Марио Милушев

КОМПЮТЪРНО ПРАВО

Марио Милушев

Компютърно право

За контакти:
+ 359888290442
E-mail: mmilushev@abv.bg

СЪДЪРЖАНИЕ

СЪКРАЩЕНИЯ

ГПК – Гражданскопроцесуален кодекс
ДПК – Данъчнопроцесуален кодекс
ЗАНН – Закон за административните нарушения и наказания
ЗАП – Закон за административното правоизводство
ЗАПСП – Закон за авторското право и сродните му права
ЗЗД – Закон за задълженията и договорите
ЗЗК – Закон за защита на конкуренцията
ЗЗППТ – Закон за защита на потребителите и за правилата за търговия
ЗМГО – Закон за марките и географските обозначения
ЗН – Закон за наследството
ЗЗК – Закон за защита на конкуренцията
ЗОДФЛ – Закон за облагане доходите на физическите лица
ЗП – Закон за патентите
ЗПД – Закон за промишления дизайн
ЗС – Закон за собствеността
ЗТИС – Закон за топологията на интегралните схеми
ЗТМПО – Закон за търговските марки и промишлените образци
К – Конституция на РБ
КТ – Кодекс на труда
НК – Наказателен кодекс
НПК – Наказателнопроцесуален кодекс
РБ – Република България
ТЗ – Търговски закон

ЗА КНИГАТА

"КОМПЮТЪРНО ПРАВО" систематизира материята, застъпена в законодателството на България, като са отразени най-новите изменения и допълнения в нормативната уредба. Проследено е развитието на компютърното право и в международен аспект.

Книгата е полезно четиво за студентите от юридическите факултети, но може да служи като справочник и за практикуващите правници – съдии, арбитри, съдия-изпълнители, нотариуси, юрисконсулти и адвокати.

От нея могат да се ползват също специалисти с инженерно-технически профил – конструктори, програмисти, информатици, студенти от техническите специалности, лица по поддръжката, експлоатацията и разпространението на електронно-изчислителна техника, както и всички други, които имат професионално отношение към проблема.

Книгата е предназнатена и за онези потребители, които проявяват интерес към правното регулиране на обществените отношения, свързани със създаването и използването на компютърната техника и технологии.

КОМПЬЮТЕРНОЕ ПРАВО

Один из основных юридических принципов заключается в так называемом опережающем действии в отношении интервенций, касающихся регуляции общественных взаимоотношений. Именно поэтому право обязано дать ответ на провокации, которые хлынули на нас с передового фронта современной науки.

Быстрое развитие научно-технического прогресса, и возможные последствия, как с положительным, так и с негативным знаком, обязывают законодательства повернуться лицом к проблеме. В **Декларации об использовании научно-технического прогресса во имя мира и добра человечества** указано, что научно-технический прогресс стал одним из важнейших факторов в развитии человечества. Он может стать решающим фактором для улучшения условий жизни народов и наций, но также может вызвать и серьезные социальные проблемы, стать угрозой правам человека и основным принципам свободы индивида. Все это вызывает потребность в оповещении основных проложений, которые послужили бы базой для каждого отдельного государства и международных организаций, создающих акты регулирования ново созданных взаимоотношений.

В настоящей и последующих работах будут рассматриваться основные положения, являющиеся закономерным результатом взаимоотношений между правом и новыми, так называемыми *hi-tech* (высокими) технологиями. Имея ввиду разнообразие материи, предусмотрено ее систематизирование в соответствии с обособленными юридическими направлениями: компьютерное право, космическое право, биомолекулярное право, нанотехнологическое право, право кибер-пространства. Каждое из них подробно будет рассматриваться в отдельной книге. Настоящая, первая книга названа **компьютерное право**.

COMPUTER LAW

One of the basic principles of law is the so-called "effect of anticipation" referring to social relations. This necessitates that the law reacts to the challenges coming from the avant-garde of modern science.

The fast development of technological process and its possible effects, which might be either positive or negative, compels the legislations to face these problems. The **Declaration for the utilization of the technological and scientific progress in the name of peace and human welfare** states that the scientific and technological progress has become one of the major factors of development for the human society. It might become a crucial factor to improve the living conditions of peoples and nations, but at the same time it might trigger serious social problems, to jeopardize human rights and man's basic freedoms. This necessitates the declaration of basic principles, which would serve as a ground for the individual governments and international institutions to draft documents regulating the newly established relations.

This work, and the following ones will discuss the major cases, arising as natural result from the relations between the law and the new high technologies. Because of the diversity of this subject matter, it will be systematized according to the differentiated branches of law: computer law, space law, biomolecular law, nanotechnological law, cyberspace law. Each of these branches will be discussed in detail in a separate book. This first book is titled **computer law**.

ПРЕДГОВОР

В процеса на интеграция на страната към европейските социално-икономически и политически структури се очертават проблеми, които изискват да се подходи към тях с необходимата юридическа задълбоченост. Един от наболелите въпроси е свързан с регулирането на най-бързоразвиващата се област от културата – научно-техническата. Нито една регионална икономика не би могла да бъде конкурентноспособна, ако не съумее да отговори на изискванията на технологичното трето хилядолетие.

Настоящото изследване обхваща определени теми от правното регулиране на обществените отношения в областта на научно-техническия прогрес, по-специално компютърните технологии и свързаните с тях обекти на правото – компютри и компютърни системи. Поради новостта на материята материалът няма претенции за изчерпателност и пълнота; идеята е да се поднесат в сравнително систематизиран вид основните положения от теорията и практиката, за да може да се получи, макар и бегла, представа за характера и особеностите на тази специфична правна област.

Следва да се има предвид, че **компютърното право не е нова правна наука**, както смятат някои юристи. Компютърното право твърдо следва постановките на класическата правна доктрина. То обаче цели да улесни нуждаещите се от информация относно правния режим на компютърните технологии, т.е. има преди всичко **практическа насоченост**. Онова, което го отличава от вече установените правни клонове е **новата систематика**, както и фактът, че изследванията се концентрират върху един единствен **обект** – **компютъра**. Не е така при някои нови правни науки, които си поставят за цел да положат различна концептуална основа на правните категории – например т.нар. информационна интерпретация на правото. |[1]| Там се залага не на философско-социологическия подход, а

[1]|| Вж. ИНФОРМАЦИОННА ИНТЕРПРЕТАЦИЯ НА ПРАВНИТЕ КАТЕГОРИИ, Кантарджиев А.

най-вече на логико-математическите прийоми и методи, намиращи приложение в точните науки. За възприемането на такива "ултрамодерни" възгледи обаче съвременната правна теория и особено практика днес са съвсем неподготвени.

Що се отнася до термина **компютърно право**, той се появява най-напред в англоговорящите страни – *computer law*. Буквално преведено, словосъчетанието е граматически непрецизно и може да бъде изтълкувано като "право на компютрите" или "право на компютърната техника". Компютрите обаче не са субекти на правото и в този смисъл не могат да имат права и задължения. Правно и логически по-издържано е: "направление в правото, обект на което са компютрите и компютърните системи". Причината, поради която този израз не е удобен за ползване, е неговата принадлежност по-скоро към определенията, отколкото към стегнатите научни термини; многословието прави употребата трудна. Затова, независимо от граматическата си непрецизност, терминът компютърно право е може би най-приемлив за ползване. (Практиката е наложила употребата и на други подобни изрази - космическо право, морско право, атомно право и т.н.) Но с уговорката в "компютърно право" да се влага смисъла на **определението** за компютърно право.

Изложението следва линията на систематизирано представяне на проблемите около компютърните системи като особени обекти на правото, както и способите за регулиране правата върху тях. В началото вниманието е съсредоточено върху правната закрила в областта на интелектуалната собственост, към която се причисляват всички правоотношения в областта на **създаването** на компютърния хардуер и софтуер. По-нататък логично следват правоотношенията, относими към **употребата** на вече създадените компютърни продукти. Накрая е обърнато внимание на екцесиите, които се наблюдават при неправномерни действия, и реактивните по своя характер правни способи за **защита**.

Ползван е богатият чуждестранен опит - предимно нормативни разпоредби от законодателствата на по-напредналите в технологично отношение страни.

