licență de "exploatare, distribuire sau utilizare". Este vorba de venit brut perceput, mai puțin cheltuielile de cercetare, de reglare, de întreținere și de evoluția unui program;
- software-ul este original. Impozitarea redusă nu se aplică decît programului informatic protejat de regimul dreptului de autor.

Impozitarea redusă se aplică de mai multă vreme brevetelor. În plus, legiuitorul a optat în legea din 3 iulie 1985, pentru o protecție juridică a software-ului prin regimul dreptului de autor. Consecința: este contradictorie prevalarea dreptului de autor în materie de protecție și a brevetului în materie fiscală.
Problema statutului fiscal al autorilor de software a fost ridicată de J. Godfrain, inițiatorul legii din 1988 privind frauda informatică. Această lege a propus copierea statutului autorilor de software după cel al scriitorilor. Art. 21 din legea finanțelor pe 1990, extinde regimul plusvalorilor pe termen lung pentru produsele extrase din "cesiunile sau concesiunile de software-uri originale sau generice", de către persoane fizice pendinte de beneficii industriale și comerciale (BIC).
Ministrul Economiei, Finanțelor și Bugetului indică drept beneficiari ai acestei dispoziții întreprinderile supuse regimului BIC, dar și pe "creatorii independenți de software-uri, care plătesc impozit pe venitul din categoria beneficiilor necomerciale și care beneficiază de protecția legii din 3 iulie 1985".
Legea din 29 decembrie 1990 vizează în mod expres orice persoană fizică, autor care cedează drepturile asupra unui software original, pendinte de beneficii necomerciale.
Examinînd software-ul în ansamblul său și pornind de la toate elementele componente, care stabilesc marca personalității autorului acestuia, autoritățile apreciază de la caz la caz dacă programul informatic poate accede la rangul de "operă de spirit". Astfel, jurisprudența a admis originalitatea tuturor tipurilor de software, criteriul fiind "un efort personalizat care pornește de la punerea în aplicare a unei logici automate și restrictive" relevînd că "materializarea acestui efort rezidă într-o structură individualizată". Creația presupune o "alegere subiectivă între diverse moduri de prezentare și de expresie".
Administrația precizează că un program este orginal atunci cînd:
- este rezultatul unei "munci intelectuale și personale";
- este o "operă originală" în concepția și exprimarea sa, ceea ce exclude utilizarea software-urilor deja existente, provenite prin traducere într-o altă limbă sau prin adaptarea la alte echipamente sau finalități.

Pe de altă parte, deoarece directiva europeană*)privind protecția programelor definește originalitatea ca fiind mai degrabă un raport între creativitate și pricepere (după modelul brevetului), decît prin referire la amprenta personalității autorului.
Impozitarea redusă privește sumele obținute în urma cesiunii de drepturi asupra unui software original.
Contribuabilii care nu au beneficiat, pot solicita reducerea impozitului printr-o plîngere adresată serviciilor fiscale:
- pentru anul 1989, taxa de impozit era de 16 % dacă autorul nu a exercitat o adevărată activitate profesională și de 11 % în cazul unei activități profesionale, exercitată cu titlul principal, de obicei și constant;
- pentru anul 1990, contribuabilii au putut supune produsele de cesiune de software cu regim de plusvaloare pe termen lung.

(van Dorsselaere B. - "Allègement fiscal pour les auteurs independants";în : Le Monde Informatique, nr. 461, 16 iunie 1991, p.16).

Traducere
Victoria Haiduc
Institutul de Cercetări în Informatică

*) Directiva europeană sub protecția software-ului din 13.dec.1990

DELICVENȚA INFORMATICĂ VIRUSII INFORMATICII

Autorul unui virus devine responsabil, atît pe plan civil cît și la nivel penal, începînd cu 1988.
Termenul de virus desemnează programele care conțin o funcție de autoreproducere, capabile să contamineze anumite elemente deja existente în memoria calculatorului. Ciclul de viață al unui virus se descompune în trei faze:
- execuția sa prin intermediul unui element contaminat;
- propagarea acestuia prin contaminarea de noi elemente;
- declanșarea acțiunii sale, care antrenează după sine pagube, de la simpla perturbare în funcționare la distrugerea conținutului unui disc fix.

