Analiza juridică a infracțiunii de fals informatic

Autor: asist.univ.dr. Maxim DOBRINOIU

From the very beginning, IT systems have been an attraction to those interested in business development, but in the same time made a turning point to those who envisaged in running the modern technology an easy way to get hold of undeserved profit.

Notable the fact that, in the same way the new information technologies have been gradually applied to traditional industrial tasks with the aim to automate certain activities or processes, the computer systems were initially used to facilitate the commission of traditional criminal offences, and thus we witnessed the emerging of real new form of crimes, computer-related crimes.

Such a crime is computer-related forgery. Coming up initially as a smart method of committing traditional forgery offences (as stated in 6th Title of the Criminal Code), computer forgery had a significant development along with technology evolution. Nowadays, almost nobody has an interest in forging a document with the help of dedicated software and a printer, but for simulating or spoofing a person's identity, banks account records, financial transactions or digital communications.

Încă de la primele arhitecturi, sistemele informatice au constituit o atracție pentru cei interesați de dezvoltarea economică, dar în acelaşi timp au suscitat interesul acelora care au văzut în exploatarea tehnologiei moderne o modalitate facilă de a dobândi foloase necuvenite.

Interesant este faptul că, în acelaşi mod în care noile tehnologii informaționale au fost gradual aplicate vechilor sarcini industriale în scopul automatizării unor activități sau procese de producție, sistemele de calcul au fost inițial utilizate pentru a perfecționa modul de comitere a unor infracțiuni tradiționale, pentru ca în cele din urmă să asistăm la apariția unor noi forme de criminalitate, specifice domeniului informatic.

O astfel de infracțiune este şi falsul informatic. Apărută inițial ca un mijloc inteligent de comitere a infracțiunilor prevăzute în Titlul VII (infracțiuni de fals) al Codului Penal, fapta a cunoscut ulterior o dezvoltare semnificativă în pas cu evoluția tehnologică. Astăzi aproape că nu mai prezintă importanță realizarea unui document fals cu ajutorul unei simple aplicații de prelucrare a imaginilor şi o imprimantă în fața posibilității de a falsifica (sau simula) identitatea unei persoane, conturi bancare, tranzacții financiare sau comunicații electronice.

§1. Conținutul legal

Constituie infracțiunea prevăzută de art. 48[1] fapta de a introduce, modifica sau şterge, fără drept, date informatice ori de a restricționa, fără drept, accesul la aceste date, dacă fapta are ca rezultat obținerea de date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecințe juridice.

§2. Condiții preexistente

1. Obiectul infracțiunii

Obiectul juridic special constă în relațiile sociale referitoare la încrederea publică în siguranța şi fiabilitatea sistemelor informatice, la valabilitatea şi autenticitatea datelor informatice, a întregului proces modern de prelucrare, stocare şi tranzacționare automată a datelor de interes oficial sau privat.

Datele informatice au dobândit un rol important în societatea actuală. Ele contribuie la facilitarea contactelor sociale şi la o mai bună comunicare între persoane fizice sau juridice, în conformitate cu exigențele statului de drept şi interesele individuale ale cetățenilor[2].

Obiectul material este reprezentat de datele informatice asupra cărora îşi îndreaptă atenția făptuitorul. Datele informatice care apar pe monitor sau la imprimantă sub formă de caractere alfanumerice cu înțeles pentru utilizatori sunt reprezentate la „nivel fizic" (al maşinii de calcul) sau pe suportul de stocare de a înşiruire logică de stări „0" şi „1" corespunzătoare unor variații de tensiune. Acționând asupra acestor date (sau introducând unele noi) este echivalent cu a acționa (prin intermediul procesorului) asupra înşiruirii de „0" şi „1" şi, implicit, asupra mediilor de stocare (*Hard Disk*, *floppy-disk*, memorie *flash*, CD, DVD etc.).

2. Subiecții infracțiunii

Subiectul activ (autorul) poate fi orice persoană responsabilă penal. Manipulările frauduloase de acest gen sunt, în general, realizate de către inițiați în ştiința calculatoarelor ori de persoane care, prin natura serviciului, au acces la date şi sisteme informatice[3].

Participația este posibilă în toate formele sale: coautorat, instigare ori complicitate.

În cazul acestei infracțiuni, subiectul pasiv va fi persoana fizică sau juridică prejudiciată în propriile interese şi față de care se produc consecințe juridice (de ordin patrimonial, moral ori social) în urma contrafacerii datelor informatice.

Subiect pasiv adiacent (secundar) va fi proprietarul, deținătorul de drept ori utilizatorul autorizat al sistemului informatic.

