care i se solicită predarea unor obiecte, raportat la privilegiul contra autoincriminării desprins din prevederile art. 118 C. proc. pen.. Dincolo de faptul că suntem de părere că predarea unor obiecte poate avea la bază o constrângere la cooperare, ce poate pune în discuție aplicabilitatea privilegiului, suntem de părere că deși autorul a ajuns parțial la o soluție corectă trimiterea făcută la art. 118 C. proc. pen. este eronată având în vedere natura acestei garanții procesuale.

[27] C. Voicu, A.S. Uzlău, G. Tudor, V. Văduva, *Noul Cod de procedură penală. Ghid de aplicare pentru practicieni*, Ed. Hamangiu, București, 2014, p. 97.

[28] A se vedea în acest sens și R. Chiriță, *op. cit.*, p. 69. Achiesăm punctului de vedere al autorului cu privire la faptul că a obliga un martor să depună jurământul deși riscul autoincriminării ulterioare depunerii acestuia este evident este criticabil. Pe de altă parte, nu este exclusă probabilitatea ca martorul să nu fie întrebat în legătură cu aspectele ce-l pot incrimina, acesta având practic dreptul de a refuza să răspundă doar cu privire la aceste aspecte. Ca o notă personală, în practica judiciară s-a putut identifica o asemenea abordare, procurorul de caz aducând la cunoștința martorului dreptului acestuia de nu a se autoincrimina cu privire la anumite aspecte punctuale, atrăgându-i atenția asupra faptului că, în ceea ce privește restul aspectelor, are obligația de a da declarație sub sancțiunea răspunderii pentru infracțiunea de mărturie mincinoasă. În ceea ce ne privește, o asemenea interpretare a privilegiului contra autoincriminării este în spiritul art. 6 din Convenție – a se vedea în acest sens și M. Berger, *Self-Incrimination and the European Court of Human Rights... precit.*, p. 520-521.

[29] N. Volonciu, A. Vasiliu, R. Gheorghe, *Noul Cod de procedură..., precit.*, p. 202.

[30] Vezi și V. Constantinescu, Comentariu în M. Udroiu, *Codul de procedură... precit.*, p. 392-393.

află că și administratorul de rețea – *martor în cauză* – are cunoștință despre cheia folosită pentru decriptarea datelor informatice. În măsura în care acesta nu are nicio implicare în activitatea infracțională a suspectului, va avea obligația de a răspunde solicitării oficiale de remitere a cheii respective, sub sancțiunea răspunderii pentru infracțiunea de obstrucționare a justiției.

Discuția se complică însă în ipoteza în care administratorul de rețea cunoaște faptul că, în realitate, el era cel care stoca materiale pornografice pe respectivul sistem informatic iar identificarea lor ar putea proba vinovăția acestuia – existând de exemplu posibilitatea asocierii datelor informatice cu contul de administrator ori prin accesarea datelor informatice se poate observa că martorul a fost cel care a filmat raporturile sale sexuale cu diferiți minori.

În doctrină,[31] **s-a susținut pe bună dreptate că un martor nu va putea răspunde pentru infracțiunea de obstrucționare a justiției dacă ulterior a dobândit calitatea de suspect în aceeași cauză, în baza unei interpretări a sintagmei „persoană urmărită".**

Ipoteza problematică este însă aceea în care martorul nu ajunge suspect ori inculpat în respectiva cauză, tocmai datorită faptului că nu permite organelor de urmărire penală să aibă acces la conținutul datelor informatice. Întrebarea care se pune în context este următoarea: ce va prevala, textul de la obstrucționarea justiției ori privilegiul contra autoincriminării? Dacă singurul element care îl poate incrimina depinde de cooperarea acestuia ne pare cu totul lipsit de logică a nu ţine cont de privilegiul contra autoincriminării. De ce ar trebui să devină privilegiul aplicabil doar după ce administratorul de reţea acceptă să coopereze – *constrâns fiind* – și devine suspect ca urmare a identificării materialelor pornografice printre datele decriptate? După acest moment, privilegiul contra autoincriminării ar fi lipsit de conţinut din moment ce, după obţinerea datelor într-un format accesibil / lizibil cooperarea acestuia nu va mai mai necesară din perspectivă probatorie. În acest context, **privilegiul contra autoincriminării ar deveni iluzoriu.**

Necesită făcută totuși o distincţie între ipoteza în care suspectul refuză să coopereze în baza privilegiului contra autoincriminării iar organele de urmărire penală descoperă faptul că martorul cunoaște de asemenea cheia pentru decriptarea datelor informatice și ipoteza în care suspectul afirmă faptul că doar martorul avea acces la respectivul sistem informatic, acesta fiind singura persoană care poate decripta datele informatice. În acest ultim caz, apreciem că martorul ajunge să fie afectat în mod semnificativ, fiind dincolo de orice dubiu că privilegiul contra autoincriminării devine aplicabil. Relevantă în acest context ar putea fi chiar cauza *Brosco c. Franța*.[32]

În literatura de specialitate,[33] raportat la Codul de procedură penală anterior, s-a apreciat faptul că, inclusiv martorul *de facto* – persoana chemată să dea declarație în faza actelor premergătoare și față de care nu există o acuzație în materie penală – putea să invoce privilegiul contra autoincriminării. În ceea ce ne privește, nu putem decât să achiesăm unui asemenea punct de vedere, apreciind că o soluție contrară s-ar plasa într-un raport conflictual cu prezumția de nevinovăție.

Revenind la discuția privitoare la infracțiunea de obstrucționare a justiției, se poate observa faptul că textul de la alin. (2) al art. 271 Cod pen. este unul restrictiv, în sensul că, dispozițiile de la alin. (1) nu se aplică decât persoanei urmărite ori judecate **pentru infracțiunea care formează obiectul procesului penal.**

Per a contrario, s-ar putea susține ideea conform căreia, într-un dosar de corupție, suspectul ori inculpatul ar putea fi obligat să ofere cheia pentru decriptarea datelor informatice deși există riscul ca organele de urmărire penală să descopere pornografie infantilă pe mijlocul de stocare al acestuia. În măsura în care persoana supusă avertismentului prevăzut de art. 271 Cod pen. este cercetată într-un dosar distinct inclusiv pentru infracțiunea de pornografie infantilă, discuția juridică devine cu atât mai relevantă.

Este adevărat faptul că legiuitorul putea să fie mai inspirat la momentul redactării acestui text de incriminare, oferind o clauză mai generoasă de impunitate, susceptibilă să acopere astfel și aceste situații. Cu toate acestea, este evident faptul că **alin. (2) al art. 271 Cod pen. are ca rațiune respectarea privilegiului contra autoincriminării**[34], motiv pentru care este suficient să clarificăm incidența acestui privilegiu în situații

---

[31] G. Bodoroncea, Comentariu în G. Bodoroncea, V. Cioclei, I. Kuglay ș.a., *Codul penal. Comentariu pe articole*, Ed. C.H. Beck. București, 2014, p. 271, parag. 5.

[32] A se vederea și analiza din V. Pușcașu, *Dreptul la tăcere..., precit.*, p. 147 și urm.

[33] V. Pușcașu, *Prezumția de nevinovăție... op. cit.*, 2010, p. 189.

[34] A se vedea în acest sens S. Bogdan, D.A. Șerban, G. Zlati, *Noul Cod penal. Partea specială*, Ed. Universul Juridic, București,

de acest tip pentru a ajunge la concluzia conform căreia răspunderea penală în caz de necooperare este exclusă *de plano*.

V. PRIVILEGIUL CONTRA AUTOINCRIMINĂRII RAPORTAT LA JURISPRUDENȚA CURȚII EUROPENE A DREPTURILOR OMULUI

Privilegiul contra autoincriminării este apreciat în literatura de specialitate ca fiind unul lipsit de claritate.[35] În esență, acesta instituie anumite restricții în ceea ce privește ancheta penală prin faptul că o persoană are posibilitatea de a nu oferi organelor judiciare informațiile solicitate și care ar putea fi folosite împotriva sa.[36] Cu toate acestea, la o analiză atentă a acestui privilegiu – inclusiv raportat la jurisprudența CtEDO în materie – se observă faptul că la nivel de conținut și implicit la nivelul sferei de aplicabilitate, lucrurile nu sunt întru totul clare.

Faptul că respectarea acestui privilegiu a devenit o cerință implicită în vederea respectării dreptului la un proces echitabil (articolul 6 din Convenție) din perspectiva jurisprudenței CtEDO este lipsit de orice controversă – a se vedea în acest sens cauza *Funke c. Franța, Saunders c. Regatul Unit* etc. O asemenea concluzie este lipsită de importanță dacă aplicabilitatea efectivă a privilegiului întâmpină probleme.

1. Rațiunea privilegiului contra autoincriminării

În ceea ce ne privește, analiza privitoare la sfera de aplicabilitate a privilegiului ar trebui să aibă ca premisă **identificarea exactă a rațiunii pentru care privilegiul în cauză este o componentă importantă a dreptului la un proces echitabil.**[37]

Or, observăm că inclusiv sub acest aspect, Curtea nu a reușit să tranșeze problema iar în literatura de specialitate opiniile sunt cât se poate de divergente.[38] De exemplu, deși CtEDO a introdus privilegiul contra autoincriminării în conținutul dreptului la un proces echitabil prin cauza *Funke c. Franța*[39], nu s-a făcut vreo precizare referitoare la întinderea privilegiului, originea ori rațiunea acestuia.[40] Această lipsă la nivel argumentativ este criticabilă cu atât mai mult cu cât în *cauza Funke* s-a constatat încălcarea art. 6 din Convenție deși **constrângerea la cooperare a vizat predarea unor documente bancare**, ipoteză ce necesita din punctul nostru de vedere o analiză mai amplă din care să rezulte clar raționamentul în baza căruia s-a ajuns la respectiva soluție.

Dacă privilegiul contra autoincriminării vizează strict **buna înfăptuire a justiției și aflarea adevărului prin prevenirea erorilor judiciare** (eroarea judiciară fiind, de exemplu, menționată în cauza *John Murray c. Regatul Unit* – parag. 49 din hot.), la prima vedere, s-ar putea susține faptul că obligarea unei persoane să ofere cheia pentru decriptare datelor informatice autorităților ori să realizeze ea însăși acțiunea de decriptare nu aduce atingere acestui privilegiu. Astfel, dacă în materia declarațiilor luate cu încălcarea acestui privilegiu se poate pune în discuție fiabilitatea acestora ca urmare a exercitării constrângerii, în materia decriptării datelor informatice situația diferă în mod considerabil. Aceasta întrucât, **spre deosebire de declarațiile date în fața organelor judiciare, conținutul datelor informatice este preexistent momentului constrângerii.** Sub acest aspect, obligația de remitere a unor documente se aseamănă cu obligația de a decripta ori de a oferi cheia pentru decriptarea datelor informatice.

Astfel, s-ar putea susține că există un element obiectiv susceptibil să ateste dincolo de orice dubiu că aflarea adevărului și implicit buna înfăptuire a justiției nu este afectată.

În ceea ce ne privește, deși privilegiul contra autoincriminării este menit să protejeze inclusiv credibilitatea mijlocului de probă obținut, aspect ce vizează prevenirea erorilor judiciare, raținea privilegiului supus analizei

---

2014, p. 345.

[35] M. Redmayne, *Rethinking the Priviledge Against Self-Incrimination*, în „Oxford Journals of Legal Studies", vol. 27, nr. 2, 2007, p. 209.

[36] Ibidem.

[37] Aceeași opinie în V. Pușcașu, *Prezumția de nevinovăție... op. cit., p. 195.*

[38] Pentru o analiză sumară a acestei chestiuni în literatura de specialitate autohtonă, se poate vedea R. Chiriță, *op. cit.*, p. 58 și urm.

[39] **Starea de fapt:** autoritățile vamale i-au solicitat lui Funke s-a remită documente referitoarele la conturile sale bancare din ultimii trei ani. Pentru refuzul său de a coopera a fost condamnat la plata unor amenzi.

[40] Vezi și A. Ashworth, *Self-Incrimination in European Human Rights Law – A Pregnant Pragmatism?,* în „Cardozo Law Review", vol. 30, 2008-2009, p. 753.

nu este / nu poate fi doar aceasta. Obţinerea unei declaraţii, prin utilizarea unor mijloace coercitive, ce rezultă în autoincriminarea persoanei asupra căreia este exercitată constrângerea ar trebui să fie considerată *de plano* ca fiind incompatibilă cu dreptul la un proces echitabil. Astfel, în cauza *Saunders c. Regatul Unit,*[41] Curtea a statuat la nivel de principiu că **privilegiul contra autoincriminării se află într-o strânsă legătură cu prezumția de nevinovăție**,[42] motiv pentru care este necesar ca acuzarea să își contruiască acuzația în materie penală fără a se folosi de probe obținute ca urmare a unor mijloace coercitive ori opresive. Exact aceeași concluzie se regăsește și în parag. 60 din cauza *Marttinen c. Finlanda*.

Tocmai de aceea, apreciem ca fiind irelevant faptul că declaraţia oferită este una în conformitate cu realitatea obiectivă ori una falsă, necorespunzătoare adevărului. În opinia noastră, **relevant este doar mijlocul prin care această declarație a fost obţinută – dacă acest mijloc implică o formă de constrângere la cooperare din partea unei persoane, privilegiul trebuie să își găsească aplicabilitatea.**

Cu toate acestea, având în vedere faptul că privilegiul contra autoincriminării a dobândit faima de care se bucură în prezent inclusiv datorită faptului că acesta are scopul de a proteja buna înfăptuire a justiţiei prin constituirea unei piedici în ceea ce privește posibilitatea organelor judiciare de a denatura adevărul, apreciem ca fiind necesar a puncta în legătură cu un anumit aspect inclusiv raportat la această chestiune.