По отношение на вътрешната структура на книгата авторът се е съобразил с някои специализирани чужди издания, но поради едностранчивостта на предлаганата в тях материя се е приддържал най-вече към собственото си разбиране. |[2]|

---

[2]|| Пример може да бъде даден с INTRODUCTION TO COMPUTER LAW, 4th Edition, David Bainbridge, 2000. Съдържанието на тази книга включва следните

теми:

Introduction
PART 1: COMPUTERS AND INTELLECTUAL PROPERTY
2. Overview of intellectual property rights
3. Copyright basics
4. Computer software and copyright
5. Copyright and databases
6. Computer-generated works
7. Copyright and electronic publishing
8. The law of confidence
9. Patent law
10. Trade marks and passing off
11. Designs
12. Semiconductor products
13. International implications and summary
PART 2:COMPUTER CONTRACTS
14. Introduction to computer contracts
15. Fundamentals of computer contracts
16. Liability for defective hardware of software
17. Contracts for writing software
18. Licence agreements for 'off-the-shelf' software
19. Contract between software author and publisher
20. Hardware contracts
21. Electronic contracting
22. Summary and checklist
PART 3:COMPUTERS AND CRIME
23. Nature of computer crime
24. Computer fraud
25. Hacking - unauthorised access to computer material
26. Unauthorised modification of computer programs or data
27. Piracy offences
28. Computer evidence and criminal proceedings
29. Computer crime - concluding remarks
PART 4: DATA PROTECTION
30. Main provisions of the Data Protection Act 1984

УВОД

"Чл. 54 (1) Всеки има право да се ползва от националните и общочовешките културни ценности, както и да развива своята култура в съответствие с етническата си принадлежност, което се признава и гарантира от закона.

(2) Свободата на художественото, научното и техническото творчество се признава и гарантира от закона.

(3) Изобретателските, авторските и сродните на тях права се закрилят от закона."

КОНСТИТУЦИЯ НА РБ

Един от основните правни принципи се изразява в т.нар. **изпреварващо действие** на законовите норми спрямо развитието на обществените отношения. |[3]| Той изисква от правото - като регулираща система, да отговаря адекватно на провокациите, които нахлуват от предния фронт на съвременната наука. |[4]|

Информационните технологии във все по-голяма степен влияят върху формирането на обществото на двадесет и първия век. Те оказват революционно въздействие върху живота на хората, тяхното образование и работа, а също върху взаимодействието между правителствата и гражданското общество. Информационните технологии бързо се превръщат в жизненоважен стимул за развитието на световната икономика. Те дават възможност на частните лица, фирмите и организациите, занимаващи се с предприемаческа дейност,

31. Exemptions form and enforcement of the Data Protections Directive
32. The Data Protection Directive
33. Summary of data protection law

[3]|| ИНФОРМАЦИЯ И ПРАВО, А. Кантарджиев,1992.

[4]|| ОТКРИТИЕТО НА ВЕКА И НЕГОВОТО ОТРАЖЕНИЕ В ПОЗИТИВНОТО ПРАВО, сп. ИЗВЕСТИЯ, кн. 2'99, 1'2000, М. Милушев, 76.

по-ефективно и творчески да решават икономическите и социалните проблеми. |[5]|

Освен това нарастващото оползотворяване на науката и технологиите за социално и икономическо развитие, уреждането трансфера и обмена на технологии изисква международно културно сътрудничество, което да покрива всички аспекти от интелектуалните и творческите дейности, отнасящи се до образование, наука и култура, както и формулирането на съответстваща национална и международна политика. |[6]|

Бързото развитие на научно-техническия прогрес принуждава законодателствата да обърнат лице към проблемите, които новите технологии създават. В **Декларацията за използването на научно-техническия прогрес в името на мира и за доброто на човечеството** се отбелязва, че научно-техническият прогрес е станал един от най-важните фактори в развитието на човешкото общество. "Той може да се окаже от решаваща роля за подобряване на условията на живот на народите и нациите, но също така и да породи сериозни социални проблеми, да заплаши човешките права и основни свободи на индивида." Затова се налага да се известят основни принципи, които да послужат за база на отделните държави и на международните институции, които създават актове за регулиране на новосъздадените отношения. |[7]|

С лице към проблемите застават както държавите-членки на Европейския съюз, така и другите държави с предстоящо членство. Като осъзнават дълбоките изменения, предизвикани от въвеждането на цифровите технологии, от конвергенцията и от постоянната глобализация на компютърните мрежи, и загрижени от опасността от използване на електронната информация за извършването на престъпления, те преценяват, че трябва да се даде приоритет на политика, насочена към приемане на съответно законодателство и към укрепване на международното сътрудничество. |[8]|

---

[5]|| ДЕКЛАРАЦИЯ ЗА СОЦИАЛНИЯ ПРОГРЕС И РАЗВИТИЕ, провъзгласена с резолюция 2542 (XXIV) на Общото събрание от 11.12.1969 г.

[6]|| ДЕКЛАРАЦИЯ ЗА ИЗПОЛЗВАНЕТО НА НАУЧНО-ТЕХНИЧЕСКИЯ ПРОГРЕС В ИМЕТО НА МИРА И ЗА ДОБРОТО НА ЧОВЕЧЕСТВОТО, Провъзгласена с резолюция 3384 (XXX) на Общото събрание на ООН на 10.11.1975г.

[7]|| Пак там.

[8]|| CONVENTION ON CYBER-CRIME (№ 19), April 27, 2000, Strasbourg.

“Нашата задача се заключава не толкова в стимулиране и съдействие за прехода към информационното общество, но също и за пълната реализация на неговите икономически, социални и културни преимущества. За достигането на тези цели трябва да се работи в няколко основни направления, едно от които е закрилата на правата в областта на интелектуалната собственост по отношение на информационните технологии.” |[9]|

Компютърните системи и производните им играят важна роля в широкия спектър от индустриални приложения, а компютърно-програмната технология има фундаментално значение за индустриалното развитие на новосформиращия се Европейски съюз. |[10]| Принципно новите обществени отношения изискват и особена правова закрила, доколкото те не се вписват в нито един от известните институти на правото. |[11]|

[9]|| Пак там.

[10]|| COUNCIL DIRECTIVE ON THE LEGAL PROTECTION OF COMPUTER PROGRAMS, (91/250/EEC) 14/05/1991.

[11]|| ПРАВОВАЯ ОХРАНА ТЕХНОЛОГИЙ, В.В. Степанов, 15 ноября 2001г.

ИЗЛОЖЕНИЕ

Част първа
ТЕРМИНОЛОГИЯ

В компютърното право освен традиционните правни понятия органически се вплитат и понятия от компютърната наука, техника и технология. Това налага на тези понятия да се придаде освен чисто технически, инженерен смисъл, още и правнорелевантно значение. Засега неголяма част от тях имат правни еквиваленти и при разглеждане на съдебни казуси правораздавателните органи често прибягват до съдействието на специалисти (експерти). Тук ще бъдат разгледани някои основни понятия, които имат отношение към разглежданата материя.

Дял първи
КОМПЮТЪРНА НАУКА. ТЕХНИКА. ТЕХНОЛОГИЯ

"Според някои компютърната наука е изкуство, подобно на литературното, други я отнасят към техническите науки, обаче и в двата случая компютърната наука има за предмет създаването и употребатата на работещо на цифров принцип изчислително устройство." |[12]|

Компютърна наука.

1. Днешният бум в развитието на така нареченото информационно общество често бива окачествяван като "**втора индустриална революция**". Докато първата индустриална революция през 19-ти и 20-ти век се отнася до заместването на **живата сила от машините**, втората фаза на индустриалното развитие прехъвърля **човешката интелектуална активност към машините**. Това сравнение илюстрира, че икономическите и социални ефекти от новото развитие далеч превъзхождат промените, причинени от първата индустриална революция. |[13]|

2. Като се имат предвид горните съображения, може да се започне с анализ на основните понятия в науката за обработка на информацията. Компютърната наука |[14]| – **информатиката,** е **наука за**

---

[12]|| PATENTING COMPUTER SCIENCE: ARE COMPUTER INSTRUCTION WRITINGS PATENTABLE? ALLEN B. WAGNER, 17 J. MARSHALl j. COMPUTER & INFO. L. 5 (1998).

[13]|| LEGAL ASPECTS OFCOMPUTER-RELATED CRIME IN THE INFORMATION SOCIETY, prepared for the European Commission by prof. Dr. Ulrich Sieber, 1998.

[14]|| COMPUTER SCIENCE. The study of the use, design and CONSTRUCTions of (largely digital) computers. Computer science heavily relies on mathematical (see mathematics) and engineering insights. In spite of its mathematically sophisticated, academically demanding, and economically profitable appearance, its body of generally acceptable fundamental laws or principles, is small. A more appropriate name for this "state of the art" - like body of knowledge would be computer technology.
WEB DICTIONARY OF CYBERNETICS AND SYSTEMS.

автоматично обработване на информация. |[15]| (Терминът е заимстван от френския език. В английския език се използва *computer sciense* - компютърна наука.)