---

[1] Conținut legal identic cu cel al art. 445 din noul Cod penal.
[2] A se vedea M. Dobrinoiu, în *V.Dobrinoiu şi colaboratorii*, Drept Penal – curs universitar, p. 542.
[3] Noul Cod penal prevede că subiect activ al infracțiunilor informatice poate fi şi persoana juridică.

§3. Conținutul constitutiv

1. Latura obiectivă

1.1. Elementul material

Elementul material se realizează printr-o acțiune alternativă de introducere, modificare sau ştergere de date informatice, ori de restricționare a accesului la aceste date. Întrucât aceste modalități normative au fost analizate în cadrul infracțiunii de alterare a integrității datelor informatice, fac trimitere la explicațiile de la respectiva subsecțiune[4].

Actele prin care se realizează elementul material al infracțiunii implică efecte negative asupra stării datelor în ce priveşte capacitatea lor de a funcționa şi atesta fapte ori situații de maniera prevăzută de persoana care dispune de ele, ajungându-se la o situație care corespunde fabricării unor documente false sau falsificării unor documente autentice[5].

Cu titlu de exemplu, falsificarea datelor informatice s-ar putea realiza sub următoarele forme:

a) inserarea, modificarea sau ştergerea de date în câmpurile unei baze de date existente la nivelul unui centru de evidență informatizată a persoanei, unei bănci sau societăți de asigurări etc., prin acțiunea directă a făptuitorului asupra tastaturii ori prin copierea datelor de pe un suport de stocare extern;

b) alterarea documentelor stocate în format electronic, prin modificarea sau ştergerea directă a cuvintelor etc.

Într-o abordare tehnică mai complexă, falsul informatic va lua una din următoarele forme: simularea poştei electronice; simularea hyperconexiunilor; simularea *Web*-ului.

A. Simulare (SPOOFING)[6]

Serviciile Transport Control Protocol (TCP) şi *Uniform Datagram Protocol* (UDP) presupun că adresa Internet Protocol (IP) a unui *host* este validă şi, ca atare, este credibilă. Totuşi, un *host* hacker poate folosi rutarea sursei IP pentru a se da drept client sau *host* credibil. Un hacker poate folosi rutarea sursă IP pentru a specifica o rută directă spre o destinație şi o cale de revenire înapoi la origine. Ruta poate include *routere* sau *host*-uri care în mod normal nu se folosesc pentru a transmite un pachet la destinație. Astfel, hackerul poate intercepta sau modifica transmisiile fără a întâlni pachetele destinate *host*-ului veritabil. Exemplul următor prezintă modul în care sistemul unui hacker poate fi disimulat drept client credibil al unui anumit server:

Pasul 1: hackerul va modifica adresa IP a *host*-ului fals pentru a corespunde adresei clientului credibil.

Pasul 2: hackerul construieşte o rută sursă către server care conține calea directă a pachetelor IP către server şi înapoi de la server către *host*-ul hacker, folosind clientul credibil drept ultim hop în drumul către server.

---

[4] A se vedea *supra*, pct.2.4.

[5] *I.Vasiu, L.Vasiu*, Informatica juridică şi drept informatic, Ed. Albastră, 2002, p. 169.

[6] *L. Klander*, Antihacker, Ed. All Educational 1999, p. 262.

Pasul 3: hackerul foloseşte ruta sursă pentru a trimite către server o cerere client.

Pasul 4: serverul acceptă cererea clientului ca şi când cererea ar fi venit direct de la clientul credibil, iar apoi returnează un răspuns către clientul credibil.

Pasul 5: clientul credibil, folosind ruta sursă, transmite pachetul către *host*-ul hacker.

O metodă mai simplă este de a aştepta până când sistemul client se închide şi apoi de a lua locul acestuia. În multe firme, membrii personalului folosesc calculatoare personale şi programe de reţea TCP/IP pentru a se conecta la *host*-uri *Unix*, respectiv a le utiliza ca servere LAN. Calculatoarele personale folosesc deseori fişierul sistem de reţea *NSF Unix* pentru a obţine acces la cataloagele şi fişierele serverului (NFS foloseşte adrese IP numai pentru autentificarea clienţilor). Un hacker poate trece drept client şi poate configura un calculator personal cu nume şi adresă IP identice cu cele ale unui alt calculator, apoi poate iniţia conexiuni cu *host*-ul *Unix*. Atacatorul poate realiza cu uşurinţă această operaţiune. De asemenea, atacul va fi „din interior", deoarece numai o persoană din interior ştie care sunt calculatoarele închise într-o reţea protejată.