Astfel, **deși datele informatice – posibil incriminatorii – nu suferă modificări ca urmare a autoincriminării prin transmiterea cheii pentru decriptare ori a decriptării acestora în mod nemijlocit, aceasta nu înseamnă că aflarea adevărului nu poate avea de suferit.** Să presupunem că o persoană este cercetată pentru comiterea infracţiunii de pornografie infantilă, existând în acest sens indicii conform căreia pe sistemul informatic aparținând acesteia sunt stocate materiale pornografice cu minori.

În măsura în care sistemul informatic este criptat iar autorităţile nu au acces la datele informatice, în lipsa unor alte elemente care să probeze dincolo de orice dubiu rezonabil existenţa elementelor constitutive ale infracţiunii și vinovăţia persoanei suspectate, tragerea acesteia la răspundere penală va fi improbabilă. În context, este evident faptul că datele informatice potenţial incriminatorii nu vor putea constitui probe în acuzare decât în măsura în care acestea urmează a fi decriptate.

Să presupunem însă că, deși există astfel de materiale cu conţinut pornografic pe sistemul informatic aparţinând suspectului, acesta nu se face vinovat de comiterea infracţiunii de pornografie infantilă deoarece o terţă persoană a „plantat" respectivele date informatice pe sistemul acestuia ori acestea au fost copiate din culpă de către agent. În măsura în care suspectului îi este cerută cheia pentru decriptarea datelor informatice, iar acesta, deși cunoaște faptul că este nevinovat, conștientizează riscul ca pe sistemul său să existe astfel de materiale pornografice, se pune întrebarea în ce măsură mai există ori nu posibilitatea concretă ca aflarea adevărului să aibă de suferit ca urmare a decriptării datelor informatice.

În cele din urmă, luarea unei declarații prin intermediul unor mijloace coercitive în sensul că suspectul s-a aflat la locul comiterii faptei poate afecta principiul aflării adevărului inclusiv în situația în care această împrejurare corespunde realității, în măsura în care stabilirea acestui fapt generează o prezumție – *chiar și relativă* – în sensul că această persoană este cea care a comis infracțiunea. **Dacă persoana acuzată este pusă în situaţia de a fi nevoită să răstoarne o prezumţie formată ca urmare a constrângerii la colaborare, se creează un dezechilibru pe care îl vedem ca fiind cu totul problematic din perspectiva dreptului la un proces echitabil.** În această situație, deși constrângerea nu a dus la o declarație care nu corespunde adevărului, modul în care este utilizată / interpretată aduce atingere acestui principiu.

În concluzie, dreptul intern prezintă unele garanţii suplimentare prin raportare la Convenţie, motiv pentru care orice concluzie în defavoarea suspectului ori inculpatului, pornind de la tăcerea acestuia este strict interzisă. Pe de altă parte, rămâne discutabil în ce măsură art. 99 alin. (2) C. proc. pen. completează prevederile art. 83 C. proc. pen.. În măsura în care în dreptul intern este recunoscut strict dreptul de a nu da declaraţii, privilegiul contra auto incriminării necesită a-și găsi aplicabilitatea, în plenitudinea sa, prin aplicare directă a

[41] **Starea de fapt:** Saunders a fost obligat să participe la o serie de interviuri în fața inspectorilor numiți de către Departamentul de Comerțului și Industriei în baza secțiunii 434 și 436 din Companies Act 1985, în caz de refuz existând riscul de a răspunde pentru *contempt of court*. Sauders a cooperat cu inspectorii, iar cele declarate de către acesta au fost folosite într-o procedură penală împotriva sa ce a rezultat într-o condamnare pentru săvârșirea mai multor infracțiuni.

[42] Aceeași opinie în P. Mahoney, *Right to a Fair Trial in Criminal Matters Under Article 6 E.C.H.R.*, în „Judicial Studies Institute Journal", vol. 4, nr. 2, 2004, p. 121; R. Chiriță, *op. cit.*, p. 60, parag. 6.

art. 6 din Convenţie. Apreciem însă că o interpretare rezonabilă a prevederilor art. 99 alin. (2) C. proc. pen. pot oferi o sferă adecvată de aplicabilitate privilegiului. În acest sens, nu discutăm neapărat despre o restrângere a privilegiului contra autoincriminării în dreptul intern, prin raportare la dispoziţiile Codului de procedură penală, ci mai degrabă este necesitatea interpretării adecvate a acestora.

În ceea ce îi privește pe martori, concluzia este una diferită. Astfel, spre deosebire de suspecţi ori inculpaţi, martorii nu beneficiază de privilegiul contra autoincriminării. Aceștia sunt obligaţi să coopereze cu organele judiciare sub sancţiunea răspunderii pentru infracţiunea de mărturie mincinoasă ori obstrucţionare a justiţiei. Beneficiul lor este acela că declaraţia – și doar aceasta – nu poate fi utilizată în mod direct în ipoteza în care survin modificări în ceea ce privește calitatea procesuală. Din acest punct de vedere, dreptul intern poate fi invalidat prin aplicarea directă a art. 6 din Convenţie.

De *lege ferenda* ar fi necesară o reformă în ceea ce privește garanţiile conferite martorilor. Un punct de plecare ar putea fi chiar art. 116 din Proiectul noului Cod de procedură penală. Martorul trebuie fie să beneficieze de o imunitate derivativă, fie să aibă opţiunea de a invoca privilegiul contra autoincriminării în condiţii identice cu suspectul ori inculpatul. De asemenea, atunci când riscul de a se autoincrimina apare ca fiind evident, autorităţile judiciare ar trebui să aibă obligaţia de a informa martorul cu privire la opţiunile pe care acesta le are la dispoziţie.

2. Procedurile în care este aplicabil privilegiul contra autoincriminării

Este dincolo de orice îndoială faptul că în cazul unei **proceduri penale** privilegiul contra autoincriminării își poate găsi aplicabilitatea, discuția fiind doar care este conținutul și întinderea acestuia.

În *cauza Saunders*, constrângerea la cooperare a avut loc în cadrul unei **proceduri considerate ca având o natură administrativă**[43], motiv pentru care Curtea a apreciat faptul că reclamantul era obligat să colaboreze cu autoritățile.[44] Cu toate acestea, **folosirea ulterioară a informațiilor obținute ca urmare a constrângerii într-un proces penal readuce în discuție respectarea privilegiului contra autoincriminării.** Astfel, dacă în *cauza Saunders* ar fi existat un refuz în ceea ce privește cooperarea cu autoritățile, condamnarea reclamantului pentru acest refuz (în speță, *contempt of court*) nu ar fi dus la încălcarea privilegiului contra autoincriminării deoarece prodcedura în cauză a fost apreciată ca fiind una pur administrativă.[45]

Rezultă așadar că reclamantul trebuia să beneficieze de imunitate cu privire la informațiile obținute în cadrul procedurii administrative, acestea neputând fi folosite împotriva sa într-un proces penal. **Folosirea acestora într-un asemenea proces a dus la activarea privilegiului contra autoincriminării**, Curtea constatând faptul că administrarea în procesul penal a unor declarații obținute ca urmare a unor mijloace coercitive contravine art. 6 din Convenție.

Acest punct de vedere a fost evidențiat mult mai clar în cauza *IJL, GMR și AKP c. Regatul* Unit (a se vedea parag. 100-101 din hot.), reclamanții fiind celelalte persoane acuzate din procesul domnului Saunders (vezi *supra*). Curtea a statuat faptul că nu obținerea informațiilor ca urmare a constrângerii atrage încălcarea art. 6 din Convenție ci folosirea ulterioară a acestora într-un proces penal.

Elementul esențial este așadar de a identifica natura procedurii prin raportare la momentul în care prevederile art. 6 din Convenție devin aplicabile. Atunci când constrângerea la cooperare face obiectul unei investigații mai degrabă de natură penală decât administrativă, încălcarea privilegiului contra autoincriminării se realizează de la momentul obținerii declarației ca urmare a constrângerii, chiar dacă aceasta are loc în fazele incipiente ale procedurii (*cauza Heaney și McGuiness c. Irlanda*[46]).

---

[43] A se vedea și cauzele *Abas c. Olanda*, *Allen c. Regatul Unit* și *King c. Regatul Unit*. În toate aceste cauze s-a constatat faptul că art. 6 din Convenție nu a fost încălcat. Totuși, în *cauza King* se poate susține faptul că reclamantul nu a fost condamnat pentru refuzul la cooperare ci pentru faptul că nu și-a îndeplinit obligațiile fiscale în ceea ce privește declararea veniturilor. Apreciem că această nuanță este extrem de importantă.

[44] Este totuși important de menționat că într-o opinie concurentă, judecătorul Morenilla a statuat că art. 6 din Convenție a fost încălcat încă de la început, indiferent de modalitatea în care au fost utilizate ulterior declarațiile luate ca efect a constrângerii exercitate.

[45] A se vedea și cauza *Kansal c. Regatul Unit* ce a vizat o procedură a falimentului în care Kansal a fost obligat să declare anumite aspecte ce au fost utilizate împotriva sa într-o procedură penală ulterioară.

[46] **Starea de fapt:** reclamanții au fost suspectați de săvârșirea unor infracțiuni de terorism, motiv pentru care au fost arestați și interogați în legătură cu locul în care se aflau la momentul comiterii infracțiunilor. Pentru refuzul de a coopera cu organele judiciare au fost condamnați la câte 6 luni de închisoare.

În ceea ce ne privește, **inclusiv în cadrul urmăririi penale *in rem*, „făptuitorul" poate invoca privilegiul contra autoincriminării deși formal nu are calitatea de suspect ori inculpat.** Sub acest aspect, apreciem ca fiind profund criticabilă reforma adusă prin C. proc. pen.. Astfel, prin renunțarea la actele premergătoare s-a dorit evitarea derapajelor prin care se obțineau probe în afara procesului penal. Cu toate acestea, în prezent, organele de urmărire penală au posibilitatea de a administra probatoriul în cursul urmăririi penale *in rem* în încercarea de a lipsi de orice fel de garanții procesuale persoana care urmează să dobândească ulterior calitatea de suspect în cauză. O asemenea abordare nu poate fi decât o reformă superficială care să îngreuneze și mai mult posibilitatea de a invoca în camera preliminară încălcarea dreptului la un proces echitabil.

Identificarea naturii investigației în cadrul căreia s-a exercitat o formă de constrângere la cooperare reprezintă de asemenea un subiect delicat. De exemplu, în *cauza Shannon c. Regatul Unit*, Curtea a constatat încălcarea privilegiului contra autoincriminării în contextul în care reclamantul a refuzat să participe la un interviu cu inspectorii fiscali pe motiv că nu a primit o garanție conform căreia informațiile furnizate nu vor fi folosite împotriva sa într-un proces penal.[47] Pentru a nu intra în conflict cu cele statuate în cauza *IJL, GMR și AKP c. Regatul* Unit, Curtea a statuat faptul că **în cauza Shannon elementul esențial a fost faptul că reclamantul urma să fie supus unui interviu ce avea ca obiect aspecte ce făceau deja obiectul unei proceduri penale** în care acesta era acuzat de comiterea mai multor infracțiuni economice.

Cu alte cuvinte, reiese faptul că deși natura interviului ar putea fi apreciată ca fiind una administrativă, având în vedere existența unui proces penal ce viza aspectele ce urmau să facă obiectul respectivului interviu, privilegiul contra autoincriminării devine aplicabil.[48] În ceea ce ne privește, o asemenea diferențiere între *cauza Shannon* și *cauza IJL, GMR și AKP c. Regatul Unit* are la bază mai degrabă **riscul ca informațiile obținute ca urmare a constrângerii la cooperare să fie folosite ulterior în cadrul unei proceduri penale.** Risc ce a fost evidenţiat inclusiv în *cauza Marttinen c. Finlanda* (parag. 73 din hot.). Un asemenea raționament pune însă în discuție concluziile oferite în *cauza Saunders* și *cauza IJL, GMR și AKP c. Regatul Unit,* din moment ce ne este greu să acceptăm teza conform căreia acest risc nu era unul cât se poate de evident în aceste cauze.[49]

Aceste exemple, ce sugerează o lipsă de coerenţă la nivelul jurisprudenţei CtEDO, nu sunt decât primele dintr-o serie lungă de exemple îngrijorătoare din perspectiva faptului că în loc să se răspundă la anumite întrebări sunt generate alte semne de întrebare.

Apreciem însă că a fost acceptat de către Curte faptul că nu este absolut necesar ca la momentul constrângerii să existe o acuzaţie în materie penală îndreptată împotriva unei persoane, privilegiul putând fi aplicabil inclusiv în acele situaţii în care o astfel de acuzaţie poate fi anticipată. Această concluzie reiese printre altele din cauzele *Weh c. Austria* (parag. 53 din hot.) și *Reig c. Austria* (parag. 30 din hot.). Astfel, în aceste cauze Curtea s-a bazat pe faptul că la momentul constrângerii nu exista o procedură penală *pendinte* ori anticipată împotriva reclamanţilor. Inclusiv în cauza Funke, cu toate că s-a constatat încălcarea art. 6 din Convenţie, a lipsit o procedură penală *pendinte* împotriva reclamantului.[50] Și în acest caz, faptul că o astfel de procedură putea să fie anticipată a fost suficient pentru a constata aplicabilitatea art. 6 din Convenţie, raportat la privilegiul contra autoincriminării.