3. Ученият в областта на природните науки изучава физични процеси, той се занимава с конкретни, обективни проблеми. За разлика от него ученият в областта на информатиката създава абстрактни логически модели за решаване на практически проблеми под формата на алгоритми. Логическият модел сам по себе си е "символна алегория", отделна от физичния процес на автоматично изпълняваните инструкции. В този смисъл особеностите, отличаващи компютърната от природната наука, са следните:

- процесът на изчисляване е абстрактен принцип, който не се среща в природата;
- процесът на изчисляване е независим от физичната форма или употребявания механизъм; и
- принципите на природната наука обикновено са няколко и са неизменяеми, докато компютърната наука е поставена в зависимост от един непостоянен принцип – гъвкавия алгоритъм на инструкцията. |[16]|

Техника.

4. В българската нормативна уредба не съществува легална дефиниция за техника. От други източници се черпи информацията, че **техниката опосредява въздействието на човека спрямо природата.** |[17]| В този смисъл тя обхваща средствата и методите на това опосредяване, които от своя страна представляват веществените оръдия на труда, начините на тяхното използване (технологии), и обекта на въздействието им (суровини, продукти на труда и т.н.) Според трети източници техниката се състои в използване на овладени от човека природни сили. Или по-общото - техниката обхваща

---

[15]|| ТЪЛКОВЕН РЕЧНИК НА БЪЛГАРСКИЯ ЕЗИК, БАН, София, 1990г.

[16]|| PATENTING COMPUTER SCIENCE: ARE COMPUTER INSTRUCTION WRITINGS PATENTABLE? ALLEN B. WAGNER, 17 J. MARSHALl j. COMPUTER & INFO. L. 5 (1998).

[17]|| ГРАЖДАНСКОПРАВЕН РЕЖИМ НА ПРОГРАМИТЕ ЗА ЕЛЕКТРОННО-ИЗЧИСЛИТЕЛНИ МАШИНИ, И. Ескенази, 1980. Трудът на И. Ескенази е едно от първите систематизирани изследвания в България в областта на закрилата на правата върху компютърните продукти. Изтъкнати са белезите на компютърните програми и софтуера като обекти на правото, разгледани са основните проблематики, които навремето са съпътствали създаването на подходящ правен режим. От него може да се проследи как еволюира правното съзнание в тази област. Някои от постановките, заложени в този труд, са актуални и днес, бел. а.

използването на овладяеми природни сили с цел постигане на каузално предвидим резултат. |[18]|

Технология.

5. Научнотехническата дейност е дейност, насочена към получаване и ползване на нови **знания** за решаване на технологични, инженерни, икономически, социални, хуманитарни и други проблеми, за обезпечаване функционирането на науката, техниката и производството като единна система. **Знанията** от своя страна **са съвкупност от сведения, намаляващи степента на неопределеност и служещи за решаването на конкретна задача**. |[19]|

6. В конкретен смисъл знанията са необходими за производството на компютърни устройства, за експлоатацията или поддържането им. В този смисъл това могат да бъдат знания, които се използват за производството на едно изделие, напр. дисплей на преносим компютър, или за производството на течнокристалната матрица като елемент от дисплея, или за производство на машина, напр. за крепежни елементи, които са необходими за закрепване на дисплея към корпуса на преносимия компютър. Това може да бъде още знание, от полза при експлоатацията или поддържането на компютъра. Това може да бъде знание от полза при опаковане на вече готовия компютърен продукт. Това може да бъде знание за предимствата на компютърния продукт и да допринесе за неговата продажба.

7. Следователно технологията се състои от знание. Но не всяко знание, не знанието като съвкупност от факти се има предвид. Знанието трябва да е системно (подредено в определен ред), за да може да се предава, прилага, да се решава чрез него проблем или да се задоволи потребност, възникнала при определен вид човешка дейност. В този смисъл дефиницията за "знание" съдържа три критерия:

- първо - знанието трябва да бъде системно. Под системно се разбира организирано с оглед предоставяне решението на даден проблем;
- второ - знанието трябва да съществува в писмен вид или в ума на някого, трябва да е разкрито или да дава възможност да бъде разкрито и така да се предава или да дава възможност да бъде предавано по някакъв начин;

---

[18]|| Пак там.

[19]|| ПРАВОВАЯ ОХРАНА ТЕХНОЛОГИЙ, В.В. Степанов.

- трето - знанието трябва да бъде насочено към получаване на определен резултат, да служи на полезна цел. |[20]|

8. В заключение: **технологията следва да се разбира като употреба на природни закони и принципи на науката с цел извършване на полезна дейност.** В този смисъл компютърните програми например са технология – технология за ползването на компютри при извършването на полезни дейности. |[21]|

9. В частен план **информационната технология** се дефинира като **технология, посредством използването на която информацията може да се обработва по електронен път.** |[22]|

Дял втори
КОМПЮТЪР. КОМПЮТЪРНА СИСТЕМА

Глава I
ОБЩИ ПОЛОЖЕНИЯ

10. За да бъде реализиран процес на обработка на информация по автоматичен (електронен) път, е необходимо да се организира така една изкуствена среда, щото тя да може да извършва необходимите за тази цел функции. В резултат от продължителни теоретически и практически усилия такава среда е създадена и е приела вида на устройства, наричани понастоящем **компютри (*computers*)**. |[23]|

---

[20]|| Пак там.

[21]|| THE RELATIVE ROLES OF PATENT AND COPYRIGHT IN THE PROTECTION OF COMPUTER PROGRAMS, DENNIS S. KARJALA, 17 J. MARSHALL J. COMPUTER & INFO. L. 41 (1998).

[22]|| THE COMPUTER SCIENCE DEVELOPMENT LAW, The State Law and Order Restoration Council Law No. 10/96, The 8th Waxing of Tawthalin, 1358 M.E. (20th September, 1996), CHAPTER 1, Title and Definition.

[23]|| През 1947г. двама учени - Екарт и Моучли, патентовали цифрово изчислително устройство, наречено *ENIAC* (*Electronic Numerical Integrator And Computer*). Този момент заема особено място в историческите анали на компютърното право по следните съображения.

11. В световен план не съществува еднозначно определение на понятието компютър. Най-общо казано "компютър" - "*computer"* |[24]| е производно на "*computing"*, |[25]| което означава изчисление, пресмятане. |[26]| Компютърът е устройство - техническо съоръжение, механизъм. Той е специализирана машина, предназначена да извършва изчисления, употребявайки енергия. Компютърът освен това е машина, работеща на електронен принцип, той е електронна машина. "Електронна технология" от своя страна означава електрическа, цифрова, магнитна, оптична, електромагнитна, или друга подобна технология. |[27]|

12. В отделните законодателства се употребяват дефиниции за "компютър", които се различават една от друга, макар и несъществено. Някъде под "компютър" разбират електронно устройство, което извършва логични, аритметични или запаметяващи операции въз основа на команди, подавани чрез електрични или магнитни импулси и

Патентът за създадената машина бил продаден на фирмата "Спери Ранд". Последната започнала да събира такси от изобретението. Един от клиентите й, корпорацията "Хонуел" обаче не желаела да заплати дължимата сума, защото й било известно, че изобретението всъщност е доработка на идея на Джон Атанасов. Завързал се спор, който довел страните до съдебната зала. Условно би могло да се приеме, че компютърното право води началото си от този именно период - съдебния процес, в който се решил спора за първия изобретен компютър. През 1972г. в дело, събрано в 20 000 страници и изслушване на 77 свидетели съдията отсъдил, че патентът за *ENIAC* е невалиден. В решението на съда се казвало, че Моучли и Екарт не са изобретили самостоятелно първия автоматичен електронен цифров компютър, а са доработили идеята на д-р Джон Атанасов.

Доказало се, че Атанасов пръв използвал четири ключови принципа за своя електронен цифров компютър: първо - електричество и електроника като работна среда; второ - двоичен код; трето - кондензатори за памет и механизъм за опресняване на систоянието им, и четвърто - логически операции, а не математически, които се използвали в тогавашните аналогови изчислителни устройства.

Разбирането - "електронно-изчислителна машина", има решаващо значение за утвърждаване на днешното понятие за компютър. В по-далечното минало също се конструирали и изработвали повече или по-малко сложни машини за извършване на изчисления. Всички те обаче функционирали на механичен принцип - например диференчната машина на *Барбидж,* и поради тази причина не са компютри в съвременния смисъл на думата. Едва с появата на електронните елементи – лампи и транзистори, станало възможно конструирането на компютър от съвременен тип.

Представените тук материали са извадки от историческото съдебно решение, в което се постановява, че Джон Винсент Атанасов е законният изобретател на електронния цифров компютър – бел.а.