B. Atacul prin disimulare

În cadrul atacului prin disimulare (*masquerade attack*) hackerul iniţiază sesiunea prin transmiterea unui pachet *SYN* (sincronizare) către server folosind adresa IP a clientului ca adresă sursă. Adresa transmisă de hacker trebuie să fie aceea a unui *host* credibil. Serverul va conforma pachetul *SYN* printr-un pachet *SYN ACK*.

Hackerul va conforma pachetul *SYN/ACK* al serverului cu propriul său pachet. Pachetul hackerului va conţine valoarea presupusă a numărului de secvenţă „SVR_SEQ_0". Pentru a avea succes, hackerul nu trebuie să intercepteze pachetele client, deoarece poate anticipa secvenţa „SVR_SEQ_0" şi, ca atare, îl poate confirma. Atacul prin disimulare are următoarele etape:

Etapa 1: clientul simulat de hacker va primi pachetul *SYN/ACK* de la server şi apoi poate genera un pachet *RST* (*reset*) către server deoarece, din punctul de vedere al clientului, nu există nicio sesiune. Potenţial, un hacker poate opri generarea *RST* de către client fie prin efectuarea unui atac în momentul când calculatorul clientului nu este conectat la reţea, fie prin depăşirea cozii TCP a clientului (folosind o variantă a atacului prin desincronizare cu date nule), astfel că adevăratul client va pierde pachetul *SYN/ACK* de la server.

Etapa 2: hackerul nu poate primi date de la server. Totuşi, hackerul poate transmite date, ceea ce uneori poate compromite un *host*.

Totuşi, dacă clientul este *off-line* sau incapabil de a recepta şi transmite pachete RST, hackerul poate folosi atacul prin disimulare pentru a stabili o conexiune TCP duplex cu serverul. Hackerul poate transmite şi primi date în numele clientului. Desigur, hackerul trebuie să treacă de bariera de identificare. Dacă sistemul foloseşte o identificare bazată pe *host*-uri credibile, cum este sistemul fişier de reţea (*network file system - NFS*) sau comanda *Unix rlogin*, hackerul va primi acces complet la serviciile *host*-ului.

Deşi deturnarea prin post-sincronizare este simplu de detectat pentru un administrator de sistem când hackerul îşi îndreaptă atacul împotriva unei reţele locale, acest tip de atac este eficient pentru reţele pe distanţe mari (cum ar fi un WAN de firmă). De asemenea, un hacker poate duce la îndeplinire un atac prin deturnare cu

desincronizarea datelor folosind aceleaşi resurse ca în cazul unor atacuri pasive prin interceptare, frecvent întâlnite pe Internet. Atât deturnarea prin post-sincronizare, cât şi atacul prin disimulare au avantajul că sunt invizibile pentru client. Invizibilitatea pentru utilizator este importantă deoarece, în condițiile în care operațiile de *hacking* într-un *host* de Internet sunt tot mai frecvente şi securitatea de rețea devine tot mai riguroasă, dibăcia unui atacator devine un element important în reuşita atacului.

C. Simularea Email-ului

Poşta electronică pe Internet este deosebit de simplu de simulat, motiv pentru care, în general, mesajele email nu pot fi credibile în lipsa unor facilități cum sunt semnăturile digitale. Ca exemplu, să considerăm schimbul de mesaje între două *host*-uri Internet. Schimbul se produce folosind un protocol simplu care foloseşte comenzi cu caractere *ASCII*. Un intrus poate introduce cu uşurință aceste comenzi manual, conectându-se prin Telnet direct la portul *Simple Mail Transfer Protocol* (*SMTP*). *Host*-ul receptor are încredere în identitatea *host*-ului emițător, astfel că hackerul poate simula cu uşurință originea mesajului prin introducerea unei adrese a emițătorului diferită de veritabila adresă a hackerului. În consecință, orice utilizator fără privilegii poate falsifica sau simula mesaje de email.