3. Întinderea privilegiului raportat la obiectul constrângerii la cooperare

Așa cum am precizat la începutul acestui material, există mai multe ipoteze în care o persoană poate să fie constrânsă la cooperare în vederea decriptării datelor informatice. De aceea, este necesar a analiza modul în care jurisprudența CtEDO poate fi raportată la aceste ipoteze.

---

[47] A se vedea şi parag. 70 din *cauza Marttinen c. Finlanda.*

[48] A. Ashworth, *op. cit.*, p. 757.

[49] A se vedea o analiză mai detaliată în M. Berger, *Self-Incrimination and the European Court of Human Rights...* precit., p. 520-525. Această discuție prezintă o relevanță deosebită prin raportare la dreptul intern, deoarece din practica judiciară rezultă faptul că sesizările privitoare la fapte de evaziune fiscală provin aproape în unanimitate ca urmare a activității desfășurate de inspectorii antifraudă. Or, potrivit art. 4 din Legea nr. 241/2005 „*constituie infracțiune și se pedepsește cu închisoare de la un an la 6 ani* ***refuzul nejustificat al unei persoane de a prezenta organelor competente documentele legale*** *și bunurile din patrimoniu, în scopul împiedicării verificărilor financiare, fiscale sau vamale, în termen de cel mult 15 zile de la somație*". A se vedea o analiză a acestei probleme în Gh. Mateuț, D. Ionescu, *Inadmisibilitatea utilizării ca mijloc de probă în procesul penal a proceselor-verbale și a actelor de constatare obținute în procedurile administrative de control*, în „Caiete de drept penal", nr. 1/2005, p. 4 și urm.

[50] Vezi în acest sens și M. Berger, *Europeanizing Self-incrimination: The Right to Remain Silent in the European Court of Human Rights*, în „Columbia Journal of European Law", vol. 12, 2006, p. 350.

a. Referitor la predarea unor documente

Faptul că și obligaţia de a furniza autorităţilor anumite documente intră sub sfera de aplicabilitate a privilegiului contra autoincriminării raportat la art. 6 din Convenţie reiese cu evidenţă din jurisprudenţa Curţii. Dacă obligaţia de a furniza anumite documente ar excede sferei de aplicabilitate a privilegiului supus analizei, în cauza *Funke* nu s-ar fi ajuns la constatarea încălcării dreptului la un proces echitabil.[51]

În opinia noastră, nu obiectul constrângerii este elementul central în analiza aplicabilităţii privilegiului contra autoincriminării, ci modalitatea în care se realizează constrângerea.[52] **Tocmai de aceea, pe parcursul acestui articol, ne-am referit în repetate rânduri la sintagma „constrângerea la cooperare".**

Susţinem acest punct de vedere deoarece, în *cauza Saunders*, există o precizare aparent problematică ce pare să excludă documentele din sfera de aplicabilitate a privilegiului. Curtea a statuat astfel faptul că de esenţa privilegiului contra autoincriminării este de a respecta *voinţa acuzatului de a păstra tăcerea.* În consecinţă, Curtea a concluzionat că *materialele ce pot fi obţinute prin mijloace coercitive dar care au o existenţă independentă de voinţa acuzatului* (de exemplu, **documente obţinute prin intermediul unui mandat** sau probe biologice) nu sunt acoperite de acest privilegiu. Or, o asemenea concluzie ar evidenţia un conflict între concluzia din *cauza Funke* și cele statuate în *cauza Saunders*, pe motiv că documentele solicitate pot avea o *existenţă independentă de voinţa acuzatului.*

Unii ar putea susține faptul că, în *cauza Saunders*, Curtea a realizat o distincție între probele „reale" (documente, probe biologice etc.) și cele obținute ca urmare a unei declarații ori prin furnizarea unor informații orale (probe testimoniale).[53] Procedându-se astfel, s-ar putea aprecia că probele „reale" obținute ca urmare a constrângerii nu oferă aplicabilitate privilegiului contra autoincriminării, spre deosebire de constrângerea în vederea oferirii unei declarații ori informații orale care nu au o existență independentă de voința persoanei ce a făcut obiectul constrângerii.[54]

Nu dorim să insistăm în legătură cu toate aceste probe „reale" la care pare să facă trimitere Curtea[55], dorind doar să precizăm faptul că în ceea ce ne privește, o astfel de concluzie este eronată. Este criticabilă în primul rând deoarece pare absolut excesiv de a-i conferi statului posibilitatea de a obliga o persoană să predea autorităţilor arma crimei. În mod cert arma crimei este o probă „reală" ce are o existenţă independentă de voinţa persoanei acuzate. Cu toate acestea, nu vedem absolut nicio raţiune în a-i permite acuzatului să nu declare nimic, dar a-l obliga totuși să remită o probă materială pe considerentul că această probă nu este una testimonială. Cu alte cuvinte, acuzatul are posibilitatea de a refuza să spună unde este arma, dar este obligat să o predea. În mod cert, o distincţie precum cea de mai sus nu poate fi acceptată.

De asemenea, așa cum am menţionat *supra*, a exclude *de plano* obținerea documentelor din sfera de aplicabilitate a privilegiului contra autoincriminării ar crea o coliziune între cele statuate în *cauza Funke* și cele statuate în *cauza Saunders*. Or, din considerentele cauzei Saunders **nu reiese în mod explicit faptul că ne aflăm în prezența unui reviriment jurisprudențial.** Curtea nu contrazice cele statuate în *cauza Funke*, nu revine asupra concluziei din această cauză, ci doar dezvoltă analiza privilegiului contra autoincriminării. Analiză care, de altfel, în *cauza Funke* lipsește cu desăvârșire.

De asemenea, la o analiză atentă a considerentelor Curții în *cauza Saunders* observăm faptul că aceasta pare să fi realizat – *cel puțin privitor la documente* – o distincție între modalitățile în care se realizează constrângerea și nu între probe „reale" ori testimoniale. În consecință, **formularea existentă în *cauza Saunders* necesită analizată cu mare atenţie, putându-se observa faptul că, nu se exclude obținerea oricărui document din sfera de aplicabilitate a privilegiului contra autoincriminării ci doar a acelor documente obținute ca urmare a unui mandat de percheziţie**[56] (sic!).

Această concluzie întărește teza conform căreia, esențial este dacă respectiva constrângere implică ori nu o colaborare din partea persoanei acuzate. În cazul mandatelor de percheziție domiciliară, organele de urmărire

[51] Aceeași opinie în A. Ashworth, *op. cit.*, p. 753.

[52] A se vedea și M. Redmayne, *op. cit.*, p. 214-215.

[53] A se vedea analiza din A. Ashworth, *op. cit.*, p. 758.

[54] Această diferențiere o vedem ca fiind superficială, în contextul în care inclusiv gândurile unei persoane pot dobândi autonomie dacă sunt transpuse pe hârtie anterior momentului constrângerii.

[55] Cu privire le probele biologice, a se vedea R. Chiriță, *op. cit.*, p. 68.

[56] A se vedea în acest sens și M. Berger, *Self-Incrimination and the European Court of Human Rights... precit.*, p. 526.

penală pot obține cu forța documentele din cuprinsul mandatului, nefiind necesară cooperarea persoanei acuzate.[57] În măsura în care se solicită însă colaborarea persoanei acuzate, privilegiul contra autoincriminării devine aplicabil, deoarece o asemenea colaborare forțată se află în contradicție cu voința acestuia[58] – motiv pentru care o asemenea colaborare este de altfel exclusă prin raportare la infracţiunea de obstrucţionare a justiţiei. Această opinie a fost susținută și în literatura de specialitate,[59] unde s-a mai statuat inclusiv faptul că probele biologice exced sferei de aplicabilitate a privilegiului contra autoincriminării pe motiv că pot fi obținute și fără cooperarea persoanei în cauză.[60]

De exemplu, o probă ADN ar putea fi luată printr-o intruziune justificată în viaţa privată a individului fără a se încălca așadar art. 8 din Convenţie și totodată, fără a fi necesară o conduită contrară art. 3 din Convenţie. În context, prelevarea unor probe biologice precum sângele ori saliva, fără consimțământul persoanei vizate, nu au fost apreciate ca fiind în conflict cu prevederile art. 3 și 8 din Convenție în cauzele *X. c. Olanda* și *Schmitd c. Germania*.[61]

Este adevărat că, în cauza *Jalloh c. Germania*, Curtea a constatat încălcarea privilegiului contra autoincriminării deși autorităţile au obţinut o probă materială din corpul reclamantului fără cooperarea acestuia. Cu toate acestea, concluzia din cauza Jalloh nu face însă decât să sublinieze încă o dată faptul că esenţial nu este obiectul constrângerii ci modalitatea în care aceasta este realizată. În ceea ce ne privește, din *cauza Jalloh* rezultă faptul că, în mod excepţional, privilegiul își găsește aplicabilitatea și atunci când discutăm despre obţinerea unei probe materiale preexistente fără cooperarea persoanei vizate și anume atunci când aceasta se realizează cu încălcarea art. 3 din Convenţie.[62] **Astfel, regula este aceea că privilegiul contra autoincriminării interzice constrângerea la cooperare, în vreme ce excepţia vizează situaţia în care, în lipsa unei cooperări, se intervine în vederea obţinerii unei probe prin încălcarea art. 3 din Convenţie.**

Raportat la regulă, deși din punct de vedere material documentele preexistente pot avea o existență independentă de voința persoanei acuzate, **producerea acestora afectează această voință**, motiv pentru care constrângerea la cooperare este cea care activează privilegiului contra autoincriminării și nu mijlocul de probă ce formează obiectul constrângerii.[63] Faptul că este așa, iar obținerea unor documente ca urmare a unei constrângeri la cooperare atrage aplicabilitatea privilegiului contra autoincriminării, **rezultă cu evidență inclusiv din *cauza Heaney și McGuiness c. Irlanda*, o cauză ulterioară *cauzei Saunders* și în care Curtea și-a însușit concluzia din *cauza Funke*.**

Această **analiză cronologică a jurisprudenței Curții** denotă faptul că în *cauza Saunders* nu a avut loc un reviriment jurisprudențial, din moment ce aceasta nu a contrazis cele statuate în *cauza Funke*, iar în *cauza Heaney și McGuiness* s-a achiesat la hotărârea Funke fără a se contrazice însă *cauza Saunders*.[64] De altfel, în cauza *JB c. Elveția*, Curtea a considerat că a fost încălcat privilegiul contra autoincriminării deși obiectul constrângerii viza predarea unor documente financiare autorităților fiscale.[65] Pentru a constata încălcarea art.

---

[57] A se vedea și A. Choo, *op. cit.*, p. 73.

[58] A. Ashworth, *op. cit.*, p. 760.

[59] M. Redmayne, *op. cit.*, p. 214.

[60] Uneori se vorbește despre *cooperare activă vs. cooperare pasivă* (V. Pușcașu, *Prezumția de nevinovăție... op. cit., p. 206*). Astfel, în cazul probelor biologice discutăm despre o colaborare pasivă în sensul că persoana vizată are obligația de a nu se opune prelevării mostrei biologice, în vreme ce cooperarea activă nu poate face obiectul constrângerii. Cu o asemenea distincție am putea să fim de acord, esențial fiind ca privilegiul contra autoincriminării să devină aplicabil atunci când constrângerea implică o cooperare... în sensul de cooperare activă.

[61] A se vedea și parag. 76 din *cauza Jalloh c. Germania*.

[62] S-ar mai putea susține inclusiv faptul că în cauza Jalloh, determinant a fost faptul că reclamantul a regurgitat o cantitate de cocaină ce a fost, fără discuție, incriminatorie. Astfel, s-ar putea face o distincție între probele biologice prelevate în vederea efectuării unei expertize și acele probe preexistente care sunt *per se* incriminatorii. A se vedea în acest sens parag. 113 din hot. *Jalloh c. Germania* și A. Choo, *op. cit.*, p. 74-75. O asemenea concluzie o apreciem însă ca fiind în contradicție cu cele statuate în *cauza Saunders*, unde Curtea s-a bazat pe ideea că este irelevant dacă probele obținute ca efect al constrângerii sunt ori nu *per se* incriminatorii – inclusiv autorul citat observând acest aspect. De asemenea, a marca acest element ca fiind unul definitoriu în ceea ce privește aplicabilitatea privilegiului contra autoincriminării ar face ca predarea unor documente ca efect al constrângerii să nu mai ridice probleme în această materie atâta vreme cât prin conținutul lor se poate proba un comportament infracțional.

[63] A se vedea în acest sens și A. Ashworth, *op. cit.*, p. 760.

[64] Observație avută în vedere și de M. Redmayne, *op. cit.*, p. 213.

[65] Facem precizarea că în literatura de specialitate (R. Chiriță, *op. cit.*, p. 65, parag. 13) se menționează în mod eronat faptul că în această cauză Curtea a constatat faptul că art. 6 din Convenția nu a fost încălcat.

6 din Convenție, Curtea a apreciat că aceste documente se diferențiază de probele biologice la care s-a făcut referire în *cauza Saunders*, făcând precizarea că doar acestea din urmă sunt obținute fără încălcarea voinței persoanei (parag. 68 din hot.). Oare dacă în cauza Saunders, Curtea s-a referit la orice fel de documente, indiferent de mijlocul prin care acestea sunt obținute, de ce în cauza *JB c. Elveția* constrângerea în vederea remiterii unor documente a dus la încălcarea art. 6 din Convenție?