което включва вход, изход, преработване, съхраняване, както и комуникации, които са свързани или зависими от устройството. “Компютър” включва също два или повече компютъра, свързани помежду си с цел да комуникират при работа в мрежа. |[28]|

13. Под “компютър” още се разбира електронно, магнитно, оптично, хидравлично или органично устройство или група от устройства, които съобразно компютърна програма, състояща се от инструкции, вкарвани от човек или постоянни инструкции, съдържащи се в устройството или групата от устройства, може автоматично да извършва операции с данни и да комуникира с друг компютър или човек. Терминът компютър включва и директно свързани помежду си устройства, които дават възможност на компютъра да съхранява, предава информация, или да комуникира чрез компютърни програми с компютърни данни или с резултатите от компютърните операции към или от човек, друг компютър или друго устройство. |[29]|

14. Според трето тълкуване терминът компютър означава електронно, магнитно, оптично, електрохимично или друго високоскоростно устройство за обработване на информация, което извършва логически и математически действия или съхранява информация, и включва приспособления за съхраняване на

HENRY HALLADAY

UNITED STATES DISTRICT COURT

DISTRICT OF MINNESOTA

FOURTH DIVISION

HONEYWELL INC.,

Plaintiff,

vs.

SPERRY RAND CORPORATION and ILLINOIS SCIENTIFIC DEVELOPMENTS, INC.,

Defendants.

CIVIL ACTION

FILE NO. 4-67 CIV. 138

FINDINGS OF FACT, CONCLUSIONS OF LAW AND ORDER FOR JUDGMENT

информация или за комуникация, пряко свързани с/или работещи във връзка с това устройство; терминът не включва автоматични пишещи машини, портативни калкулатори или други подобии устройства. |[30]|

15. В българското право се срещат следните определения за компютър:

- "64. **Компютър.** ***Computer*** **е устройство, изпълняващо серия от последователни аритметични и логически операции с данни без намесата на човека.** В тази инструкция **терминът "Компютър" може да означава изчислителен комплекс, състоящ се от един или няколко компютъра и периферно оборудване."** (Курс. е на авт.) |[31]|
- С последните изменения и допълнения в Наказателния кодекс бе въведено определение за **компютърна информационна система**: **"21. (Нова - ДВ, бр.92 от 2002г.) "Компютърна информационна система" е всяко отделно устройство или съвкупност от взаимосвързани или сходни устройства, което в изпълнение на определена програма осигурява или един от елементите на което осигурява автоматична обработка на данни."** (Курс. е на авт.) |[32]|
- Освен горните определения за "компютър" в нормативните актове доскоро се срещаше описателното "**електронно-изчислителна машина**" ("**ЕИМ**"). Така например според старата редакция на Закона

---

3. Atanasoff

3.1 The subject matter of one or more claims of the ENIAC was derived from Atanasoff, and the invention claimed in the ENIAC was derived from Atanasoff.

3.1.1 SR and ISD are bound by their representation in support of the counterclaim herein that the invention claimed in the ENIAC patent is broadly "the invention of the Automatic Electronic Digital Computer."

3.1.2 Eckert and Mauchly did not themselves first invent the automatic electronic digital computer, but instead derived that subject matter from one Dr. John Vincent Atanasoff.

3.1.3 Although not necessary to the finding of derivation of "the invention" of the ENIAC patent, Honeywell has proved that the claimed subject matter of the ENIAC patent relied on in support

за патентите (ЗП) |[33]| не се считаха за изобретения "...програми за електронноизчислителни машини." (На законодателя му предстои да уточни дали "компютърна информационна система", "електронно-изчислителна машина" и "компютър" се припокриват, бел.а.)

16. За да бъде едно устройство компютър, то трябва да извършва **аритметически** или **логически операции**. Обикновено се дава следното определение за **операция**: математическо, логическо действие, осъществяване на постоянен контрол, функции на съхраняване или четене на данни и други комбинации между тях без

3.1.8 By August, 1940, in connection with efforts at further funding, Atanasoff prepared a comprehensive manuscript which fully described the principles of his machine, including detail design features.

3.1.9 By the time the manuscript was prepared in August, 1940, construction of the machine, destined to be termed in this litigation the Atanasoff-Berry computer or "ABC," was already far advanced.

3.1.10 The description contained in the manuscript was adequate to enable one of ordinary skill in electronics at that time to make and use an ABC computer.

3.1.11 The manuscript was studied by experts in the art of aids to mathematical computation, who recommended its financial support, and these recommendations resulted in a grant of funds by Research

3.1.17 Prior to his visit to Ames, Iowa, Mauchly had been broadly interested in electrical analog calculating devices, but had not conceived an automatic electronic digital computer.

3.1.18 As a result of this visit, the discussions of Mauchly with Atanasoff and Berry, the demonstrations, and the review of the manuscript, Mauchly derived from the ABC "the invention of the automatic electronic digital computer" claimed in the ENIAC patent.

3.1.19 The Court has heard the testimony at trial of both Atanasoff and Mauchly, and finds the testimony of Atanasoff with respect to the knowledge and information derived by Mauchly to be credible.

ограничение, също така комуникации, съхраняване или четене на данни от друго устройство, опериращо с електронни или магнитни импулси, или данни, ръчно въвеждани от човек. Под "компютърна операция" може да се разбира и друга функция, която компютърът е създаден да изпълнява. |[34]|

17. Необходимо е още електронното устройство, което извършва аритметически и логически операции, да работи с **висока скорост**. Понятието висока скорост няма точно количествено изражение и оценката се прави субективно.

The document scanned is a photocopy of the original decision written by Judge Earl Richard Larson presiding over the United States District Court, District of Minnesota, Fourth Division. The document is referenced as "File NO. 4-67 CIV. 138".

[24]|| 47 U.S.C. 553. SEARCHING AND SEIZING COMPUTERS, Scott C. Charney, Chief, Martha J. Stansell-Gamm, Computer Search and Seizure Working Group, General Litigation and Legal Advice Section Criminal Division Department of Justice, JULY 1994, FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS.

[25]|| COMPUTING. (From com-putare) literally, to reflect, to contemplate (putare) things in concert (com-). Any operation, not necessarily numerical, that transforms, modifies, re-arranges or orders physical markers in a medium. The physical markers maybe objects or events in their own right as in the computations carried out by the human cell or they may be symbols and descriptions of events as in data processing by a man-made computer. The early (1936) concept of computing by a Turing Machine involved writing and erasing characters by specific rules on a theoretically infinite tape. Examples are the simple permutation of the three letters A, B, C into C, A, B, the obliteration of the commas between them, yielding CAB, and the semantic transformation that changes CAB into TAXI, the recursive association of various adjectives before TAXI, etc. (von Foerster). Although computation by electronic computers is largely geared toward a desirable result computing does not imply a purpose.
WEB DICTIONARY OF CYBERNETICS AND SYSTEMS.

[26]|| АНГЛИЙСКО-БЪЛГАРСКИ РЕЧНИК, GABEROFF, П. изд., 1998-1999.

[27]|| TRANSACTION – CLA, SELECTED PROVISIONS AND COMMENTS FROM PROPOSED ARTICLE 2B, September, 1997 Draft.

[28]|| TEXAS PENAL CODE, SECTION 1. Title 7, Chapter 33, Section 33.01., DEFINITIONS.

[29]|| SENATE BILL NO. 881 Offered January 13, 1999 A BILL to amend and reenact § 18.2-152.2 of the Code of Virginia, relating to the Virginia Computer Crimes Act; penalty.

[30]|| 18 U.S.C. § 1030. Fraud and Related Activity in Connection with Computers.

[31]|| ИНСТРУКЦИЯ № 4444 ОТ 13.10.1999 Г. ЗА ПРАВИЛАТА ЗА ПОЛЕТИ И ОБСЛУЖВАНЕТО НА ВЪЗДУШНОТО ДВИЖЕНИЕ. Издадена от министъра

18. **Не са компютри** някои устройства, които работят на електронен принцип и имат сходни функции – електронни пишещи машини, мобилни телефони и т.н. Основното им предназначение не е да извършват аритметически и логически операции с висока скорост. Погрешно е да се смята, че един мобилен телефон с възможности да изпраща и получава съобщения по Интернет е компютър (освен ако не е конструиран с цел да бъде използван и като компютър - т. нар. **смартфон**).

19. От техническа гледна точка компютрите са вид машини, способни да съхраняват и/или обработват данни. |[35]| Следователно **запаметяването на данни** е друга основна функция на компютъра. В най-общ план - данните са информация, пригодна за четене, преработване, съхраняване и предаване чрез компютърното устройство.

20. От горното става видно, че точно определение на понятието компютър няма. Най-общо казано - **компютърът е обработваща информация машина**. При всички положения компютърът трябва да може да изпълнява **четири основни функции – приемане, съхраняване, обработка и предаване на данни**.

21. За да е компютър, устройството трябва да е в състояние да извършва аритметическите и логическите операции **самостоятелно**, без помощта на други устройства. За тази цел то трябва да се състои от минимум **необходими устройства**, като при липсата на което и да е от тях не би могло да функционира. Такива необходими устройства според съвременното състояние на техниката например са: централен процесор, харддиск, дънна платка, оперативна памет, флопи и/или *CD-ROM* устройство, както и интерфейсни устройства, правещи възможна комуникацията между компютър и човек - клавиатура, мишка,

---

на транспорта, обн., ДВ, бр. 100 от 19.11.1999 г., в сила от 7.02.2000 г., изм., бр. 37 от 5.05.2000 г., в сила от 5.05.2000 г.