D. Simularea Hiperconexiunilor

În secțiunile anterioare s-a discutat despre unele atacuri hacker împotriva comunicațiilor TCP şi Telnet. Această secțiune, care discută simularea hiperconexiunilor, precum şi următoarea, care detaliază simularea în *Web*, explică unul dintre atacurile folosite de hackeri împotriva calculatoarelor care comunică prin protocolul de transport pentru *hypertext* (*HTTP*). Hackerii pot construi atacuri asupra protocolului de autentificare a serverului *Secured Socket Layer* folosit la crearea de *browsere* şi servere de *Web* sigure, cum sunt cele ale firmelor *Microsoft* şi *Netscape*. Un hacker poate convinge *browser*-ul să se conecteze la un server fals, în acest timp, *browser*-ul prezentând aspectul obişnuit al unei sesiuni sigure. Un hacker „intermediar” este un hacker care se introduce în fluxul de pachete, între client şi server. Ca apoi să convingă utilizatorul să dezvăluie informații (gen numere de cărți de credit, numere de identificare personale pentru telefoanele mobile etc.) către serverul fals. Un alt risc la simularea hiperconexiunii este acela că utilizatorul (de exemplu un client bancar sau bază de date) poate transfera şi rula *applet*-uri Java rău intenționate de pe falsul server, având convingerea că acestea provin de la serverul adevărat şi sunt, implicit, sigure.

Se reține că atacul prin simularea hiperconexiunii exploatează un neajuns în modul în care majoritatea *browser*-elor folosesc certificate digitale pentru securizarea sesiunilor *Web*. Atacul prin simularea hiperconexiunii nu este orientat numai asupra criptografiei de nivel scăzut sau asupra funcționalității protocolului *SSL*. În consecință, atacul poate fi îndreptat şi împotriva altor aplicații securizate cu certificat digital, în funcție de modul în care aceste aplicații îşi folosesc certificatele.

Hackerii se pot „transforma” în orice server cu facilități *SSL* folosind convențiile de certificat obişnuite sau prin accesarea *browser*-elor prezentate anterior. De asemenea, certificatele server, cum ar fi cele de la *Verisign* sau *Thawte* sunt susceptibile la atacul prin simularea hiperconexiunii atunci când *browser*-ul foloseşte *Internet Explorer* sau *Netscape*.

Aşa cum am mai arătat, când un utilizator creează o conexiune *SSL*, *browser*-ul şi serverul partajează un protocol pentru autentificarea serverului şi, opțional,

a clientului. Atacul prin simularea hiperconexiunilor se concentrează numai asupra autentificării serverului. Certificatul serverului este o structură cu semnătură digitală care oferă anumite atribute cheii publice a serverului.

Atacul prin simularea hiperconexiunilor reuşeşte deoarece majoritatea utilizatorilor nu obişnuiesc să se conecteze la nume *DNS* sau *URL*-uri, ci urmează traseul hiperconexiunilor. Dar, instalarea curentă a unui *SSL* verifică numai porțiunea de server a *URL*-ului, nu şi hiperconexiunea pe care utilizatorul a efectuat *click* (care poate reprezenta orice, un text sau o imagine).

Aşa cum numele DNS sunt subiecte ale simulării DNS (adică un server DNS oferă o adresă de Internet falsă), la fel şi URL-urile sunt expuse simulării hiperconexiunilor, caz în care, o pagină indică un nume DNS fals al unui URL. Ambele forme de simulare duc la un alt site Internet decât cel dorit. Totuşi, simularea hiperconexiunilor este mai simplă din punct de vedere tehnic decât simularea DNS. De exemplu, un hacker poate alimenta un *browser* cu cod HTML după cum urmează: <A HREF=https://www.hacker.com/infogatherer/>This way to free books!</A>.

Se obține o conexiune pe care scrie „Pe aici către cărți gratuite”. Totuşi, dacă se efectuează *click* pe hyperconexiune, aceasta va trimite utilizatorul către un alt server sigur (la „hacker.com”), la un director numit *infogatherer*. *Browser*-ele reale vor detecta existența unei conexiuni sigure şi vor prezenta pictograme ca atare, dar utilizatorul tocmai a căzut victimă unui hacker. Hackerul a folosi anumite trucuri pentru a cere *browser*-ului să indice utilizatorului existența unei conexiuni private cu serverul propus.

Din păcate, chiar dacă utilizatorul are o conexiune privată, aceasta este stabilită cu un alt server. Desigur, site-ul *infogatherer* nu dispune de cărți gratuite, dar, în cazul unui atac real, hackerul va controla destinația, căreia îi va da aspectul paginii *Web* reale, destinație care în final va cere utilizatorului numărul cărții de credit înainte de a-i trimite acestuia cărțile gratuite. Dacă utilizatorul examinează meniurile *browser*-ului şi vizualizează sursa documentului sau informația despre document, va observa că identitatea autentificată a serverului nu este cea presupusă.

Pe măsură ce utilizarea certificatelor server devine tot mai extinsă, simularea autentificării serverului devine mai simplă. Pe măsură ce tot mai multe servere dispun de certificate, hackerii vor avea de ales între mai multe site-uri care vor putea redirecta un utilizator *Web* neatent. De asemenea, mulți utilizatori vor dezactiva casetele dialog privind certificatele, dacă *browser*-ul îi va înştiința pe aceştia la fiecare intrare într-o pagină *Web*. Dacă fiecare conexiune şi document sunt sigure, atunci faptul că utilizatorul a solicitat un document sigur nu este de mare ajutor, în sensul că verificarea conexiuni server devine lipsită de sens.