În concluzie, apreciem că doar o interpretare inadecvată a considerentelor hotărârii *Saunders* poate genera confuzie la nivelul sferei de aplicabilitate a privilegiului contra autoincriminării prin raportare la predarea unor documente, ca obiect al constrângerii la cooperare.[66]

Orice interpretare rezonabilă a jurisprudenței Curții indică faptul că predarea unor documente ca efect al constrângerii la cooperare este contrară privilegiului contra autoincriminării. Doar documentele obținute prin intermediul unui mandat de percheziție domiciliară și fără cooperarea forțată a persoanei acuzate face ca art. 6 din Convenție să nu își găsească aplicabilitatea (a se vedea și parag. 102 din cauza *Jalloh c. Germania*).

b. Referitor la oferirea unei mostre de voce

În cauza *P.G. și J.H. c. Regatul Unit*, Curtea a statuat că obținerea unor mostre de voce prin intermediul unor înregistrări neconsimțite nu atrage o încălcare a privilegiului contra autoincriminării. Din aceasta perspectivă, Curtea a concluzionat practic faptul că, atâta timp cât mostrele de voce nu conțin declarații incriminatorii pot fi privite precum sângele, firele de păr ori alte asemenea specimene folosite în analiza criminalistică și care, potrivit cauzei Saunders, nu intră sub incidența privilegiului (a se vedea parag. 80 din hot.).

Deși nu criticăm soluția la care a ajuns Curtea din perspectiva respectării privilegiului contra autoincriminării, nu putem să nu ne punem întrebarea cum ar putea decurge o constrângere realizată în conformitate cu prevederile art. 6 din Convenție dacă persoana vizată refuză să coopereze iar autoritățile nu au posibilitatea de a se folosi de înregistrări ambientale ori convorbiri telefonice prin care să obțină mostre de voce „oferite" involuntar. În măsura în care singura posibilitate de a obține astfel de mostre este prin „participarea activă" a unei persoane, se pune problema în ce măsură constrângerea acesteia la cooperare este conformă cu privilegiul supus analizei.

Discuția în acest context devine oarecum problematică datorită faptului că, o cooperare se poate realiza fie prin intermediul unei constrângeri fizice / morale, fie prin intermediul unei norme legale ce instituie o sancțiune în caz de refuz la cooperare. Constrângerea fizică / morală devine problematică deoarece pune în discuție conformitatea cu art. 3 și 8 din Convenție, existând riscul ca intervenția disproporționată să atragă exact consecințele din *cauza Jalloh c. Germania*.

Singura soluție ar rămâne așadar instituirea unei obligații legale la cooperare sub sancțiunea aplicării unei sancțiuni în caz de refuz, similar prevederilor referitoare la recoltarea de probe biologice în cazul participanților la traficul rutier.[67]

Dincolo de aceste aspecte, raportat la problematica decriptării datelor informatice, esențial este de a vedea în ce măsură o astfel de constrângere devine ori nu o excepție de la regulă. Fără a insista la acest moment în legătură cu această chestiune, facem mențiunea că, în ceea ce ne privește, decriptarea datelor informatice prin intermediul unei comenzi vocale necesită a beneficia de un tratament distinct. Aceasta deoarece **cheia pentru decriptarea datelor informatice constând în vocea titularului sistemului informatic nu implică doar necesitatea identificării unor caracteristici ale vocii, fiind de asemenea esențial conținutul.** Cu alte cuvinte, pentru decriptarea datelor informatice nu contează doar identificarea vocii titularului sistemului informatic, fiind de asemenea necesar ca titularul să rostească un cuvânt ori o anumită frază, aspect ce denotă o componentă testimonială acoperită de privilegiul contra autoincriminării.

4. Posibilitatea de a restrânge aplicabilitatea privilegiului contra autoincriminării ori de a-l anula

În *cauza Funke*, Curtea a recunoscut implicit faptul că **privilegiul nu poate fi pus în balanță cu interesul public în vederea determinării unei încălcări a dreptului la un proces echitabil.** Aceasta rezultă din faptul că, soluția favorabilă reclamantului a fost dată în contra opiniei Comisiei în același caz, ce a statuat faptul

[66] Nu putem însă să nu observăm faptul că jurisprudența Curții în materia privilegiului contra autoincriminării ridică probleme de interpetare îndeosebi datorită cauzelor în care pârât a fost Regatul Unit.

[67] În legătură cu aceste prevederi, Curtea Constituțională a statuat în mai multe rânduri faptul că obligația legală de a coopera în vederea recoltării de probe biologice este în conformitate cu privilegiul contra autoincriminării. A se vedea în acest sens V. Pușcașu, *Dreptul la tăcere..., precit.*, p. 206-207.

că mijloacele coercitive au fost necesare pentru a proteja „*interesele economice vitale ale statului*".[68] Că este așa rezultă inclusiv din cauzele *Heaney și McGuiness c. Irlandei* și *Quinn c. Irlandei* unde acuzaţia – *una de terorism* – prezenta fără îndoială o relevanţă deosebită din perspectiva interesului public, dar cu toate acestea s-a constatat încălcarea art. 6 din Convenție prin nerespectarea privilegiului contra autoincriminării.[69]

În *cauza Saunders*, **Curtea a respins de asemenea argumentul Guvernului potrivit căruia interesul public ar putea justifica o restrângere a privilegiului contra autoincriminării** (a se vedea parag. 74 din hot.)[70], iar în cauza *Jalloh c. Germania*, Curtea a statuat (parag. 97 din hot.) cât se poate de clar faptul că cerințele generale privitoare la echitatea unei proceduri penale își păstrează aplicabilitatea indiferent de tipul infracțiunii ori interesul public invocat.[71]

O cauză extrem de importantă sub acest aspect s-ar putea dovedi *Ibrahim ș.a. c. Regatului Unit*, unde acuzaţia de terorism a generat în opinia noastră o soluţie eronată din partea Curţii, aceasta apreciind că nu a fost încălcat privilegiul contra autoincriminării nici măcar în ceea ce priveşte declaraţia unui martor căruia nu i s-a adus la cunoştinţă dreptul de a nu se autoincrimina în momentul în care acest risc era unul cât se poate de evident. Aceste aspecte urmează însă a fi reevaluate de către Marea Cameră, motiv pentru care nu dorim să insistăm asupra unei hotărâri ce ar putea fi inversată.[72]

În cauza *John Murray c. Regatul Unit*, Curtea a stabilit totuși faptul că privilegiul contra autoincriminării **nu este unul absolut**[73] prin aceea că, în situaţii particulare, tăcerea acuzatului poate produce consecinţe defavorabile în sarcina acestuia (parag. 49 din hotărâre). Relevante în acest sens sunt și cauzele *Averill c. Regatul Unit* și *Telfner c. Austria*, cauze în care Curtea a subliniat de asemenea ideea conform căreia, în anumite circumstanţe, tăcerea acuzatului poate fi întoarsă – *în anumite limite* – împotriva acestuia.

Necesită observat totuși faptul că, în toate aceste cauze, **accentul a fost pus pe circumstanţele în care are loc această pasivitate a acuzatului și nu pe natura ori gravitatea infracţiunii ce face obiectul acuzaţiei.** Aceste circumstanţe vizează, de exemplu, gradul în care a fost probată acuzația independent de cele declarate de persoana acuzată. Astfel, în măsura în care probele în acuzare sunt importante (urme incriminatorii pe corp ori pe hainele acuzatului – cauza *Averill c. Regatul Unit*) și se consideră că este necesară o explicaţie din partea acuzatului (cauza *John Murray c. Regatul Unit*), dreptul la tăcere poate suferi anumite restrângeri, CtEDO apreciind ca fiind rezonabil a se concluziona în aceste circumstanţe că tăcerea nu poate indica decât o recunoaștere implicită a vinovăţiei. Necesită însă observat că această concluzie s-a datorat și secțiunii 35 din Criminal Justice and Public Order Act 1994, ce stabilea practic cadrul normativ intern pentru restrângerea privilegiului. CtEDO nu a ajuns așadar la concluzia de mai sus decât prin raportare la dreptul intern supus analizei.

O asemenea abordare este însă în contradicție cu prevederile art. 83 lit. a) C. proc. pen.. Strict sub acest aspect, **nivelul de protecţie din dreptul intern este mai ridicat decât cel conferit de art. 6 din Convenţie.**

În cauza *O'Halloran și Francis c. Regatul Unit*, Curtea a constatat faptul că privilegiul contra autoincriminării nu a fost încălcat deși contrângerea a fost una cât se poate de directă în sensul că reclamanții au primit o notificare prin care **le-a fost solicitat să informeze poliția cine a condus vehiculul** care a fost detectat de aparatul radar ca depășind limita legală de viteză.

Este evident faptul că, prin această hotărâre, **Marea Cameră a CtEDO a decis că privilegiul contra autoincriminării nu este unul absolut ci poate fi limitat prin raportare la anumiți factori.** Criticabil este însă faptul că nu s-au oferit criterii clare pentru a putea fi aplicate în alte cauze (a se vedea analiza făcută *infra*).

În ceea ce ne privește, această cauză nu este reprezentativă pentru aprecierea sferei de aplicabilitate a privilegiului contra autoincriminării, părând mai degrabă că soluția dată s-a datorat contextului în care a avut loc constrângerea și anume în vederea prevenirii accidentelor rutiere. Cu alte cuvinte, ***cauza O'Halloran***

---

[68] A se vedea în acest sens și A. Ashworth, *op. cit.*, p. 753.

[69] A se vedea în acest sens și M. Berger, *Self-Incrimination and the European Court of Human Rights: Procedural Issues in the Enforcement of the Right to Silence*, în „European Human Rights Law Review", nr. 5, 2007, p. 358-359.

[70] Opinie însușită ulterior și în *cauza Marttinen c. Finlanda* (parag. 74-75 din hot.).

[71] Interes public ce este pus într-o cu totul altă perspectivă în parag. 107 din hot.

[72] Pentru o critică a acestei hotărâri, se poate vedea M. Seet, *Suspected Terrorists and the Privilege Against Self-Incrimination*, în „Cambridge Law Journal", vol. 74, nr. 2, 2015, p. 208.

[73] A. Ashworth, *op. cit.*, p. 754.

***și Francis c. Regatul Unit* pare să instituie mai degrabă o excepţie de la regulă în loc să clarifice aspectele ce necesitau a fi clarificate.**

În sprijinul soluţiei din această cauză, s-ar putea susţine faptul că, la nivelul Uniunii, există un consens în sensul că privilegiul contra autoincriminării nu se aplică în ceea ce privește identificarea persoanei care a condus vehiculul.[74] Astfel, în unele state membre, în măsura în care proprietarul vehiculului refuză să indice persoana care a condus vehiculul este posibilă utilizarea unei prezumții în sensul că proprietarul mașinii a fost și conducătorul acesteia.[75]

De asemenea, **s-ar putea conchide că privilegiul contra autoincriminării poate fi limitat în baza riscului asumat de către participanții la traficul rutier.** Inclusiv judecătorul Borrego Borrego, în opinia concurentă, a insistat pe ideea conform căreia cei care decid să dețină un vehicul și să participe cu acesta la traficul rutier își asumă anumite obligații în vederea prezervării siguranței traficului, iar renunțarea la privilegiul contra autoincriminării poate fi una dintre acestea.

Acest raţionament, deși persuasiv, este însă unul **extrem de periculos deoarece există riscul de a fi extins în alte sfere de activitate lipsind practic de conținut privilegiul contra autoincriminării.** În cele din urmă, inclusiv teroriștii își asumă anumite riscuri în activitatea acestora, fapt ce nu poate rezulta în abolirea, în ceea ce îi privește, a garanțiilor conferite de art. 6 din Convenție. La fel, precum în cazul traficului rutier, activităţile comerciale, vamale etc. sunt strict reglementate, putându-se susţine de asemenea că acele persoane care consimt să ia parte la asemenea activităţi acceptă riscurile ce decurg din acestea – inclusiv riscul de a fi obligate să colaboreze cu anumite autorităţi / organisme de control. Or, o asemenea abordare ar lipsi de conţinut drepturile conferite de art. 6 din Convenţie, acestea devenind practic iluzorii.

5. Posibile criterii pentru justificarea constrângerii

Din toată jurisprudenţa CtEDO în materie pare să reiasă concluzia – *criticabilă ori nu* – conform căreia privilegiul contra autoincriminării poate suferi anumite restrângeri, nefiind unul absolut. Sau, cu alte cuvinte, este posibil ca în anumite împrejurări, deși ne aflăm în prezenţa unei constrângeri la cooperare, aceasta să nu fie incompatibilă cu esenţa dreptului la un proces echitabil.

Chiar dacă ar fi să acceptăm un asemenea punct de vedere, apreciem faptul că este necesar să se identifice niște criterii clare și rezonabile, calităţi ce nu par să fie întrunite raportat la criteriile regăsite sporadic în jurisprudenţa Curţii.

1. Interesul public

În ceea ce privește acest criteriu, am învederat *supra* aparenta direcţie a CtEDO în materia privilegiului contra autoincriminării. Deși aceasta nu este întru totul clară și pe alocuri intră într-un conflict nepermis cu propria jurisprudenţă, este posibil să asistăm în curând la legitimarea din partea CtEDO a unui „tratament preferenţial" oferit persoanelor acuzate de infracţiuni de terorism.

Fără a neglija importanţa luptei împotriva terorismului, rămâne extrem de problematică această repoziţionare a CtEDO ce aduce în discuţie „dreptul inamicului" în care o persoană acuzată de terorism își pierde statutul de beneficiar al unor drepturi elementare și totodată fundamentale. Nu ar fi oare mai corect și mai sincer în a ne raporta la aceste persoane ca la niște combatanţi și a renunţa la a mai considera că sancţionarea acestora ţine de sistemul judiciar? Cea mai mare problemă este că problema terorismul poate degenera într-o problemă la nivelul respectării drepturilor omului inclusiv în alte materii în care interesul public va fi ușor de evidenţiat ca și criteriu în vederea limitării ori abolirii privilegiului contra autoincriminării – de exemplu, în cazul traficului de droguri, infracțiunilor de corupție, al criminalității informatice etc.