În iunie 1991, 504 tipuri de viruși MS-DOS au fost recenzați la nivel mondial, dintre aceștia 35 fiind prezenți în Franța.
Victimele virușilor au două posibilități de a face recurs: acțiune în responsabilitate civilă și aplicarea legislației penale.
În ceea ce privește responsabilitatea civilă, Codul civil precizează că "orice faptă a unei persoane care cauzează

alteia o pagubă, obligă pe cea dintîi să aducă reparaţii victimei".
În practică, pentru a angaja responsabilitatea civilă a unui autor de virus informatic, victima va trebui să cheme în faţa justiţiei civile pe autorul sau autorii identificaţi ai virusului şi să deschidă proces conform procedurii, celor care au participat la actul păgubitor.
Dacă victima optează pentru acţiunea penală, aceasta va depune o plîngere, constituindu-se în parte civilă în faţa judecătorului de instrucţie, împotriva persoanei nominalizate. Procedura simplificată de citaţia directă în faţa tribunalului corecţional, destinată contravenţiilor sau delictelor pentru care instrucţiunea este facultativă, nu va fi modificată, autorul infracţiunii fiind cel mai adesea necunoscut.
Această plîngere va avea drept efect sesizarea jurisdicţiei respective prin reclamaţia victimei, de a lua act de cererea sa cu titlu de daune şi interese şi de a începe acţionare publică, dacă ministerul public nu a intentat-o deja. Operaţiunile de instruire vor putea demara după ce victima a achitat la grefier o sumă anumită, considerată drept cheltuieli de procedură.
A difuza un virus se încadrează la cele mai de sus în măsura în care acesta constituie într-adevăr o creaţie intelectuală a omului, destinată să provoace un prejudiciu. De asemenea, mai este necesar ca victima să identifice pe autorul virusului, să facă dovada actului păgubitor şi a legăturii de cauzalitate între aceste două elemente.

Identificarea autorului virusului

În cazurile în care autorul nu va fi identificat sau virusul va fi identificat chiar înainte ca acesta să fi putut acţiona, nu va exista responsabilitate civilă, deoarece nu există pagube.
Cea de a doua cale de recurs este Codul penal. Legea din 5 ianuarie 1988 privind frauda informatică, sancţionează toate prejudiciile directe sau indirecte aduse unui sistem de prelucrare automată a datelor, ceea ce ar putea fi mai eficace decît acţiunea în responsabilitate civilă, în multe cazuri.
Punerea în aplicare a responsabilităţii penale a autorului virusului prezintă două avantaje:

- instrucţiunea procură facilităţi de dovadă, victima profitînd de mijloacele de care dispun judecătorii pentru a lămuri o afacere (mărturisiri, posibilităţi de perchiziţii şi de sechestrare...);
- responsabilitatea penală va putea fi angajată chiar dacă nu există nici o pagubă, tentativa fiind pasibilă de aceleaşi pedepse ca în cazul unui delict în domeniul fraudei informatice, deci responsabilitatea civilă se ia în considerare numai în cazul unui prejudiciu raportat.

Dimpotrivă, acţiunea represivă prezintă două riscuri pentru victimă:

- de a se vedea reclamată din partea inculpatului, în cazul în care acesta nu se face vinovat de acţiune frauduloasă;
- de a nu putea fi audiată în cadrul instruirii şi dezbaterilor, fiind parte în cadrul procedurii. Aceasta s-ar afla într-o situaţie neplăcută, în cazul în care victima este singurul martor.

Oricare ar fi prejudiciul cauzat, sancţiunile cele mai grele reprimă atît simpla tentativă de injectare cu virus, cît şi numai participarea la o contaminare.
Victima va putea depune o plîngere, virusul căzînd în mod direct sub incidenţa legii privind frauda informatică, oricare ar fi paguba cauzată.
Textul represiv defineşte în sens larg sistemele informatice. Acesta protejează atît software-urile, cît şi datele şi relaţiile, în scopul de a lua în considerare reţelele, într-un cuvînt tot ceea ce poate fi distrus de un virus.
Pasibile de pedeapsă sînt:

- accesul şi menţinerea frauduloasă în funcţiune a sistemului sau a unei părţi a acestuia;
- obstrucţionarea premeditată a funcţionării unui sistem;
- prejudiciu adus datelor, ca şi legăturilor.