Hackerul nu doreşte să trimită utilizatorul la site-ul său sigur (oferind, astfel, certificatul şi un indiciu serios asupra identității sale). Hackerul îl poate trimite pe utilizator către cutia SSL a altcuiva, cutie în care hackerul a intrat în prealabil. Hackerul îl mai poate trimite pe utilizator într-o altă regiune a site-ului sigur unde acesta dorea să se deplaseze, cu alte cuvinte, URL-ul poate fi „*/attacpage*” în loc de „*/securepage*”. Acest timp de inducere în eroare poate surveni pe site-uri *Web* cu *host*-uri virtuale sau site-uri *Web* unde URL-urile reprezintă scripturi CGI sau clase Java, dintre care unele controlate de hacker în mod legitim.

E. Simularea WEB-ului

Simularea *Web*-ului este un alt tip de atac hacker. La simularea *Web*-ului, hackerul creează o copie convingătoare, dar falsă a întregului *Web*. *Web*-ul fals este o reproducere exactă a celui veritabil, adică are exact acelaşi pagini şi conexiuni ca şi adevăratul *Web*. Cu toate acestea, hackerul controlează integral falsul *Web*, astfel încât întregul trafic de rețea între *browser*-ul victimei şi *Web* trece prin sistemul hacker.

La executarea unei simulări a *Web*-ului, hackerul poate observa sau modifica toate datele trimise de la victimă la serverele *Web*. De asemenea, hackerul are controlul întregului trafic returnat de serverele *Web* către victimă. În consecință, hackerul dispune de multiple posibilități de exploatare. După cum am mai arătat, cele mai cunoscute metode de pătrundere într-o rețea sunt interceptarea şi simularea. Interceptarea (*sniffingul*) este o activitate de tip supraveghere, deoarece hackerul urmărește traficul de rețea în mod pasiv. Simularea este o activitate de intercepție, deoarece hackerul convinge un *host* că este un alt *host* credibil, care poate primi informații.

La simularea *Web*-ului, hackerul înregistrează conținutul paginilor vizitate de către victimă. Când victima completează un formular pe o pagină HTML, *browser*-ul său trimite datele introduse către serverul *Web*. Deoarece este interpus între client şi server, hackerul poate înregistra toate datele introduse de către client. De asemenea, hackerul poate înregistra şi conținutul răspunsului trimis de server către client. Deoarece majoritatea activităților comerciale *online* folosesc formulare, hackerul poate citi numere de cont, parole sau alte informații confidențiale introduse cu bună-ştiință de victimă în formularele simulate.

Hackerul poate efectua chiar şi activități de supraveghere, deşi victima dispune de o conexiune presupus sigură. Indiferent dacă această conexiune presupus sigură foloseşte sau nu *Secure Socket Layer* sau *Secure-http*, hackerul poate simula conexiunea. Cu alte cuvinte, chiar dacă *browser*-ul victimei indică pictograma de conexiune sigură (imaginea unui lacăt sau a unei chei), victima transmite folosind o conexiune desecurizată.

De asemenea, hackerul are posibilitatea de a modifica toate datele care se deplasează în orice direcție între victimă şi serverul *Web*. De exemplu, dacă victima comandă *online* 100 de lănțişoare de argint, hackerul poate modifica numărul produsului, cantitatea sau adresa de expediere, comandând 200 de lănțişoare de aur. Totodată, hackerul poate modifica datele returnate de serverul de *Web*. De exemplu, hackerul poate insera materiale derutante sau ofensatoare în documentele returnate de server pentru a determina inducerea unui antagonism între victimă şi server.

Cheia atacului prin simularea *Web*-ului este ca serverul hackerului să se afle între victimă şi restul *Web*-ului. După cum am mai arătat, acest aranjament este cunoscut sub numele de atac prin intermediar.

Prima etapă întreprinsă de hacker este rescrierea tuturor URL-urilor pe o anumită pagină *Web*, astfel ca URL-urile să indice spre serverul hackerului şi nu spre serverul real. Să presupunem că serverul hackerului se află pe domeniul „hacker.hck". Apoi, hackerul rescrie un URL prin adăugarea porțiunii „http://www.hacker.hck/" în fața etichetei URL. De exemplu, „http://www.jamsa.com" devine „http://www.hacker.hck / www.jamsa.com/".