O asemenea abordare ar duce practic la limitarea dreptului la un proces echitabil în funcţie de gradul interesului public identificat în cauza supusă analizei. Or, **deși un asemenea examen de proporţionalitate își poate găsi justificarea în ceea ce privește art. 8-10 din Convenţie, ridică serioase semne de întrebare în ceea ce privește respectarea dreptului la un proces echitabil**.[76]

Ne este imposibil să acceptăm că o persoană care a comis o infracţiune gravă trebuie se beneficieze într-o mai mică măsură de un proces echitabil în raport cu o altă persoană ce a avut „inspiraţia„ de a alege să

[74] Vezi A. Ashworth, *op. cit.*, p. 753 şi 771.

[75] Ibidem.

[76] A se vedea în acest sens şi D. Ionescu, *Gäfgen c. Germania:* un moment de reflecție şi multe întrebări, în „Caiete de drept penal", nr. 4/2012, p. 25-26.

comită o infracţiune ce nu denotă un interes public „semnificativ". Situaţia poate deveni cu atât mai dramatică cu cât gravitatea unei infracţiuni ori interesul public poate diferi semnificativ de la un stat membru la altul. De exemplu, în România, infracţiunile de corupţie ori cele asimilate acesteia generează dezbateri publice intense și sugerează faptul că interesul public în combaterea unor asemenea infracţiuni este enorm. Cu toate acestea, avem serioase rezerve că infracţiuni precum abuzul în serviciu ori conflictul de interese justifică o limitare a dreptului la un proces echitabil.

Dacă pentru acestea se justifică o astfel de abordare, nu ne rămâne decât să oferim un tratament similar și în cazul unor infracţiuni contra persoanei (omor, lipsire de libertate, viol etc.), deoarece inclusiv acestea prezintă o gravitate deosebită ce ar trebui să releve un interes public „semnificativ". Așa am ajunge să ne raportăm la infracţiuni de criminalitate organizată (trafic de persoane ori de droguri, criminalitate informatică etc.) ori economice (spălare de bani, evaziune fiscală etc.), deoarece a nu ţine cont de acestea nu ar mai avea o „justificare reală". În context, nu putem decât să ne întrebăm retoric ce ar mai rămâne atunci din art. 6 din Convenţie? Un cumul de reguli – aparent stricte – dar aplicabile doar în cazul unei infracţiuni de furt ori înșelăciune? Căci privitor la infracţiunile rutiere, Curtea ne-a lămurit deja (sic!).

2. Imposibilitatea / dificultatea de a obţine mijlocul de probă prin alte mijloace

În *cauza Funke* s-a constatat încălcarea art. 6 din Convenţie deși Curtea a avut în vedere faptul că autorităţile vamale „***nu puteau*** *sau nu doreau să procure documentele prin alte mijloace*" (parag. 44 din hot.). Precizarea este importantă în contextul în care s-ar putea invoca inaplicabilitatea privilegiului având în vedere dificultatea ori, uneori, imposibilitatea decriptării datelor informatice în lipsa colaborării suspectului, inculpatului ori martorului prin oferirea cheii pentru decriptare ori prin oferirea în mod nemijlocit a conţinutului într-un format lizibil (necriptat).

Este greu de crezut că privilegiului contra autoincriminării ar deveni inaplicabil de fiecare dată când organele judiciare ar întâmpina dificultăţi în stabilirea vinovăţiei. De altfel, **privilegiul în cauză, prin raportare la prezumţia de nevinovăţie, se bazează exact pe acest raport dintre stat și acuzat, în care condamnarea trebuie obţinută fără sprijinul acestuia din urmă**[77] (a se vedea inclusiv parag. 100 din cauza *Jalloh c. Germania*)**.** Or, este evident faptul că posibilitatea de a proba dincolo de orice dubiu că o persoană se face vinovată de comiterea unei infracţiuni nu mai justifică o necesitate reală de a restrânge sfera de aplicabilitate a privilegiului contra autoincriminării.

Această necesitate apare cu evidenţă în exact acele situaţii în care acuzarea este vulnerabilă din perspectivă probatorie. Apreciem așadar că **exact aceste situaţii trebuie să genereze garanţii suplimentare în favoarea persoanei acuzate,** deoarece din vulnerabilitatea probelor în acuzare rezultă și tentaţia de a transforma persoana acuzată într-un martor al acuzării – adică exact ceea ce a subliniat Curtea în *cauza Saunders* (parag. 68 din hot.).

Pe de altă parte, a utiliza un astfel de criteriu pentru restrângerea aplicabilităţii privilegiului poate genera consecinţe absurde în care acesta devine inaplicabil și în ipoteza luării unei declaraţii prin constrângere. În măsura în care aspectele ce ar trebui învederate de către persoana acuzată sunt extrem de relevante sub aspect probator iar singura posibilitate rezonabilă de a obţine informaţiile dorite este prin audierea persoanei acuzate, ar crea exact cadrul avut în vedere *supra*. Din nou, acuzatul s-ar transforma într-un martor al acuzării atunci când acuzarea nu își poate proba propriul caz. Or, tocmai această abordare se află în conflict cu prezumţia de nevinovăţie.

3. **Natura și gravitatea sancţiunii în caz de refuz**

Un posibil criteriu ar fi acela de a ne raporta la un prag minimal al consecinţelor adverse pe care le-ar avea de suferit persoana care refuză să colaboreze.[78]

În *cauza Saunders*, pedeapsa în caz de refuz în ceea ce privește colaborarea (*contempt of court*) era de 2 ani închisoare, în vreme ce în *cauza Allen* – unde Curtea a apreciat că nu s-a adus atingere privilegiului contra autoincriminării - riscul era sancţionarea cu o pedeapsă cu amendă în cuantum maxim de 300£. În *cauza O'Halloran și Francis c. Regatul Unit*, Curtea a considerat important faptul că pedeapsa în caz de refuz era una „moderată" și nu una privativă de libertate.

[77] A se vedea în acest sens și R. Chiriță, *op. cit.*, p. 60-61; M. Udroiu, *Principiile fundamentale cuprinse în Proiectul noului Cod de procedură penală – spre un nou model de proces penal*, în „Caiete de drept penal", nr. 2/2009, p. 71.

[78] A se vedea și M. Berger, *Self-Incrimination and the European Court of Human Rights... precit.*, p. 518.

Dacă acest privilegiu este o componentă esenţială a dreptului la un proces echitabil, o asemenea abordare nu se dovedește decât incoerentă și absurdă. Pe de altă parte, deși în *cauza Funke* reclamantul a fost sancţionat pentru refuzul de a remite autorităţilor anumite documente bancare solicitate de acestea cu aplicarea unor amenzi, Curtea a constatat totuși încălcarea privilegiului contra autoincriminării.

***4.* Natura și gradul constrângerii**

Curtea a făcut trimitere expresă la acest criteriu atât în *cauza Jalloh c. Germania* (parag. 116 din hot.) cât și în *cauza O'Halloran și Francis c. Regatul Unit* (parag. 55 din hot.). În *cauza Jalloh c. Germania* regurgitarea forţată a drogurilor prin imobilizarea suspectului și administrarea unor substanţe chimice prin intermediul unui tub introdus prin nas în stomac a fost apreciată ca fiind incompatibilă cu prevederile art. 3 din Convenţie și cu privilegiul contra autoincriminării.

În cauza *Allan c. Regatul Unit*, prin soluţia pe care a dat-o, Curtea a statuat practic faptul că această constrângere nu trebuie să implice în mod necesar violenţă.[79] Astfel, inclusiv utilizarea unor subterfugii în vederea obţinerii unei declaraţii involuntare este susceptibilă să atragă incidenţa privilegiului contra autoincriminării.

5. Existenţa unor garanţii procedurale

Tot în *cauza Jalloh c. Germania*, Curtea s-a raportat la acest criteriu (parag. 120 din hot.) în analiza privitoare la distrugerea esenţei dreptului la un proces echitabil prin nerespectarea privilegiului contra autoincriminării. Din nou, analiza unui criteriu utilizat într-o cauza excepţională precum *cauza Jalloh* ridică anumite dificultăţi.

Suntem însă de acord că existenţa unor garanţii procedurale ar putea face ca privilegiul contra autoincriminării să dobândească o aplicabilitate mai restrânsă. În cauza *Jalloh c. Germania*, s-a avut însă în vedere mijlocul impropriu prin care s-a intervenit asupra corpului reclamantului. Singurul exemplu în care subiectul decriptării datelor informatice ar putea fi raportat la *cauza Jalloh* ar fi acela în care persoana vizată înghite entitatea materială pe care este stocată cheia pentru decriptarea datelor informatice.

În ceea ce privește garanţiile procedurale pentru evitarea unor abuzuri și intervenţii arbitrare, apreciem că dreptul intern este departe de a reprezenta un exemplu demn de urmat. Astfel, am precizat deja faptul că în ceea ce îi privește pe martori, imunitatea conferită de art. 118 C. proc. pen. este insuficientă, fiind necesară în acest sens o imunitate derivativă (*derivative-use immunity*).

De asemenea, strict prin raportare la problematica decriptării datelor informatice, necesită observat faptul că **art. 168 C. proc. pen. nu oferă garanţii suficiente.**

În mod evident, necesitatea de a avea acces la un conţinut necriptat vizează posibilitatea de a efectua o percheziţie informatică. Or, **în ceea ce privește efectuarea percheziţiei informatice, doar la o analiză extrem de superficială s-ar putea susţine faptul că prevederile art. 168 C. proc. pen. oferă garanţii suficiente în ceea ce privește respectarea dreptului la apărare ori a art. 8 din Convenţie.**

Nu este momentul pentru a oferi o critică *in extenso* a acestor prevederi ori a modului în care acestea sunt aplicate de către organele judiciare. Dorim totuși să atragem atenţia asupra faptului că art. 168 alin. (11) C. proc. pen. impune doar prezenţa suspectului ori a inculpatului. În mod excepţional, când suspectul ori inculpatul nu poate participa, se impune prezenţa unui reprezentant ori a unui martor asistent – art. 168 alin. (11) rap. la art. 159 alin. (11) C. proc. pen.. Reglementarea este ridicolă în contextul în care sistemul informatic ori mijlocul de stocare a datelor informatice percheziţionat poate să aparţină unei alte persoane decât suspectului ori inculpatului. Mai mult decât atât, entitatea percheziționată poate să aparțină făptuitorului, iar percheziția informatică să se desfășoare în cadrul urmăririi penale *in rem*, adică anterior dobândirii calității de suspect ori învinuit. În context, apreciem ca fiind injust a obliga o persoană să coopereze în vederea decriptării datelor informatice, fără a-i oferi posibilitatea de a participa la percheziţia informatică efectuată asupra dispozitivului ridicat de la aceasta. **O primă soluție în remedierea acestei grave inechități este aceea de a conferi și persoanelor „interesate" dreptul de a participa la o asemenea procedură.** Când ne referim la persoane interesate avem în vedere partea vătămată, făptuitorul ori o altă persoană de la care s-a ridicat sistemul informatic ori mijlocul de stocare a datelor informatice.

Aceasta cu atât mai mult cu cât, **legiuitorul nu s-a gândit să limiteze activităţile prevăzute în conţinutul art. 168 alin. (1) C. proc. pen. prin impunerea judecătorului de drepturi și libertăţi a obligaţiei**

[79] Vezi și A. Ashworth, *op. cit.*, p. 761-762.

de a stabili anumite limite prin conţinutul mandatului de percheziţie informatică. În lipsa acestor limite, specialistul are posibilitatea de a identifica materiale cu conţinut pornografic într-o cauză privind fapte de corupţie, fără a exista în acest sens o sancţiune expres prevăzută de C. proc. pen..

Mai mult decât atât, **art. 168 C. proc. pen. nu prevedere obligaţia de a sigila copia efectuată în baza art. 168 alin. (9) C. proc. pen., ulterior finalizării percheziţiei informatice.** Această omisiune permite specialistului ori organului de urmărire penală de a analiza conţinutul copiei (ce reprezintă practic o clonă fidelă a sursei originale) și de a obţine date informatice suplimentare, în afara procedurii percheziţiei informatice.

Acestea sunt doar câteva dintre criticile ce evidențiază modul deficitar în care a fost reglementată instituția percheziției informatice. Dincolo de aceste critici, necesită observat și cadrul legislativ ce permite organelor de urmărire penală să dispună **efectuarea unor constatări tehnico-științifice care să aibă ca obiect aspect la care face referire art. 168 alin. (1) C. proc. pen..**

În concluzie, ne aflăm în situaţia în care orice persoană trebuie să fie de maximă bună credinţă și să coopereze cu organele judiciare prin oferirea cheii pentru decriptarea datelor informatice ori a conţinutului acestora într-un format lizibil, sperând că acestea la rândul lor nu vor abuza de cadrul extrem de permisiv stabilit de art. 168 C. proc. pen.. Și când spunem asta avem în vedere inclusiv practica constantă a organelor de urmărire penală de a efectua percheziţii informatice prin intermediul unor constatări tehnico-ştiinţifice, în vederea eludării tuturor garanţiilor – chiar așa deficitare cum sunt – prevăzute de art. 168 C. proc. pen..