[32]|| НАКАЗАТЕЛЕН КОДЕКС, ДВ, бр. 92 от 2002 г. Тук понятието може би е излишно усложнено - компютърната система не може да бъде друга, освен информационна. Освен това е плеоназъм изразът "...автоматична обработка на данни." Не е много ясно и какво би следвало да се разбира под "сходни устройства", бел. а.

[33]|| ЗП - ЗАКОН ЗА ПАТЕНТИТЕ. (Всички съкращения са дадени в СЪКРАЩЕНИЯ, бел. а.)

[34]|| SENATE BILL NO. 881 Offered January 13, 1999 A BILL to amend and reenact § 18.2-152.2 of the Code of Virginia, relating to the Virginia Computer Crimes Act; penalty.

[35]|| ИНТЕЛЕКТУАЛНО ПРАВО, Б. Йотов, 2000.

монитор. Не са съществени за нормалната работа на компютъра някои **допълнителни устройства**, чиято функция е да подпомагат работата на компютъра, както и да изпълняват специфични функции - скенер, принтер, плотер, модем и подобни. Следва да се отбележи, че някои допълнителни устройства, интегрирани в самия компютър, независимо че не са от съществено значение за функционирането на компютъра, също може да бъдат причислени към необходимите устройства, особено когато имат определяща роля за отличаването на една конкретна машина като самостоятелен компютър. Към тях може да се причислят модеми, звукови карти, видеоускорителни платки, ТВ-тунери, допълнителни процесори, допълнителни хардискови и флопидискови устройства, и други.

22. Нерядко под "компютър" още се разбира "**компютърна система**". Когато компютърът и периферията се свързват в единен комплекс от устройства, тогава се получава компютърна система. Компютърните системи могат да бъдат асемблирани в неограничен брой варианти с разнообразни входно-изходни устройства. |[36]|

23. Под "компютърна система" в повечето случаи се разбира устройство или група от свързани помежду си устройства, които въз основа на програма извършват автоматично преработване на данни (или изпълняват други сходни функции). "Компютърна система е всяка комбинация на компютър или компютърна мрежа с документация, софтуер или допълнителни устройства, поддържани от компютъра или компютърната мрежа." |[37]|

24. "Компютърна система" означава всяко отделно устройство или съвкупност от взаимосвързани или сходни устройства, което осигурява, или един от елементите на което осигуряват, в изпълнение на определена програма, автоматична обработка на данни. |[38]|

---

[36]|| When people speak of searching or seizing computers, they usually are not referring only to the CPU (Central Processing Unit). After all, a computer is useless without the devices that allow for input (e.g., a keyboard or mouse) and output (e.g., a monitor or printer) of information. These devices, known as "peripherals," are an integral part of any "computer system."
FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS, US Department of Justice Criminal Division Office of Professional Development and Training, Judd Robbins JULY, 1994.

[37]|| TEXAS PENAL CODE, SECTION 1, TITLE 7. OFFENSES AGAINST PROPERTY, CHAPTER 33. COMPUTER CRIMES, 33.01. Definitions.

[38]|| DRAFT CONVENTION ON CYBER-CRIME (Draft N° 19), April 27, 2000, Strasbourg, Declassified Public Version, PC-CY (2000), EUROPEAN COMMITTEE ON CRIME PROBLEMS (CDPC), COMMITTEE OF EXPERTS ON CRIME IN CYBER-SPACE (PC-CY).

25. Проличава известна неяснота относно съдържанието на понятието компютърна система. Трябва да се определи какво точно следва да се разбира под "компютърна система"; преработката на данни може да включва всяка система, която е базирана на тази функция, т.е. всички свързани помежду си системи – радио, телекомуникационни и т.н., да се включат в понятието. Не би трябвало да се разглежда като компютърна система в атомарния смисъл на това понятие съвкупността от компютри, свързани в мрежа, за изпълнение на разнообразни, предварително неуточнени задачи. Съвкупност от компютри е световната компютърна мрежа – Интернет. Става реч за система от компютри, свързани помежду си, за да решават комуникационни задачи. Например могат да се свържат в система две или повече устройства, всяко от които функционира като самостоятелен компютър. (Такива системи следва да се различават от т.нар. суперкомпютри. Последните се състоят от отделни функционални блокове, обединени конструктивно в една машина.) Тази самостоятелност тук се разглежда по два начина:

- **конструктивна**. Компютърът притежава всички необходими физични устройства и прилежащия софтуер – т.нар. компютърна система в атомарния смисъл на понятието, за да извършва специфичните за него операции самостоятелно;
- **функционална**. Поради необходимостта от извършване на по-голям обем изчисления понякога се налага да се свържат в единен изчислителен комплекс два или повече отделни компютъра. В резултат се получава мощен компютър, съставен от няколкото по-маломощни, с цел да бъде решена определена задача. Полученият изчислителен комплекс се доближава по своята структура до т. нар. суперкомпютър. В този смисъл би следвало да се използва терминът **система от компютри**, а не **компютърна система**.

26. Компютрите биват няколко вида. Разграничителни критерии са мобилността, предназначението, мощността и т.н.

- От гледна точка на **мобилността** компютрите се делят на преносими и стационарни. **Преносимите** компютри се характеризират с малки размери и автономен режим на работа. От своя страна те обикновено се делят на два подвида. Към първия спадат т.нар. **хандхелд** (*handheld*) устройства. Характеризират се с размери, които дават възможност да се носят в ръка или в дреха. Към втория спадат т.нар. **нотбук** (*notebook*) компютри. В сравнение със свръхмалките устройства тези компютри имат по-удобен за ползване интерфейс, а по технически данни се доближават до стационарните. За правото преносимите компютри представляват интерес с възможността да

бъдат обект на противозаконно отнемане, докато стационарните компютри основно се използват в качеството им на средство за извършване на престъпление. **Стационарните** компютри се отличават от мобилните по своята относителна неподвижност. Те са конструирани за работа във фиксирано положение. Делят се основно на **персонални компютри** *(PC),* които съставляват основната маса компютри за домашно ползване. Стационарните компютри, които се използват за професионални цели, се подразделят на **работни станции** – компютри, които се използват главно за решаване на специализирани задачи – в областта на инженерното проектиране, дизайна и т.н.; **сървъри** - главно за комуникационни цели; и **суперкомпютри**, предназначени за научноизследователски, военни и други цели, изискващи голяма изчислителна мощ.

- С оглед на **предназначението** си компютрите биват - за решаване на сравнително елементарни задачи (т. нар. органайзери), за обикновени офис-приложения (домашните компютри и използваните в офиси - персонални компютри, за професионални цели (работните станции, сървърите и др.), за сложни инженерни изчисления и научноизследователски и военни цели (суперкомпютрите).
- С оглед на **мощността** делението на компютрите в общи линии следва по-горната схема.

27. За правото делението на компютрите според различни критерии може да има значение основно за определяне **степента на вредите, които могат да се нанесат на тях и чрез тях**, а оттук - степента на обществената опасност.

28. Компютрите - като машини, имат отношение към други машини със сходни функции и предназначение - роботи, системи с изкуствен интелект, експертни системи.

29. **Роботите** (*robots)* за разлика от компютрите извършват изключително механична, химична, биологична работа и осъществяват физично, химично и биологично въздействие върху околната среда, а **не обработват информация**.

30. **Изкуственият интелект** (*AI*) е машинна система, която моделира дейността на човешкия мозък. По това тя се отличава от компютъра, който може да включва в себе си и изкуствен интелект, но задачите, които решава, по принцип са по-разнообразни. |[39]|

---

[39]|| Изследванията в областта на съвременния изкуствен интелект започват през 50-те години, след изобретяването на компютъра. През 1950г. Алан Тюринг публикува първата научна статия на тази тема със заглавие "Изчислителни машини и интелект". В нея се дефинират критериите, чрез които може да се определи интелигентността на една изчислителна машина.

31. Експертните системи (*ES*) са компютърни системи, програмирани да изпълняват функциите на експерти в дадена област. Технологията на изкуствения интелект се свързва с близката ѝ технология за база данни, която се явява основа на експертната система. Експертната система се състои от два компонента:

- програмата на изкуствения интелект се употребява за определяне точното правило или схема, които се съхраняват в базата данни;
- базата данни, съдържаща се в експертната система, е информационния резервоар, към който потребителят се обръща, за да намери отговор на свой въпрос. Това става, като той зададе на експертната система въпроси от типа: "ако - тогава" *("if – then")*, чрез серия от команди. "Ако" се извърши дадено действие, "какъв" ще бъде резултатът? Експертната система екстраполира голям брой възможни варианти и последствията от всеки от тях, като накрая изнамира най-подходящото решение. |[40]|

(последващите глави - в книгата)

През 1956г. на конференция на колежа в Дартмут група изследователи стига до извода, че компютърът трябва така да се програмира, че да моделира мисловната човешка дейност.