Când utilizatorul ajunge la pagina *Web* rescrisă, URL-urile vor avea un aspect normal, deoarece hackerul va simula aceste URL-uri. Dacă se efectuează *click* pe hiperconexiunea „http://www.jamsa.com/" *browser*-ul va solicita pagina de la „www.hacker.hck", întrucât URL-ul începe acum cu „http://www.hacker.hck/". Restul

URL-ului indică serverului hacker unde anume se află în *Web* pagina solicitată de utilizator.

După ce serverul hackerului a preluat documentul veritabil necesar pentru satisfacerea cererii, hackerul rescrie URL-urile din document în forma specială folosită pentru simularea inițială. Cu alte cuvinte, hackerul inserează şirul „http://www.hacker.hck/" la începutul fiecărui URL din pagina solicitată. În final, serverul hackerului furnizează *browser*-ului pagina rescrisă.

Deoarece toate URL-urile din pagina rescrisă sunt acum orientate către serverul hackerului, dacă se urmează o conexiune din noua pagină, serverul hacker va prelua pagina din nou. Utilizatorul va rămâne prins în *Web*-ul fals al hackerului şi poate urma conexiunile la nesfârşit, fără a avea posibilitatea să-l părăsească.

După cum am mai arătat, dacă se completează un formular într-o pagină de *Web* falsă, în aparență *Web*-ul a tratat formularul în mod corect. Simularea formularelor se desfăşoară natural, deoarece protocoalele *Web* de bază au facilități extinse de integrare a formularelor. *Browser*-ul codifică transmisiile de formulare Internet în cereri HTTP, iar un server de *Web* răspunde la solicitările de formulare folosind HTTP obişnuit. Din acelaşi motive care stau la baza simulării oricărui URL, hackerii pot simula orice formular. Aşa cum cererile de pagini *Web* ajung la serverul hacker, tot acolo ajung şi datele trimise de victimă. Ca atare, hackerul poate modifica după cum doreşte aceste date înainte de a le transmite serverului veritabil. Serverul hacker mai poate modifica datele returnate ca răspuns la trimiterea formularului.

Unul dintre aspectele deosebit de supărătoare ale atacului prin simularea *Web*-ului este acela că atacul are efect chiar şi atunci când victima solicită o pagină cu o conexiune sigură. Dacă, de exemplu, se încearcă un acces la *Web* sigur (adică un acces la *Web* folosind S-HTTP sau SSL) într-un *Web* fals, pe ecranul *browser*-ului totul va avea un aspect normal. Serverul hacker va livra pagina şi *browser*-ul va activa indicatorul de conexiune sigură. *Browser*-ul va informa utilizatorul că există o conexiune sigură cu un server, deoarece *browser*-ul are o conexiune sigură. Din păcate, conexiunea sigură este cu serverul hacker şi nu cu pagina *Web* dorită, iar *browser*-ul şi utilizatorul presupun că totul este în regulă pentru că indicatorul de origine sigură oferă un fals sentiment de siguranță.

Este dificil de a scăpa dintr-un atac prin simularea *Web*-ului, acesta odată început. Cu toate acestea, lansarea unui astfel de atac necesită acțiune din partea victimei. Pentru a începe atacul, hackerul trebuie să atragă în vreun fel victima în *Web*-ul fals. Cu alte cuvinte, hackerul trebuie să determine victimele să efectueze *click* pe o hyperconexiune falsă. Un hacker poate face accesibilă o hyperconexiune falsă în mai multe moduri, astfel:

a) un hacker poate insera o hyperconexiune la *Web*-ul fals într-o pagină *Web* frecvent accesată;

b) dacă victima foloseşte email pentru *Web*, hackerul poate transmite victimei, prin email, un indicator către falsul *Web*;

c) hackerul poate transmite victimei (tot prin email) conținutul unei pagini din *Web*-ul fals;

d) hackerul poate determina un instrument de căutare *Web* să indexeze o parte dintr-un *Web* fals;

e) dacă victima foloseşte *Internet Explorer*, hackerul poate scrie un control *ActiveX* pe care *Explorer* îl va folosi de fiecare dată când victima rulează

browserul. Controlul *ActiveX* al hackerului poate înlocui un URL corect, normal, cu unul fals.