Poate ar fi momentul ca legiuitorul să conștientizeze faptul că un mijloc atât de intruziv precum percheziţia informatică necesită a avea la bază niște garanţii pe măsură. Credem că este departe de cultura noastră să instituim astfel de garanţii acolo unde legea nu le prevede, motiv pentru care aceste lacune legislative sunt extrem de periculoase, organele de urmărire penală având de cele mai multe ori tentaţia de a face tot ceea ce legea nu interzice. Or, în context, acest „tot ceea ce legea nu interzice" implică o intruziune în viaţa privată a unei persoane în lipsa unui mecanism eficient de control. În context, nu putem spune decât că așteptăm cu mare interes prima condamnare a României la CtEDO prin raportare la art. 8 din Convenție.

6. Informaţia oferită nu este *per se* incriminatorie

În *cauza Weh c. Austria*, reclamantul a refuzat să indice persoana care a condus vehiculul, refuz ce nu s-a aflat din perspectiva Curţii sub incidenţa privilegiului contra autoincriminării. Deși argumentul esenţial al Curţii a fost acela că, la momentul refuzului reclamantului, o procedură penală nu putea fi nici măcar anticipată, în considerentele hotărârii s-a concluzionat inclusiv faptul că identificarea numelui persoanei care a condus vehiculul în momentul comiterii unei infracţiuni rutiere nu este incriminatorie *per se*.

În ceea ce ne privește, **ambele concluzii sunt extrem de criticabile.** Astfel, este cel puţin bizar a se susţine faptul că identificarea persoanei care a condus vehiculul nu este *per se* incriminatorie în condiţiile în care reprezintă elementul central al oricărei infracţiuni rutiere. Dacă ceea ce s-a dorit a se evidenţia este faptul că identificarea numelui conducătorului vehiculului nu este incriminatorie deoarece trebuie probată și conduita infracţională, am ajunge în situaţia în care majoritatea declaraţiilor luate sub efectul constrângerii ar fi lipsite de această caracteristică din simplul motiv că din aceasta este posibil să nu reiasă toate elementele constitutive ale infracţiunii. Multe probe necesită a fi coroborare cu altele în vederea obţinerii unei forţe probante, dar aceasta nu înseamnă că, luate individual, nu sunt *ele însele* incriminatorii.

Pe de altă parte, din moment ce se solicită informaţii cu privire la persoana care a condus vehiculul în contextul suspiciunii ori certitudinii că acest vehicul a fost folosit la comiterea unei infracţiuni rutiere este greu de crezut că la momentul refuzului reclamantului de a oferi informaţia solicitată nu se putea preconiza iniţierea unei proceduri penale împotriva sa.

Având însă în vedere posibilitatea de a utiliza acest criteriu în viitor, ne vedem nevoiţi să analizăm aplicabilitatea acestuia prin raportare la cheia folosită la decriptarea datelor informatice. Aceasta cu atât mai mult cu cât este posibil ca, în cauza *Jalloh c. Germania*, inclusiv faptul că proba obţinută (cocaină) era *per se* incriminatorie să fi contribuit la concluzia Curţii conform căreia privilegiul contra autoincriminării a fost încălcat. Cu toate acestea, în *cauza Saunders*, Curtea a constatat încălcarea privilegiului deși informaţiile furnizate nu erau *per se* incriminatorii.

Astfel, unii ar putea susține teza conform căreia o cheie folosită la criptate / decriptare nu este incriminatorie *per se*, doar datele informatice criptate având această caracteristică. Cu alte cuvinte, s-ar putea invoca faptul că o asemenea cheie este neutrală din perspectivă probatorie, cu excepția situației în care

conținutul acesteia este incriminatoriu (de exemplu, cheia este „*am-dat-mită-10000-euro-judecătorului-în-data-de-10-noiembrie-2012*").

În ceea ce ne privește, un asemenea punct de vedere este eronat și denotă o confuzie la nivelul funcției pe care o are o asemenea cheie. Fie că discutăm despre o parolă, un dispozitiv fizic ori o urmă papilară, cheia pentru criptare / decriptare **are la bază întotdeauna o informație binară ce devine parte a datelor informatice criptate.** De exemplu, dacă datele informatice sunt criptate / decriptate prin intermediul unei urme papilare, procesul constă în scanarea acesteia și preluarea unui cod binar relevant ce oferă unicitate urmei papilare. Cu alte cuvinte, chiar dacă discutăm despre o cheie biometrică (*biometric key*), la bază discutăm tot despre un cod binar format dintr-un șir de „1" și „0".

Dacă se insistă pe ideea că această cheie nu este incriminatorie *per se,* ci doar datele informatice criptate prezintă această caracteristică, atunci nu vedem de ce organele judiciare nu folosesc împotriva persoanei acuzate conținutul criptat (sic!). Orice analogie cu cheia ori codul unui seif este eronată[80], din moment ce **o cheie folosită la decriptate nu este doar mijlocul prin care se accesează conținutul lizibil al datelor informatice ca urmare a decriptării acestora.**

Din punct de vedere tehnic, cheia de criptate / decriptare este o variabilă într-o funcție, alături de datele informatice criptate / necriptate. O criptare absolut elementară poate avea loc prin înlocuirea unei litere din alfabet cu următoarea – A devine B, B devine C, Z devine A etc. Numărul folosit pentru acest schimb reprezintă o variabilă (n) ce reprezintă de fapt cheia pentru criptarea / decriptarea informației. Astfel, dacă n=1 atunci A devine B (A + n) în momentul criptării, iar B devine A în momentul decriptării (A - n). Dacă n=2 atunci A devine C în momentul criptării, iar C devine A în momentul decriptării. Se observă așadar faptul că identificarea conținutului variabilei n implică identificarea cheii de criptare / decriptare. În mod evident, în cazul algoritmilor de criptare moderni, modificarea datelor informatice prin raportare la variabila ce conţine cheia de criptare denotă o complexitate deosebită. Cu toate acestea, concluzia conform căreia cheia afectează conţinutul se menţine.

Această cheie nu este identică – *din perspectiva rolului ei* – cu parola (codul de acces) utilizată pentru autentificarea în cadrul unui sistem de operare ci are inclusiv rolul de a modifica conținutul datelor informatice[81], devenind parte integrantă a funcției de criptare / decriptare. De aceea este eronat a asimila această cheie cu codul unui seif.[82]

În ceea ce privește seiful, codul de acces permite doar deschiderea acestuia fără a produce modificări la nivelul informațiilor conținute de acesta. Exact aceeași funcție o are și parola pentru autentificarea în cadrul unui sistem de operare. Dacă agentul nu cunoaște parola pentru logare nu se va putea loga (autentifica) în cadrul sistemului de operare (*Windows, Linux* etc.). Aceasta nu înseamnă însă că datele informatice nu pot deveni accesibile prin conectarea directă la mijlocul de stocare al acestora. Tocmai de aceea, atunci când se efectuează o percheziție informatică este irelevant dacă utilizatorul are sau nu setată o parolă pentru autentificarea în cadrul sistemului de operare, deoarece specialistul nu va încerca – *de regulă* – o astfel de autentificare ci va interacționa direct cu datele informatice prin montarea mijlocului de stocare (de exemplu, un *hard-disk*) la propriul sistem informatic prin intermediul unui *blocker*. Doar în măsura în care această parolă are inclusiv o funcție de criptare, nu doar de autentificare în cadrul sistemului, ea devine o veritabilă cheie pentru decriptarea datelor informatice.

În ceea ce ne privește, obligarea unei persoane să ofere cheia pentru decriptarea datelor informatice ori remiterea acestora într-un format lizibil / accesibil este similar cu a obliga o persoană să traducă un document[83] într-o limbă cunoscută de organul judiciar. În toate cazurile, ceea ce se dorește este conversia unui conținut ilizibil într-unul lizibil / accesibil prin intermediul constrângerii.

În concluzie, o cheie de criptare / decriptare are două funcții ce se întrepătrund: permite accesul la

---

[80] A se vedea în acest sens P. Reitinger, *Compelled Production of Plaintext and Keys*, în „The University of Chicago Legal Forum", 1996, p. 173, 175; M. Smith apud J. Larkin, *Compelled Production of Ecrypted Data*, în „Vanderbilt Journal of Entertainment and Technology Law", vol. 14, 2012, p. 256; D. Terzian, *The Fifth..., op. cit.*, p. 306.

[81] A se vedea și N. McGregor, *The Weak Protection of Strong Encryption: Passwords, Privacy, and Fifth Amendment Privilege*, în "Vanderbilt Journal of Entertainment and Technology Law", vol. 12, 2010, p. 602.

[82] A se vedea și B. Folkinshteyn, *A Witness Againsts Himself: A case for Stonger Legal Protection of Encryption*, în „Santa Clara High Technology Law Journal", vol. 30, 2014, p. 400-402.

[83] Aspect ce a făcut obiectul cauzei U.S. c. Ragauskas – citată în B. Folkinshteyn, *op. cit.*, p. 399-400.

datele informatice **(1)** într-un format lizibil ca urmare a procesului de decriptare sau *viceversa* **(2).** Tocmai de aceea necesită acceptat faptul că inclusiv cheia de criptare / decriptare este incriminatorie.

Dacă această chestiune ar fi înțeleasă și acceptată de către unii, suntem convinși că nu s-ar mai ajunge la concluzii pripite bazate pe o premisă eronată conform căreia cheia este absolut neutrală din perspectivă probatorie.

Dincolo de faptul că a cunoaște cheia folosită la decriptarea datelor informatice generează o **prezumție rezonabilă**[84] conform căreia persoana ce deține cheia deține și datele informatice criptate prin intermediul acesteia[85], așa cum am precizat *supra,* **aceasta nu este neutră** (nu permite doar accesul) ci devine parte a conținutului criptat (are rol direct în modificarea datelor informatice). În ceea ce ne privește, vedem o asemenea cheie ca reprezentând bucați dintr-un puzzle față de care restul pieselor nu ar putea fi puse în ordine pentru a forma o imagine completă și inteligibilă.

VI. IPOTEZELE ÎN CARE S-AR PUNE PROBLEMA INCIDENŢEI PRIVILEGIULUI CONTRA AUTOINCRIMINĂRII

1. *Atunci când cheia de criptare / decriptare este reprezentată de o parolă care nu se regăsește pe un suport material (aceasta existând doar în memoria unei persoane)*

În ceea ce ne privește, într-o asemenea ipoteză **privilegiul contra autoincriminării ar trebui să își găsească *de plano* aplicabilitatea –** în acest sens s-a statuat și în cauza *Statele Unite c. Kirschner* unde s-a solicitat transmiterea parolei pentru decriptarea datelor informatice**.**[86] Aceasta deoarece obligaţia de a colabora implică în acest caz un element testimonial – **fiind practic necesar a se declara conţinutul cheii pentru decriptarea datelor informatice constând într-un șir de caractere**. Că acest lucru se realizează prin **transmiterea cheii pe cale orală** (ce va rezulta foarte probabil în întocmirea unui proces-verbal) **ori în scris** (prin consemnarea acesteia într-o declaraţie) este absolut irelevant din moment ce discutăm practic despre o informaţie ce **nu are o existenţă independentă faţă de voinţa persoanei** în cauză și **implică un efort cognitiv** din partea acesteia.[87] Din acest punct de vedere, inclusiv prin raportare la jurisprudenţa CtEDO apreciem că nu există niciun impediment în a oferi aplicabilitate privilegiului contra autoincriminării.

Există însă voci ce afirmă faptul că o asemenea cheie nu poate avea o natură testimonială deoarece este creată de suspect și este stocată cel puţin în format electronic pe mediul de stocare criptat.[88] **Se merge așadar pe argumentul potrivit căruia odată stocată informaţia (cheia pentru decriptare), aceasta dobândește o existenţă independentă faţă de voinţa persoanei.**

Se mai susţine faptul că premisa conform căreia o astfel de cheie ar avea o natură testimonială este eronată din moment ce criptarea poate avea loc și prin intermediul unor elemente biometrice. Astfel, se insistă asupra faptului că, procedându-se astfel se creează o distincţie arbitrară ce se află în conflict cu

---

[84] În conformitate cu jurisprudenţa CtEDO (spre exemplu, *cauza Salabiaku c. Franţa*), o prezumție de drept ori de fapt este compatibilă cu art. 6 din Convenție atâta vreme cât este rezonabilă. Astfel, prezumția din dreptul francez (Codul vamal) conform căreia persoana aflată în posesia bunurilor interzise se face vinovată de săvârșirea infracțiunii de contrabandă nu a fost apreciată ca incompatibilă cu prezumția de nevinovăție – vezi în acest sens și P. Mahoney, *op. cit.*, p. 123. **Precizarea este importantă deoarece este greu de crezut că identificarea unor materiale pornografice cu minori pe sistemul informatic aparţinând persoanei acuzate de comiterea infracţiunii de pornografie infantilă nu va genera o prezumție – extrem de dificil de răsturnat – în sensul că aceasta a deținut ori stocat respectivele materiale pornografice.** Prezumția este cu atât mai rezonabilă cu cât respectivele date informatice ce conțineau materiale pornografice cu minori erau criptate, iar persoana acuzată cunoaștea cheia în vederea decriptării acestora. Având în vedere acest context, nu putem să nu luăm în serios necesitatea aplicării privilegiului contra autoincriminării în ipoteze de acest gen.

[85] A se vedea în acest sens I. Smith, *Is the Right Againsts Self-Incrimination Properly Protected in Europe?*, în „International Legal Practitioner", vol. 27, 2002, p. 117.

[86] Citată în A.T. Winkler, *Password Protection and Self-Incrimination: Applying the Fifth Amendment Privilege in the Technology Era*, în „Rutgers Computer and Technology Law Review", vol. 39, 2013, 198-199.