Virusul care se caracterizează prin modul său de reproducere, ca şi prin efectul său distructiv, este în mod direct vizat.Acesta nu se mulţumeşte numai să înregistreze căile de acces, ci prejudiciază utilizarea programelor de aplicaţie, sistemul de afişare a datelor şi, mai grav, ajunge să distrugă blocuri întregi de date, de programe, de module de sisteme, afectînd chiar sectorul de iniţializare de date. De asemenea, se pot cumula diverse tipuri de atacuri.
Legea împarte sancţiunile în funcţie de gravitatea prejudiciului cauzat şi de caracterul voluntar sau involuntar al actului. Dacă accesul sau menţinerea frauduloasă constituie fraude simple şi dacă pagubele care decurg demonstrează o fraudă agravată, difuzarea unui virus informatic va da loc la pedepsele cele mai grele, deoarece paguba depăşeşte simplul acces sau menţinerea într-un sistem, fiind cauzată în mod voluntar. Această fraudă "supra-agravată" se aplică în cazul prejudiciului voluntar, cauzat sistemului informatic şi se pedepseşte cu închisoare de la 3 luni la 3 ani şi cu amendă de la 10.000 F la 100.000 F. Amenda poate fi de la 2000 F la 500.000 F în cazul modificării modului de transmisie sau de prelucrare şi de prejudiciu adus unei date, fie că este vorba de suprimare, introducere sau modificare a acesteia. Se are, de asemenea, în vedere repararea prejudiciului adus victimei, potenţial considerabil.
Pentru o mai bună eficacitate, legea adaugă cîteva măsuri preventive. Aceste pedepse se aplică şi la delictul de înfăptuire completă a fraudei, ca şi la simpla tentativă de a contamina un sistem cu viruşi, fără însă să se ajungă la aceasta, sau de a injecta un virus care nu şi-a făcut însă efectul, deoarece a fost detectat la timp; sînt acţiuni suficiente pentru a fi considerate delicte, chiar dacă nu a apărut nici un prejudiciu.

Sancţiuni pentru toţi cei implicaţi

Sancţiunile se aplică atît celor care au comis delictul, cît şi celor care au participat la înţelegerea stabilită în vederea realizării fraudei. Căderea de comun acord este reprimată cu aceeaşi pedeapsă ca delictul principal. De asemenea, cel care a ajutat numai la pătrunderea virusului la victimă va fi greu sancţionat. Acelaşi lucru se întîmplă cu cel care a ajutat la difuzarea unui virus, de exemplu prin distribuirea unei publicaţii: va fi pus sub urmărire pentru participarea la înţelegere sau pentru complicitate.

Utilizarea unui software-virus fiind în orice caz ilicită, responsabilitatea sa poate fi angajată, cu titlul de complicitate la atingerea unui sistem automat de prelucrare de date, cu condiţia să se facă dovada că agresorul, în mod conştient a furnizat utilizatorilor un program distructiv, elementul intenţional fiind greu de dovedit şi cel mai adesea neconstituit.

În materie de viruşi informatici, nu se acceptă invocarea unei legitime apărări, programul nefiind o apărare proporţionată unui atac injust. Pe de altă parte, obiectivul nu este defensiv, deoarece virusul urmează să producă perturbaţii în funcţionarea aplicaţiilor, fără însă a fi fost declanşate de comportamentul utilizatorului.

Pe de altă parte, agresiunea se dovedeşte disproporţională, deci imposibil de stăpînit. Prejudiciul nu se limitează la un program, dar va atinge multiple aplicaţii; reproducîndu-se în lanţ în alte programe, va atinge sistemul de exploatare şi va putea chiar să declanşeze procese care pot defecta discul fix.

Legea protejează chiar şi sistemele neasigurate

Asigurate sau nu, legea protejează toate sistemele de "prelucrare automată a datelor". Astfel, actele de sabotaj, prin injectarea de virus sau prin alt mijloc, aduse sistemelor neprotejate, devin pasibile de sancţiuni penale. Chiar dacă nu există metode eficace 100%, se impun anumite precauţii indispensabile împotriva virusilor, ca de exemplu: salvarea regulată a datelor, conservarea mai multor seturi de salvare, controlarea software-ului care provine din afară, formatarea dischetelor înainte de utilizare, verificarea dimensiunilor fişierului etc.

Din păcate textul legii din 5 ianuarie 1988 nu incită şi la alocarea de investiţii pentru dezvoltarea unei politici în domeniul securităţii în informatică. Legea nu impune instalarea de mijloace tehnice necesare prevenirii fraudei, dar dreptul penal trebuie să compenseze slăbiciunea mijloacelor de securitate. În practică, existenţa sau absenţa dispozitivului de securitate va fi luată în consideraţie de către instanţa de judecată, deoarece spiritul legii autorizează punerea în legătură a realizării delictului informatic de existenţa unei protecţii suficiente a sistemului.

(van Dorsselaere, B. - "Quel recours face aux virus informatiques?"; în: Le monde informatique, nr. 464, 8 iulie 1991, p.12)

Traducere
Victoria Haiduc
Institutul de Cercetări în Informatică