Problema importantă de reținut este aceea că hackerul trebuie să atragă într-un fel utilizatorul către falsul *Web*. Acesta va încerca să-şi atragă victimele folosind o varietate de metode. Astfel, deoarece atacul trebuie să convingă victimele că acestea se află în continuare în *Web*-ul real, atacul prin simularea *Web*-ului nu este perfect. Dacă hackerul nu este atent sau dacă utilizatorul a dezactivat anumite opțiuni din *browser*, paginile *Web* simulate vor afișa anumite informații în bara de stare. Aceste informații de pagină vor oferi suficiente indicii pentru a detecta intrarea în falsul *Web*. De exemplu, la indicarea cu mouse-ul a unei hiperconexiuni, majoritatea *browser*-elor vor afișa adresa absolută a hiperconexiunii în fereastra lor de stare. Din păcate, un hacker atent poate folosi anumite tehnici de programare pentru a elimina, practic, toate indiciile existenței unui atac. Acestea sunt relativ uşor de eliminat, datorită simplității de personalizare a *browser*-ului. Capacitatea unei pagini *Web* a de controla comportamentul *browser*-ului este de dorit, dar când pagina este ostilă acest lucru poate fi periculos pentru utilizator.

Deseori, mesajele din bara de stare descriu starea tranzacțiilor HTTP în curs de desfăşurare sau adresa indicată de o hyperconexiune. Totuși, autorul unei pagini poate modifica linia de stare pentru a afișa un text la alegerea sa.

Atacul prin simularea *Web*-ului lasă două categorii de urme pe bara de stare. Mai întâi, aşa cum am mai arătat, la menținerea indicatorului de mouse deasupra unei hiperconexiuni, bara de stare a *browser*-ului va afișa URL-ul inclus în hyperconexiune. Astfel, victima poate observa că hackerul a rescris URL-ul hiperconexiunii. În al doilea rând, atunci când *browser*-ul preia o pagină, bara de stare va afișa numele serverului contactat de *browser*. Astfel, victima va constata ca pe bara de stare este afişat numele de „www.hacker.hck” în loc de „www.jamsa.com”, aşa cum se aştepta.

Hackerul poate folosi un program *Java, JavaScript* sau *VBScript* pentru fiecare pagină rescrisă în scopul de a acoperi ambele indicii vizuale prezentate. Deoarece programul adăugat de hacker poate insera un conținut în bara de stare, hackerul poate aranja lucrurile de aşa manieră încât bara de stare să fie parte a iluziei. În plus, hackerul îşi poate aranja programul în funcție de evenimente, astfel încât pe bara de stare să fie afişate mesajele corespunzătoare *Web*-ului veritabil, chiar şi pentru conectarea la o nouă pagină. Controlul mesajelor afişate pe bara de stare determină un plus de credibilitate pentru conținutul simulat. Se afirmă chiar că, în lipsa unei bare de stare simulate, conținutul în sine al paginii nu este destul de convingător.

Bara de stare are potențialul de a compromite un *Web* fals, dacă hackerul nu ia măsuri pentru a se asigura că aceasta afişează informațiile dorite de el sau pe care le aşteaptă utilizatorul. De asemenea, bara de locație a *browser*-ului poate da în vileag atacul prin simularea *Web*-ului. Bara de locație a *browser*-ului afişează URL-ul paginii pe care victima o vizualizează în acel moment. Totodată, victima poate tasta un URL în bara de locație, cerând *browser*-ului să solicite resursa situată la acea adresă. Fără alte modificări, atacul prin simularea *Web*-ului va afișa URL-ul rescris. Independent de celelalte puncte slabe ale acestui tip de atac, majoritatea utilizatorilor vor sesiza URL-ul rescris din bara de locație a *browser*-ului. Dacă victima observă URL-ul rescris, va realiza, probabil, că se află în cursul unui atac. Din nou, hackerul poate ascunde URL-ul rescris folosind un program din serverul de simulare, care va ascunde bara de locație veritabilă şi o va înlocui cu una falsă care arată aparent identic. Bara de locație falsă

poate indica URL-ul pe care victima se aşteaptă să-l vadă. De asemenea, bara de locaţie falsă poate accepta intrări de la tastatură, permiţând victimei să introducă URL-uri în mod normal. Programul inclus poate să rescrie URL-urile tastate înainte ca *browser*-ul să solicite accesul.

Indiciul final la care victima poate avea acces sunt informaţiile despre document. Dacă victima selectează articolul de meniu *View Document Source*, hackerul poate înlocui informaţiile despre document folosind o bară de meniuri simulată. Dacă hackerul creează o bară de meniuri simulată, acesta poate afişa caseta de dialog cu informaţiile despre document folosind informaţii manipulate.

Pe scurt, hackerul poate anula toate posibilele indicii pe care victima le poate accesa pentru a determina o falsă conexiune *Web* prin limbaje de *Scripting*. Unica apărare a victimei atacate este de a dezactiva limbajele de *scripting* din *browser*.