Оттогава до днес изследователската дейност, свързана с изкуствения интелект, се извършва предимно в академичната и научната сфера. През 1960г. Джоузеф Вайзбаум разработва компютърен психотерапевт с наименование ELIZA, който симулира диалог между пациент и психоаналитик. Слага се началото на клон в областта на изкуствения интелект, наречен обработка на естествен език. Днес тази технология се използва в програмите за разпознаване на говор и търсещите машини в уеб-пространството. Изкуственият интелект се използва и за създаване на експертни системи, бел. а.

[40]|| Типичен пример за експертна система е суперкомпютърът на IBM Deep Blue II, който през 1997г. побеждава световния шампион по шах Гари Каспаров.

Дял трети
НАКАЗАТЕЛНОПРАВНА ЗАЩИТА

Глава I
КОМПЮТЪРНИ ПРЕСТЪПЛЕНИЯ - СЪЩНОСТ

32. Навлизането в новата информационна ера закономерно води до разширяване полето на престъпните посегателства. Всеки може, разполагайки с подходящо компютърно оборудване и без да излиза от дома си, да извърши престъпление на другия край на света. |[41]|

33. Особено опасни са престъпленията във високотехнологичната индустрия - кражбите на интелектуална собственост. Печалбите тук са значителни и се съпътстват със значително по-малък риск за извършителите, защото е трудно да се идентифицират онези устройства, които са обект на престъплението, също така и поради относително по-леките присъди за тези престъпления. |[42]|

34. Все по-голяма опасност представляват компютърните саботажи, измами и кражби - включително кражбата на търговски тайни, |[43]| икономическия шпионаж, |[44]| както и всички случаи, в които компютърът е обект или средство за извършване на престъпление. Особено привлекателни се оказват персоналните компютри, в които се съхраняват данни от секретен характер. |[45]|

35. Компютърните престъпления вече не се свеждат единствено до икономически престъпления, а засягат по-широк кръг интереси. Устремното развитие на телекомуникационния сектор и по-специално разпространяването на *WWW* през 1990-те години засилва

[41]|| HIGH TECHNOLOGY CRIME INVESTIGATION ASSOCIATION, 1999 INTERNATIONAL TRAINING CONFERENCE, Town & Country Resort & Convention Center, San Diego, California, Monday, September 20, 99, Janet Reno.

[42]|| HIGH-TECH CRIME SUMMIT, U.S. Department of Justice, United States Attorney, Chris Watney, Judiciary Center, January 12, 2000.

[43]|| 18 U.S.C. 1832. §1832. THEFT OF TRADE SECRETS.

[44]|| 18 U.S.C.,§1341. ECONOMIC ESPIONAGE.

[45]|| ИНТЕЛЕКТУАЛНО ПРАВО, Б. Йотов, 2000, 196.

разпространението на нелегално и вредно съдържание – порнография, насилие, расова омраза и др. |[46]|

36. В законодателен план още не е ясно дали традиционните наказателни мерки са адекватни на новите видове престъпления, след като тези норми са създадени с цел да защитават правата върху осезаеми вещи, но не и върху нетелесни вещи, каквито се явяват повечето обекти на интелектуалната собственост.

37. В повечето държави дискусиите около компютърните престъпления започват още през 60-те със защитата на собствеността, която се дискутира като "*data protection"* и впоследствие се интегрира под концепцията за "*computer crime"*.|[47]|

38. През 70-те научните търсения се концентрират върху специфичните компютърни икономически престъпления, компютърния саботаж, компютърния шпионаж и компютърното пиратство. Започват първите изследвания в областта на компютърните престъпления, включително и криминалистични проучвания в тази област. |[48]| Тези изследвания хвърлят светлина върху все още ограничения брой случаи, оказали влияние върху съдебните решения по онова време, като например *the American Equity Funding case*, |[49]| *the German Herstatt case*, |[50]| или *the Swedish Volvo manipulations*. |[51]|

39. Обществеността и научно отношение към компютърните престъпления радикално се променило през 80-те, когато в пресата зашочнали да се публикуват непознати дотогава случаи за хакери, вируси и червеи, |[52]| и което предизвикало нуждата от нова наказателна стратегия. През 1983г. група от експерти на OECD дефинира термина

---

[46]|| LEGAL ASPECTS OFCOMPUTER-RELATED CRIME IN THE INFORMATION SOCIETY, prepared for the European Commission by prof. Dr. Ulrich Sieber, 1998.

[47]|| Пак там.

[48]|| Пак там.

[49]|| Пак там.

[50]|| Пак там.

[51]|| Пак там.

[52]|| The danger of "hacking" became especially evident in 1989 when criminal proceedings in the Federal Republic of Germany identified German hackers who were using international data networks to gain access to information inside American, British, and other foreign computer systems in order to sell their findings to the former Soviet secret service KGB.
Ammann/Lehnhard/Meißner/Stahl, Hacker für Moskau, 1989; Bundesminister des Inneren (ed.), Verfassungsschutzbericht 1989, 1990, p. 188; Hafner/Markoff, Cyberpunk, 1991, pp. 139 et seq.; Stoll, The Cuckoo's Egg, 1989.

”**компютърно престъпление**” (или “компютърно-относимо престъпление”) като: **всяко противозаконно действие, включващо автоматично преработване на данни и/или предаване на данни**. |[53]| (Последващите разработки въвеждат по-широката концепция за “*data and/or information crime”*.) |[54]| Широчината на тази дефиниция позволява употребата на същите работни хипотези за всички правни науки. |[55]|

40. В същото време употребата на компютърите и модерните комуникационни технологии от организираната престъпност прави очевиден факта, че от феноменологична точка “еднородно” компютърно престъпление вече не съществува.

41. Всяко престъпление, в това число и компютърното, има своя криминалистична характеристика, чийто елементи определят специфичните особености на методиката за тяхното разкриване и разследване. Поради малкия брой дела у нас, свързани с разкриването и разследването на компютърни престъпления, все още не е възможно да се направи пълна характеристика само на базата на собствени данни, без използването на чуждестранния опит на страни, в които този вид престъпления се извършват в големи мащаби и в продължение на много години. |[56]|

42. За да се проследи еволюцията на компютърните престъпления, криминолозите често прибягват до резултатите на статистиката. Това става особено наложително след драматичното увеличаване на пиратството с компютърни програми и хакерството от средата на 80-те години насам. Например в Германия през този период се забелязва значително увеличаване на нелегалното придобиване на компютърни данни. |[57]|

Around the same time, the peril of viruses and worms became especially obvious when the "Internet-worm" created by an American student affected and closed down about 6,000 computer systems within the "Internet"-network in only a couple of days.

Hafner/Markoff, Cyberpunk, 1991, pp. 251 et seq.; Markoff, Computer Intruder is Found Guilty, New York Times, 23 January 1990, at A 21, col. 1; Weihrauch, Der Morris-Wurm im Internet, (1988) Datenschutz-Berater, issue 12, pp. 1 et seq.

LEGAL ASPECTS OFCOMPUTER-RELATED CRIME IN THE INFORMATION SOCIETY, prepared for the European Commission by prof. Dr. Ulrich Sieber, 1998.

[53]|| Пак там.

[54]|| Пак там.

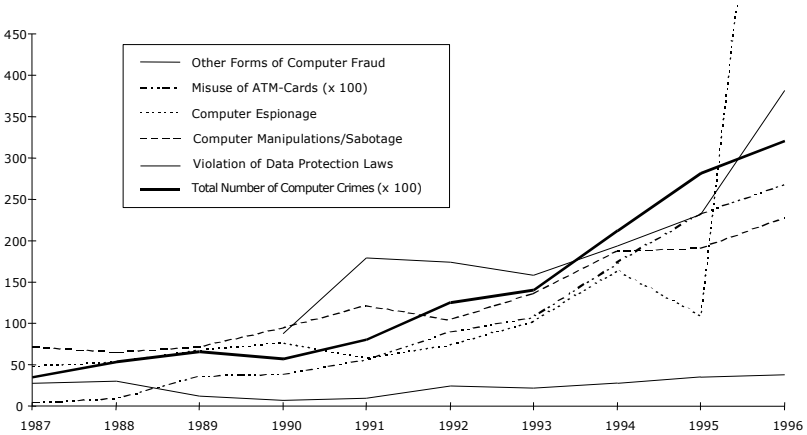
[55]|| Пак там.