[87] A se vedea și S. Brenner, *Encryption, Smartphones and the Fifth Amendment*, în „Whittier Law Review", vol. 33, 2012, p. 537; C. Bales, *Unbreakeable: The Fifth Amendment and Computer Passwords*, în „Arizona State Law Journal", vol. 44, 2012, p. 1293, 1303-1304. Teza conform căreia dezvăluirea cheii, constând într-un șir de caractere, pentru decriptarea datelor informatice se află sub incidența privilegiului contra autoincriminării a fost acceptată inclusiv în jurisprudența din SUA – a se vedea în acest sens *cauza U.S. c. Kirscher* (citată în C. Bales, *op. cit.*, p. 1301).

[88] J. Larkin, *Compelled Production of Ecrypted Data*, în „Vanderbilt Journal of Entertainment and Technology Law", vol. 14, 2012, p. 269.

scopul privilegiului contra autoincriminării.[89] Nu putem decât să remarcăm încercarea de a exclude cu totul aplicabilitatea privilegiului contra autoincriminării pe motiv că ar fi arbitrar ca acesta să fie aplicabil în unele cazuri, iar în altele nu.

Cu alte cuvinte, autorul pare să sugereze faptul că, în măsura în care privilegiul contra autoincriminării nu este aplicabil tot timpul, este eronat să își găsească aplicabilitatea uneori (sic!). În ceea ce privește criptarea datelor informatice prin intermediul unor elemente biometrice, urmează a ne pronunţa ulterior. Subliniem însă faptul ce este discriminatoriu în a accepta posibilitatea unei aplicări diferenţiate a privilegiului contra autoincriminării în funcţie de modalitatea în care se realizează criptarea / decriptarea datelor informatice.

În ceea ce ne privește, **interpretarea conform căreia privilegiul contra autoincriminării este inaplicabil inclusiv în acele situaţii în care cheia pentru decriptarea datelor informatice este formată dintr-un șir de caractere este excesivă și eronată.**

În primul rând, a exclude aplicabilitatea privilegiului contra autoincriminării în toate acele situaţii în care informaţia a fost notată, scrisă, stocată ori imprimată și pe un suport fizic / material (hârtie, hard-disk etc.) ar reduce enorm sfera de aplicabilitate a privilegiului. Astfel, dacă o persoană își expune gândurile într-un jurnal iar organele judiciare ajung să cunoască acest aspect, privilegiul contra autoincriminării nu ar mai putea produce efecte deoarece gândurile persoanei au dobândit, în momentul transpunerii lor pe hârtie, o existenţă indepententă faţă de voinţa acesteia. În mod evident o asemenea poziţie necesită a fi respinsă în mod cât se poate de categoric. **Dacă această informaţie a dobândit o existenţă independentă faţă de voinţa unei anumite persoane, organele judiciare nu au decât să profite de acest lucru fără a plasa însă această persoană într-un raport obligaţional în care cooperarea activă rămâne în afara sferei de protecţie a privilegiului contra autoincriminării.** O asemenea cooperare implică din punctul nostru de vedere o ingerinţă în mintea unei persoane, aspect apreciat de către CtEDO în repetate rânduri ca fiind inacceptabil.

Dincolo de acestea, chiar dacă informaţia solicitată (cheia pentru decriptare) este stocată într-un format digital ori este imprimată pe un suport fizic, comunicarea acesteia nu implică doar o formă de comunicare ce aduce atingere voinţei unei persoane, ci implică și alte grave urmări.

În primul rând, prin comunicarea acestei chei **se recunoaște implicit (sau chiar explicit) faptul că datele informatice sunt criptate.** Așa cum cum menţionat *supra*, criptarea datelor informatice generează și dificultatea de a identifica faptul că acestea sunt criptate. Aceasta întrucât, procesul de criptare oferă aparenţa că datele informatice reprezintă un șir aleatoriu de biţi. Astfel, colaborarea activă prin oferirea cheii în vederea decriptării datelor informatice oferă răspuns la întrebarea: „*sunt aceste date informatice criptate?*".

Nu în ultimul rând, **oferirea cheii pentru decriptarea datelor informatice implică faptul că respectiva persoană are ori a avut acces la acestea**, fapt ce poate genera o prezumţie conform căreia respectivele date informatice au fost create, modificate ori / și accesate de respectiva persoană.

În consecinţă, chiar dacă am accepta prin absurd faptul că privilegiul contra autoincriminării nu se aplică unei informaţii ce a dobândit o existenţă independentă faţă de voinţa persoanei în cauză, consecinţele de mai sus se datorează unei comunicări implicite ce încălcă fără dubiu voinţa acesteia.

Nu în zadar urmează să analizăm și ipoteza în care cheia de criptare / decriptare este reprezentată de o parolă ce este imprimată pe un suport material (de exemplu, un înscris de mână). Acest lucru este necesar deoarece se pare că argumentul de mai sus asimilează obligativitatea de a transmite cheia pentru decriptarea datelor informatice cu obligativitatea remiterii unor documente, pornind de la ideea că orice cheie este stocată cel puţin pe mijlocul de stocare al datelor informatice criptate.[90]

2. *Atunci când cheia de criptare / decriptare este reprezentată de o parolă ce este imprimată pe un suport material (de exemplu, un înscris de mână)*

În acest caz, analiza are la bază o analogie cu obligația de a remite documente (de exemplu, documente contabile ori bancare). Având în vedere că o bună parte din acest articol a vizat analiza acestei ipoteze, nu mai apreciem ca fiind necesar să reiterăm argumentele pentru care apreciem faptul că privilegiul contra autoincriminării își găsește aplicabilitatea inclusiv în contextul remiterii unor documente / înscrisuri.

În ceea ce ne privește, **inclusiv atunci când discutăm despre un document fizic, constrângerea la**

[89] Idem, p. 270.

[90] J. Larkin, *Compelled..., op. cit.*, p. 270.

cooperare se află în conflict cu privilegiul contra autoincriminării. Deși se poate face o analiză nuanţată în funcţie de natura procedurii (administrativă ori penală) în care sunt solicitate documentele, nu avem nicio ezitare în a respinge inaplicabilitatea *de plano* a privilegiului contra autoincriminării atunci când obiectul constrângerii la cooperare constă în remiterea unui document. Pe parcursul acestui articol am mai menţionat faptul că o interpretare rezonabilă a *cauzei Saunders* denotă faptul că ceea ce se află în afara sferei de aplicabilitate a privilegiului este cooperarea pasivă în contextul obţinerii unor documente în baza unui mandat de percheziţie.

Dincolo de analiza făcută *supra*, se mai poate argumenta faptul că în cazul remiterii unui asemenea înscris discutăm și despre **o componentă testimonială implicită** deoarece persoana care remite înscrisul ca urmare a constrângerii la cooperare, declară implicit faptul că a avut o posesie și un control asupra informației și că aceasta este autentică în sensul că poate produce conținutul într-o formă lizibilă.[91]

3. *Atunci când cheia pentru decriptare este stocată pe un mijloc de stocare a datelor informatice (USB stick, SD card, CD ori DVD etc.)*

În ceea ce ne privește, **concluzia trebuie să fie identică cu cea de mai sus.** Nu vedem nicio diferenţă între obligaţia de a cooperare prin remiterea unui document ori a unui mijloc de stocare a datelor informatice (USB stick, SD card, CD etc.).

4. *Atunci când decriptarea se realizează prin intermediul unor elemente biometrice (de exemplu, urma papilară a utilizatorului sistemului informatic ori vocea acestuia)*

În ceea ce privește urma papilară, în literatura de specialitate s-a susținut faptul că, deși este o probă obținută de pe corpul persoanei în cauză, atunci când aceasta are funcția unei chei pentru decriptarea datelor informatice trebuie să se afle sub incidența privilegiului contra autoincriminării.[92] Argumentul esențial pare a fi acela că, spre deosebire de situațiile tradiționale, în contextul decriptării datelor informatice prin intermediul urmei papilare, aceasta nu este doar un mijloc de identificare al persoanei ci se află într-o legătură directă cu elemente de ordin testimonial cuprinse în informația criptată. De asemenea, **s-a apreciat faptul că urma papilară nu este decât un înlocuitor al cheilor tradiționale (de exemplu, cele constând într-un șir de caractere), motiv pentru care nu s-ar justifica o diferență de tratament**.[93]

A accepta o asemenea concluzie ar face practic aplicabil privilegiul contra autoincriminării pentru orice constrângere la cooperare prin utilizarea unor elemente biometrice – scanarea retinei ori a irisului, utilizarea vocii etc.[94]

În ceea ce ne privește, nu putem să fim atât de categorici în sensul că privilegiul contra autoincriminării urmează să își găsească aplicabilitatea inclusiv prin raportare la urma papilară folosită ca o cheie în vederea decriptării datelor informatice. În măsura în care organele de urmărire penală nu cunosc modalitatea în care se realizează decriptarea, acestea nu pot constrânge persoana să aducă clarificări în acest sens. Aceasta întrucât, o astfel de constrângere la cooperare este în contra voinței persoanei în cauză.

În măsura în care organele judiciare cunosc însă faptul că datelor informatice pot fi decriptate prin intermediul unei urme papilare, aceasta poate fi în principiu obținută fără consimțământul titularului. În acest caz, cooperarea este una pasivă ce nu se află sub incidența privilegiului supus analizei. Astfel, **atâta vreme cât obținerea urmei papilare nu atrage încălcarea art. 3 și art. 8 din Convenție, legalitatea utilizării acesteia nu va fi pusă în principiu în discuție.** Pentru aceasta, apreciem însă că este necesar un cadru normativ adecvat, pentru a exista o conformitate cu exigențele prevederilor art. 8 din Convenție. În lipsa unui asemenea cadru normativ, discuția devine extrem de problematică inclusiv în acest context.

Aceeași concluzie poate fi reținută și în cazul scanării retinei ori irisului în vederea decriptării unor date informatice, ori prin utilizarea unei mostre ADN. Precum în cazul urmei papilare, retina, irisul ori mostra ADN pot reprezenta cheia pentru criptarea / decriptarea unor date informatice.

În ceea ce privește vocea, apreciem că lucrurile se prezintă cu totul diferit. Astfel, spre deosebire de urma papilară, în cazul vocii nu discutăm doar despre analiza caracteristicilor acesteia. Cu alte cuvinte, **nu este**

---

[91] A se vedea în acest sens D. Terzian, *The Fifth...., op. cit.*, p. 304.

[92] A se vedea în acest sens K. Goldman, *Biometric Passwords and the Privilege Against Self-Incrimination*, în „Cardozo Arts & Entertainment", vol. 33, 2015, p. 226.

[93] Idem, p. 228.

[94] Idem, p. 234.

importantă doar forma (caracteristile vocii) ci și conținutul (mesajul vocal transmis și analizat).[95] În acest context, conținutul are o natura testimonială ce se află într-o relație indisolubilă cu voința persoanei ce face obiectul constrângerii la cooperare.

Având în vedere faptul că persoana constrânsă nu are posibilitatea de a rosti orice, ci este nevoită să folosească exact conţinutul cheii, concluzia în ceea ce privește aplicabilitatea privilegiului contra autoincriminării ar trebui să fie identică cu cea de la pct. 1 (cheia constă într-un șir de caractere și se regăsește doar în memoria persoanei).

În măsura în care procesul de autentificare implică doar o analiză a caracteristicilor vocii, cheia vocală fiind independentă de conținut, argumentul de mai sus și-ar putea pierde din autoritate. Aceasta întrucât, într-o asemenea ipoteză mostra de voce este precum acea mostră oferită în vederea expertizării vocii pentru a se stabili identitatea persoanei. Or, în ceea ce privește acest aspect, este larg acceptată teza conform căreia privilegiul contra autoincriminării nu își găsește aplicabilitatea.

Analiza este similară și în ceea ce privește „semnătura" unei persoane. În măsura în care autorităţile cunosc semnătura necesară în vederea decriptării datelor informatice, nu vedem neapărat o problemă în obţine respectiva semnătură de la titular prin intermediul unei constrângeri la cooperare compatibilă cu prevederile art. 3 și 8 din Convenţie. Altfel, obligarea unei persoane să folosească semnătura necesară (semnătură ce poate avea orice conţinut) în vederea decriptării datelor informatice, implică un element cât se poate de testimonial ce se află practic sub protecţia privilegiului contra autoincriminării.

Necesită reţinut faptul că **elementele biometrice prezintă caracteristici aparte ce le diferenţiază de cheile tradiţionale pentru decriptarea datelor informatice.** Astfel, dacă o parolă este ușor transmisibilă, cheia constând într-un element biometric (urmă papilară, semnătură, voce etc.) se află practic într-o relaţie de interdependenţă cu titularului acestuia. Deși nu excludem posibilitatea ca inclusiv o asemenea cheie să devină transmisibilă (înregistrarea vocii și remiterea acesteia pe un suport optim de redare), apreciem că este cât se poate de rezonabil a conchide că doar persoana care se identifică printr-un anumit element biometric se află în posesia cheii pentru decriptarea datelor informatice. Această observaţie este extrem de relevantă în contextul în care discutăm despre o componentă testimonială implicită, fiind greu de crezut că decriptarea datelor informatice incriminatorii prin utilizarea vocii unei persoane nu implică o recunoaștere implicită a faptului că respectivele date îi aparţin și au fost criptate de către aceasta.