Se afirmă că unica modalitate de prevenire a unui atac prin simularea *Web*-ului este localizarea şi pedepsirea hackerului. Datorită naturii atacului, serverul hackerului trebuie să-şi precizeze locaţia pentru a putea realiza atacul. Dacă victima detectează atacul, locaţia serverului va fi aproape sigur dezvăluită. Din păcate, hackerii care realizează atacuri prin simularea *Web*-ului vor acţiona în majoritatea cazurilor de pe computere furate. Sistemele furate reprezintă baza ideală pentru atacurile prin simularea *Web*-ului, din acelaşi motiv pentru care spărgătorii de bănci folosesc maşini furate pentru a dispărea[7].

1.2. Urmarea imediată şi legătura de cauzalitate

Urmarea imediată constă în obţinerea de date necorespunzătoare adevărului şi, prin aceasta, crearea unei stări de pericol pentru încrederea care se acordă datelor informatice şi, în general, prelucrării automate a acestora.

Legătura de cauzalitate între activitatea făptuitorului şi urmarea produsă trebuie dovedită.

2. Latura subiectivă

Infracţiunea de fals informatic se săvârşeşte numai cu intenţie directă, calificată prin scop.

În condiţiile inserării, modificării sau ştergerii de date informatice, va exista infracţiune chiar dacă persoana a alterat adevărul din cuprinsul acestor date cu un scop „legitim” (de exemplu, pentru a crea proba unei situaţii juridice reale). De asemenea, nu este necesară utilizarea efectivă a acestor date, ci numai obţinerea lor în vederea realizării scopului propus.

Scopul urmărit îl reprezintă utilizarea datelor necorespunzătoare obţinute în vederea producerii unei consecinţe juridice. Datele sunt susceptibile să producă

[7] Bineînţeles că prin acţiunea de săvârşire a infracţiunii de fals informatic se pot întruni şi elementele constitutive ale altor infracţiuni îndreptate împotriva datelor şi sistemelor informatice (spre exemplu, se poate folosi falsul informatic pentru a realiza o interceptare a datelor informatice ori se poate realiza falsul informatic ca urmare a accesului ilegal la un sistem informatic ori pentru săvârşirea unei fraude informatice etc.). Am analizat aceste modalităţi în cazul infracţiunii de fals informatic datorită specificului pe care îl prezintă, respectiv obţinerea de date necorespunzătoare adevărului şi aptitudinea de a produce consecinţe juridice.

consecințe juridice dacă sunt apte să dea naştere, să modifice sau să stingă raporturi juridice, creând drepturi şi obligații[8].

§4. Forme. Modalități. Sancțiuni şi aspecte procesuale

1. Forme

Actele pregătitoare, deşi posibile, nu sunt incriminate şi ca atare nu sunt pedepsite.

Tentativa se pedepseşte (conform art. 50 din lege).

Infracțiunea se consideră consumată atunci când făptuitorul a introdus, modificat ori şters în vreun fel acele date informatice dintr-un sistem ori a restricționat accesul la respectivele date dacă prin aceasta s-au produs alte date sau situații juridice necorespunzătoare valorii de adevăr inițiale.

2. Modalități

Infracțiunea analizată prezintă patru modalități normative, respectiv introducerea, modificarea, ştergerea de date informatice, precum şi restricționarea accesului la aceste date. Acestor modalități normative pot să le corespundă variate modalități de fapt.

3. Sancțiuni şi aspecte procesuale

Pedeapsa prevăzută este închisoarea de la 2 la 7 ani[9].

Acțiunea penală se pune în mişcare din oficiu.

---

[8] A se vedea în acest sens *V. Dongoroz, S. Kahane, I. Oancea, I. Fodor, N. Iliescu, C. Bulai, R. Stănoiu, V. Roşca*, Explicații teoretice ale codului penal român, vol. IV, Ed. Academiei Române, Bucureşti, 1972, p. 428, *V. Dobrinoiu şi colaboratorii*, op. cit., p. 618; *A. Boroi, G. Nistoreanu*, Drept penal, Partea specială, Ed. All Beck, Bucureşti, 2004, p. 723; *O. Loghin, A. Filipaş*, Drept penal român. Partea specială, Casa de Editură şi Presă „Şansa" S.R.L., Bucureşti, 1992, p. 269; *T. Toader*, Drept penal, Partea specială, Ed. All Beck, Bucureşti, 2002, p. 386.

[9] Aceeaşi pedeapsă este prevăzută şi de art. 445 din noul Cod penal.