[56]|| КРИМИНАЛИСТИКА, Бобев К., 2000

[57]|| Дадената по-долу таблица отразява сериозността на проблема:

43. Смисълът от приспособяването на правото към новите форми на престъпна дейност не изхожда единствено от технологичните промени, а по-скоро от фундаменталните промени на парадигмите: до средата на 20-ти век наказателните кодекси на всички държави защитават веществените, осезаемите обекти. |[58]| Обаче към края на века новозараждащото се информационно общество поставя на преден план ценността на информацията. Тази нова ценност не може да бъде защитавана като осезаем, веществен обект, а изисква нови законодателни подходи. |[59]|

44. САЩ са измежду първите държави, които отговарят чрез законодателни мерки на предизвикателствата в тази област. В Европа статутът на компютърните престъпления се установява към 1980г. Оказва се, че действията в тази област минават националните граници, а интернационалните аспекти на проблема въвличат институции като *Organisation for Economic Cooperation and Development, the Council of Europe* и *the European Community* в дебати за нуждата от законова



German Police Crime Statistics: Number of Computer Crimes Reported to the German Police.

LEGAL ASPECTS OFCOMPUTER-RELATED CRIME IN THE INFORMATION SOCIETY, prepared for the European Commission by prof. Dr. Ulrich Sieber, 1998

[58]|| Пак там.

[59]|| Пак там.

интервенция. |[60]| Днес важна роля играят и редица други международни организации. |[61]|

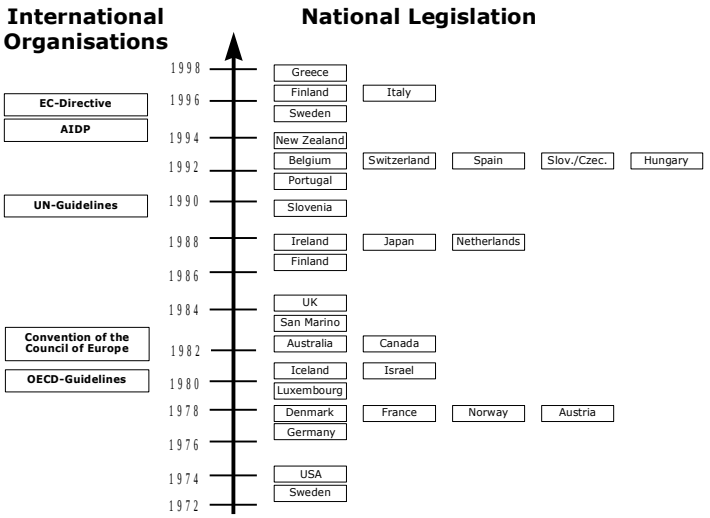
45. Като се има предвид казаното дотук, може да се направят някои изводи относно особеностите на компютърните престъпления:

- **компютърните престъпления са по-чести, по-разнообразни и по-опасни;**
- **компютърните престъпления могат да бъдат извършени почти срещу всеки;**
- **компютърните престъпления са по-мобилни и обикновено имат интернационален характер;**
- **компютърните престъпления стават все по-атрактивни за организираната престъпност.**

---

[60]|| COMPUTER LAW, Chris Reed, 1992.

[61]|| Тези графики илюстрират ролята, която по-известните международни организации играят в борбата за предотвратяване на компютърните престъпления:



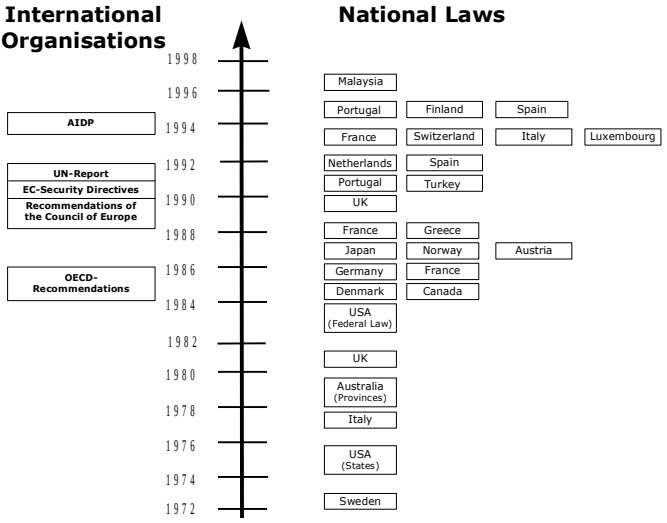
Privacy Protection (Primarily General Administrative and Civil Data Protection Law)

46. След спорове и обсъждания към 1995г. се стига до извода, че спецификата на компютърните престъпления изисква да се преразгледат основните наказателноправни постановки и да се предприемат адекватни мерки за защита на правата върху компютърните продукти. |[62]|

Глава II
ОСОБЕНОСТИ НА КОМПЮТЪРНИТЕ ПРЕСТЪПЛЕНИЯ

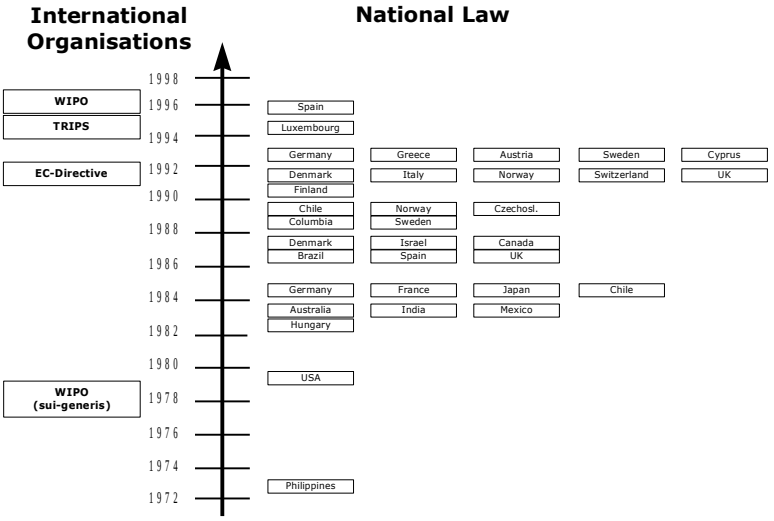
47. Теорията разглежда компютърните престъпления в няколко аспекта. |[63]|

48. Компютърната система може да бъде предмет (обект) на престъпно деяние. В тези случаи най-вече се говори за **кражба** на



компютърна техника. Тук се отнасят традиционните способи за извършване на престъпления, насочени към отнемане на чуждо имущество. Характерна особеност на този начин за извършване на престъплението е, че предметът на престъпното посегателство е компютърната техника, а средствата, които се използват, са традиционните инструменти – обикновено за взлом, и други. |[64]| Освен чисто физическото отнемане на обекта на престъплението е възможно също да бъде откраднатa **услуга** или **информация**. |[65]|

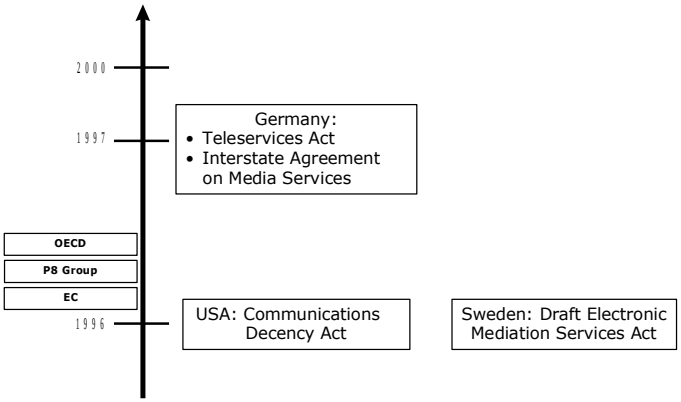
49. Компютърната система може да бъде средство за извършване на престъпното деяние. |[66]| Тази категория обхваща престъпления като детска порнография, измами, посегателства срещу интелектуалната собственост, продажба на забранени стоки он-лайн и т.н. |[67]| Прихващането на данни като пример за такъв вид престъпление може да бъде извършено чрез използване на персонален компютър за претърсване на "кошчето за боклук"**,** при което престъпникът намира изхвърлена документация. |[68]| Примери може да се дадат и с незаконния достъп до компютърна техника: престъпникът използва момента, когато лицето, отговарящо за компютърната система, на-



Intellectual Property Protection (Using the Example of Copyright Protection of Computer Programs)

пуска работното си място, като оставя персоналния компютър в режим на работа; престъпникът се включва към линия за връзка и след получаване на сигнал за свободен модемен вход се включва със собствен модем и персонален компютър; престъпникът се представя за законен потребител, като използва кодовете и идентификационните шифри, получени чрез подкуп, корупция и други противоправни действия. |[69]|