5. *atunci când se solicită decriptarea nemijlocită a datelor informatice și remiterea acestora într-un format accesibil / lizibil*

În jurisprudența din SUA s-a apreciat că atunci când organele judiciare nu cunosc ce date conține mijlocul de stocare nu pot solicita remiterea acestuia ori a unei copii după acesta într-o formă lizibilă (necriptată).[96] În sens contrar, se aplică teoria *foregone conclusion*, iar privilegiul contra autoincriminării devine inaplicabil (în acest sens, cauza *Statele Unite c. Fricosu*[97]). În ceea ce ne privește, **este absolut indiferent dacă organele judiciare au ori nu cunoștinţă despre conţinutul datelor criptate ori faptul că acestea sunt criptate.**

Am mai afirmat anterior în acest articol faptul că procesul de criptare face ca inclusiv identificarea acesteia să devină improbabilă. În consecinţă, în măsura în care organele judiciare bănuiesc faptul că datele informatice sunt criptate și solicită predarea acestora într-un format lizibil, această predare denotă și o componentă „testimonială". În măsura în care o persoană este obligată să coopereze prin remiterea nemijlocită a conţinutului necriptat, e ca și cum aceasta ar declara faptul că: **1.** Da, conţinutul este unul criptat și **2.** Da, conţinutul îi aparţine. Cu alte cuvinte, remiterea datelor informatice într-un format necriptat (lizibil) reprezintă un **act de producere** a unor mijloace probatorii ce confirmă existenţa (materialului incriminator), posesia, controlul și autenticitatea. Din acest punct de vedere, apreciem ca fiind dincolo de orice dubiu că **acest act de producere are o componentă cât se poate de testimonială.**

Chiar dacă se respinge acest argument, apreciem faptul că o persoană nu poate fi obligată să remită conţinutul într-un format lizibil atâta vreme cât privilegiul contra autoincriminării se aplică și ipotezei în

---

[95] A se vedea E.M. Sales, *The „Biometric Revolution": An Erosion of the Fifth Amendment Privilege to Be Free from Self-Incrimination*, în „University of Miami Law Review", vol. 69, 2014-2015, p. 216-217.

[96] A se vedea în acest sens *In re: Grand Jury Subpoena Duces Tecum (11th Circuit 2012),* citată în D. Terzian, *The Fifth..., op. cit.*, p. 300 și urm.

[97] Citată în A. T. Winkler, *op. cit.,* p. 202-203.

care se solicită predarea unor documente. Din această perspectivă, putem discuta despre refuzul de a remite documente ori / și înscrisuri digitale. Ne este greu de crezut că un înscris în format tipărit ar intra în sfera de incidenţă a privilegiului, dar același înscris scanat și stocat pe un mijloc de stocare a datelor informatice ori creat direct prin intermediul unui sistem informatic ar putea face obiectul unei constrângeri la cooperare fără a exista o încălcare a art. 6 din Convenţie.

O altă problemă este aceea că solicitarea de a remite toate datele informatice criptate implică *per se* riscul de a obliga persoana în cauză în a remite inclusiv date informatice al căror conţinut nu prezintă absolut nicio relevanţă în cauză.[98] Pe de altă parte, dacă organele judiciare solicită decriptarea doar a anumitor date informatice (de exemplu, a materialelor cu pornografie infantilă), persoana în cauză este pusă în situaţia de a face o selecţie ce are o natură testimonială. Situaţia este similară cu cea în care o persoana este obligată să remită anumite documente, fiind astfel nevoită să facă o selecţie printre o sumedie de alte documente. Selectarea materialelor cu conținut pornografic implică o recunoaștere a faptului că anumite materiale digitale au un asemenea conținut.

Aspectul esenţial îl apreciem totuși ca fiind acela că datele informatice în formă necriptată nu există decât în momentul în care s-a utilizat cheia pentru decriptarea datelor informatice. În mod evident, organele judiciare ar solicita remiterea nemijlocită a conţinutului necriptat atunci când acestea nu au acces decât la conţinutul criptat. **Or, în ceea ce ne privește, obligarea la decriptarea datelor informatice implică practic un proces de „creare a informaţiei incriminatorii".** Susţinem acest lucru deoarece, în principiu, datele criptate nu pot fi folosite ca probe în acuzare deoarece nu au un conţinut susceptibil de a fi interpretat într-un sens sau altul. Situaţia se schimbă radical atunci când aceste date sunt decriptate, deoarece în acel moment conţinutul ilizibil dobândește valenţă probatorie.[99]

Cu alte cuvinte, obligarea unei persoane de a decripta conţinutul implică faptul că respectiva persoană este pusă în situaţia de a (re)crea informaţia incriminatorie prin procesul de decriptare. Or, în ceea ce ne privește, o asemenea constrângere la cooperare reprezintă o încălcare vădită a privilegiului contra autoincriminării.

VII. O CONCLUZIE ATIPICĂ

Tehnologia reprezintă arsenalul tuturor persoanelor capabile să o înţeleagă și să o utilizeze. Organele de urmărire penală se folosesc de orice evoluţie tehnologică în vederea combaterii ori prevenirii criminalităţii, în vreme ce potenţialii suspecţi își criptează comunicările și datele informatice în vederea îngreunării activităţii organelor de urmărire penală.

Cu alte cuvinte, tehnologia reprezintă un atuu ce se transformă într-un obstacol, în funcţie de entitatea la care ne raportăm. În ceea ce ne privește, posibilitatea de a apela la noua tehnologie în vederea strângerii de probe necesită o regândire a modului în care ne raportăm la dreptul la viaţă privată. Aceasta întrucât, organele de urmărire penală au la dispoziţie mijloace tot mai intruzive iar de multe ori, acestea nu sunt folosite ca *ultima ratio* ci mai degrabă reprezintă regula într-o anchetă penală.

În acest context, apreciem ca fiind un dezechilibru în ceea ce privește egalitatea armelor atunci când se susţine faptul că tehnologia folosită în detrimentul organelor de urmărire penală reprezintă o problemă ce poate fi soluţionată doar prin restrângerea drepturilor cetăţenești. Dacă în ceea ce privește dreptul la viaţă privată o asemenea restrângere își poate găsi justificarea în anumite limite, suntem de părere că reducerea dreptului de a nu participa la propria incriminare (privilegiul contra autoincriminării) la statutul de drept iluzoriu în contextul criptării datelor informatice reprezintă un real regres în materia respectării drepturilor omului.

Dincolo de argumentele *pro* sau *contra*, rămânem la părerea că privilegiul contra autoincriminării rămâne o garanţie extrem de importantă în ceea ce privește dreptul la un proces echitabil, iar riscul de a transforma suspectul, inculpatul ori martorul devenit ulterior suspect sau inculpat într-un agent al statului prin instituirea unui raport obligaţional între acesta și organele de urmărire penală lipsește de conţinut o regulă elementară a procesului penal și anume aceea că organele de urmărire penală și doar acestea au obligaţia de a proba conduita infracţională. A lipsi orice persoană de protecţia conferită de art. 6 din Convenţie atunci când apare problema

[98] A se vedea în acest sens inclusiv L. Larkin, *Compelled... op. cit.*, p. 272.

[99] A se vedea în acest sens și N. McGregor, *The Weak Protection... op. cit.*, p. 602.

unor date informatice criptate reprezintă o „pantă alunecoasă" ce va avea grave repercusiuni în acea eră în care digitalul va absorbi cu totul tradiţionalul în materia probaţiunii.

NOTA REDACŢIEI: *Având în vedere faptul că problematica relației existente între privilegiul contra autoincriminării și criptografie a fost abordată pentru prima dată în literatura de specialitate autohtonă în acest articol, așteptăm cu interes orice notă, analiză sumară ori in extenso cu privire la acest subiect, în vederea publicării.*

Facem de asemenea precizarea că prezentul articol a fost redactat cu mult timp înaintea evenimentelor tragice din Paris (noiembrie 2015). Opiniile regăsite în acest articol aparţin în întregime autorului, iar acesta ţine să precizeze faptul că indiferent de contextul actual, ideile regăsite în conţinutul prezentului articol își păstrează valabilitatea deoarece, în opinia acestuia, emoţiile puternice nu ar trebui niciodată să suprime esența dreptului la un proces echitabil. Din punctul de vedere al autorului, soluția nu este abolirea drepturilor omului ci combaterea terorismului prin alte mecanisme decât cele specifice sistemului judiciar.

În momentul în care Curtea Europeană a Drepturilor Omului nu va înțelege acest lucru și va deveni sentimentală, Convenţia va ajunge o compilaţie romantică de drepturi iluzorii

References / Bibliografie

Ashworth, A., *Self-Incrimination in European Human Rights Law – A Pregnant Pragmatism?*, în „Cardozo Law Review", vol. 30, 2008-2009

Bales, C., *Unbreakeable: The Fifth Amendment and Computer Passwords*, în „Arizona State Law Journal", vol. 44, 2012

Berger, M., *Europeanizing Self-incrimination: The Right to Remain Silent in the European Court of Human Rights*, în „Columbia Journal of European Law", vol. 12, 2006

Berger, M., *Self-Incrimination and the European Court of Human Rights: Procedural Issues in the Enforcement of the Right to Silence*, în „European Human Rights Law Review", nr. 5, 2007

Bodoroncea, G., Cioclei, V., Kuglay, I. ș.a., *Codul penal. Comentariu pe articole*, Ed. C.H. Beck. București, 2014

Bogdan, S., Șerban, D.A., Zlati, G., *Noul Cod penal. Partea specială*, Ed. Universul Juridic, București, 2014

Brenner, S., *Encryption, Smartphones and the Fifth Amendment*, în „Whittier Law Review", vol. 33, 2012, p. 537

Casey, E., ș.a., *The growing impact of full disk encryption on digital forensics*, în „Digital Investigation", vol. 8, 2011

Chiriță, R., *Dreptul la tăcere și privilegiul contra autoincriminării*, în „Caiete de drept penal", nr. 4/2006

Choo, A., *The Privilege against self-incrimination and Criminal Justice*, Hart Publishing, Oxford, 2013

Folkinshteyn, B., *A Witness Againsts Himself: A case for Stonger Legal Protection of Encryption*, în „Santa Clara High Technology Law Journal", vol. 30, 2014

Goldman, K., *Biometric Passwords and the Privilege Against Self-Incrimination*, în „Cardozo Arts & Entertainment", vol. 33, 2015

Ionescu, D., *Gäfgen c. Germania:* un moment de reflecţie şi multe întrebări, în „Caiete de drept penal", nr. 4/2012

Larkin, J., *Compelled Production of Ecrypted Data*, în „Vanderbilt Journal of Entertainment and Technology Law", vol. 14, 2012

Mahoney, P., *Right to a Fair Trial in Criminal Matters Under Article 6 E.C.H.R.*, în „Judicial Studies Institute Journal", vol. 4, nr. 2, 2004

Mateuț, Gh., Ionescu, D., *Inadmisibilitatea utilizării ca mijloc de probă în procesul penal a proceselor-verbale și a actelor de constatare obținute în procedurile administrative de control*, în „Caiete de drept penal", nr. 1/2005

McGregor, N., *The Weak Protection of Strong Encryption: Passwords, Privacy, and Fifth Amendment Privilege*, în "Vanderbilt Journal of Entertainment and Technology Law", vol. 12, 2010

Oltmann, S.M., *Encryption and Incrimination: The Evolving Status of Ecrypted Drives*, în „Bulletin of the Association for Information Science and Technology", nr. 2, vol. 40, 2014

Oprea, M., *Infracțiuni contra înfăptuirii justiției*, Ed. Universul Juridic, București, 2015

Pușcașu, V., *Dreptul la tăcere și la neautoincriminare*, Ed. Universul Juridic, București, 2015

Pușcașu, V., *Prezumția de nevinovăție*, Ed. Universul Juridic, București, 2010

Redmayne, M., *Rethinking the Priviledge Against Self-Incrimination*, în „Oxford Journals of Legal Studies", vol. 27, nr. 2, 2007

Reitinger, P., *Compelled Production of Plaintext and Keys*, în „The University of Chicago Legal Forum", 1996

Sales, E.M., *The „Biometric Revolution": An Erosion of the Fifth Amendment Privilege to Be Free from Self-Incrimination*, în „University of Miami Law Review", vol. 69, 2014-2015

Seet, M., *Suspected Terrorists and the Privilege Againsts Self-Incrimination*, în „Cambridge Law Journal", vol. 74, nr. 2, 2015

Smith, I., *Is the Right Againsts Self-Incrimination Properly Protected in Europe?*, în „International Legal Practitioner", vol. 27, 2002

Soares, N., *The Right to Remain Encrypted: The Self-Incrimination Doctrine in the Digital Age*, în „American Criminal Law Review", vol. 49, 2012

Terzian, D., *The Fifth Amendment, Encryption, and the Forgotten State Interest*, în „UCLA Law Review Discourse", vol. 61, 2014

Udroiu, M., (coord.), *Codul de procedură penală. Comentariu pe articole*, Ed. C.H. Beck, București, 2015

Udroiu, M., Predescu, O., *Protecția europeană a drepturilor omului și procesul penal român. Tratat*, Ed. C.H. Beck, București, 2008

Udroiu, M., *Principiile fundamentale cuprinse în Proiectul noului Cod de procedură penală – spre un nou model de proces penal*, în „Caiete de drept penal", nr. 2/2009

Voicu, C., Uzlău, A.S., Tudor, G., Văduva, V., *Noul Cod de procedură penală. Ghid de aplicare pentru practicieni*, Ed. Hamangiu, București, 2014

Volonciu, N., Vasiliu, A., Gheorghe, R., *Noul Cod de procedură penală adnotat. Partea generală*, Ed. Universul Juridic, București, 2014

Winkler, A.T., *Password Protection and Self-Incrimination: Applying the Fifth Amendment Privilege in the Technology Era*, în „Rutgers Computer and Technology Law Review", vol. 39, 2013

Zlati, G., *Percheziția sistemelor informatice și a mijloacelor de stocare a datelor informatice (I)*, în „Caiete de drept penal", nr. 3/2014