50. Възможно е заниженият контрол от страна на длъжностните лица, както и ниската надежност на мерките за защита да дадат възможност на престъпницитс да променят установените форми на отчетност и резултатите от финансово-счетоводните операции. Незаконнното манипулиране с данни може да стане по няколко начина: промяна на данните чрез подмяна или въвеждане на нови данни както на входа, така и на изхода на системата; въвеждане на специална разрушителна програма (вирус), която е в състояние да зарази работната програма и да я накара да изпълни команди за



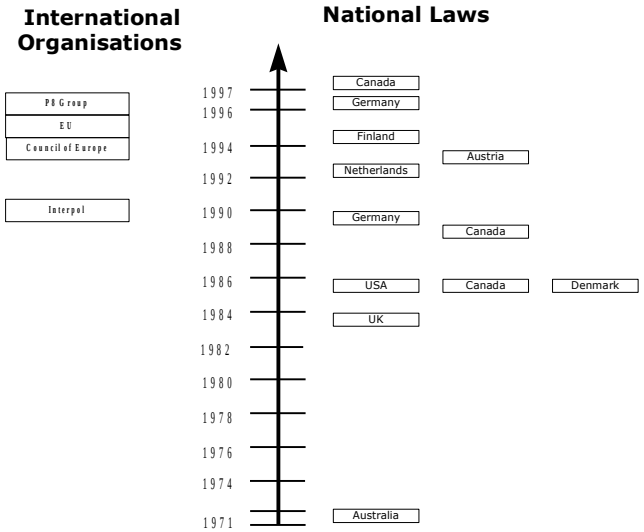
изтриване на данни; претоварване на машинната памет; създаване на смущения в работата на компютърната система, и други. |[70]|

51. Компютърната система може да се разглежда като случаен елемент на престъпното деяние. |[71]| Например педофили могат да съхраняват престъпна информация в своите компютри, продавач на дрога да съхранява информация за своите клиенти, и т.н.|[72]|

52. Компютърната система може да бъде използвана и като доказателство в съда. |[73]|

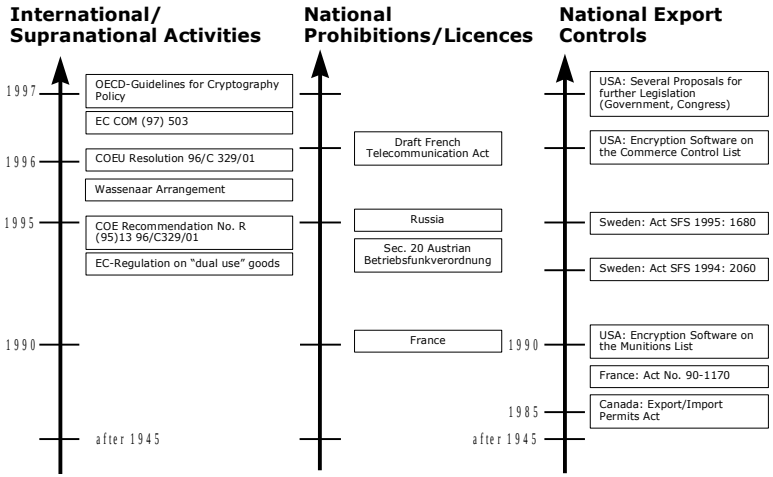
53. В редица случаи компютърната система може да изпълни в престъплението две или три роли едновременно. Например хакер употребява своя компютър, за да вкара вируси в друга система. |[74]| В този случай неговият компютър може да се яви както инструмент на престъплението, така и доказателство в съда. |[75]|

54. За да бъде деянието квалифицирано като престъпление, между факта на деянието и настъпилите последици трябва да съществува **причинна връзка**. |[76]| Простото съвпадение на момента на излизането от строя на компютърната система, предизвикано от неизправности или програмна грешка, и момента, в който е



осъществен незаконен достъп, без да е налице причинна връзка между тях, няма да доведе до наказателна отговорност за излизането от строя на компютърната система. |[77]|

55. По отношение на **субективната страна** на деянието не се забелязват съществени отличия от общите наказателноправни постановки. Престъпникът трябва да е извършил деянието **умишлено**, да съзнава, че е нарушил законова норма чрез неправомерното си въздействие върху обекта на престъплението, и да желае или



Security Regulations (Using the Examples of Prohibitions and Export Controls for Cryptography)

LEGAL ASPECTS OFCOMPUTER-RELATED CRIME IN THE INFORMATION SOCIETY, prepared for the European Commission by prof. Dr. Ulrich Sieber, 1998. [62]|| There are no precise, reliable statistics on the amount of computer crime and the economic loss to victims, partly because many of these crimes are apparently not detected by victims, many of these crimes are never reported to authorities, and partly because the losses are often difficult to calculate. Nevertheless, there is a consensus among both law enforcement personnel and computer scientists who specialize in security that both the number of computer crime incidents and the sophistication of computer criminals (i.e., hackers) is increasing rapidly. Estimates

съзнателно да допуска причиняването на последствията, или да се отнася към тяхното настъпване безразлично. |[78]|

56. Освен умишлено, престъпното деяние може да бъде извършено и по **небрежност**. Отговорност за извършване на деяние по небрежност може да се носи например от специалист, инсталирал компютърна програма без да извърши необходимата антивирусна проверка, и в резултат от действието на вирус бъде изтрита важна информация. |[79]| Изобщо за да бъде едно деяние квалифицирано като престъпление, то трябва да притежава предвидените от закона белези. В противен случай не може да се конституира като правнорелеватно.

---

are that computer crime costs victims in the USA at least US$ 50 10^8/year, and the true value of such crime might be substantially higher. Experts in computer security, who are not attorneys, are beginning to speak of "information warfare". While such "information warfare" is just another name for computer crime, the word "warfare" does fairly denote the amount of damage inflicted on society.
COMPUTER CRIME, Ronald B. Standler, 1999.

[63]|| COMPUTER EVIDENCE PROCESSING, Potential Law Enforcement Liabilities, Michael R. Anderson, NEW TECHNOLOGIES, Inc. February 22, 2001.

[64]|| КРИМИНАЛИСТИКА, Бобев К., 2000.

[65]|| STATEMENT OF ROBERT S. LITT, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION UNITED STATES DEPARTMENT OF JUSTICE, BEFORE THE SUBCOMMITTEE ON SOCIAL SECURITY SENATE WAYS AND MEANS COMMITTEE, UNITED STATES SENATE, MAY 6, 1997.

[66]|| Similarly, many crimes involving computers are no different from crimes without computers: the computer is only a tool that a criminal uses to commit a crime. For example:

- Using a computer, a scanner, graphics software, and a high-quality color laser printer for forgery or counterfeiting is the same crime as using an old-fashioned printing press with ink.
- Stealing a laptop computer with proprietary information stored on the hard disk inside the computer is the same crime as stealing a briefcase that contains papers with proprietary information.
- Using the Internet or online services to solicit sex is similar to other forms of solicitation of sex, and so is not a new crime.
- Using computers can be another way to commit larceny.

COMPUTER CRIME, Ronald B. Standler, 1999

[67]|| STATEMENT OF ROBERT S. LITT, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION UNITED STATES DEPARTMENT OF JUSTICE, BEFORE THE SUBCOMMITTEE ON SOCIAL SECURITY SENATE WAYS AND MEANS COMMITTEE, UNITED STATES SENATE, MAY 6, 1997.

[68]|| КРИМИНАЛИСТИКА, Бобев К., 2000.

[69]|| Пак там.

[70]|| Пак там.

Обстоятелства, свързани с личността на престъпника.

57. При изследванията, правени в страните с висока компютъризация, относно **мотивацията на извършителите** на компютърни престъпления са установени три групи лица, нарушаващи закона.

- Първата група включва специалисти, които притежават **висок професионализъм** в областта на компютърната техника и програмирането, съчетан с определена степен на **изобретателност и фанатизъм.** Характерна особеност за престъпниците от тази група е,

---

[71]|| Before preparing a warrant to seize all or part of a computer system and the information it contains, it is critical to determine the computer's role in the offense. First, the computer system may be a tool of the offense. This occurs when the computer system is actively used by a defendant to commit the offense. For example, a counterfeiter might use his computer, scanner, and color printer to scan U.S. currency and then print money. Second, the computer system may be incidental to the offense, but a repository of evidence. For example, a drug dealer may store records pertaining to customers, prices, and quantities delivered on a personal computer, or a blackmailer may type and store threatening letters in his computer.
In each case, the role of the computer differs. It may constitute "the smoking gun" (i.e., be an instrumentality of the offense), or it may be nothing more than an electronic filing cabinet (i.e., a storage device). In some cases, the computer may serve both functions at once. Hackers, for example, often use their computers both to attack other computer systems and to store stolen files. In this case, the hacker's computer is both a tool and storage device. Whatever the computer's role in each case, prosecutors must consider this and tailor warrants accordingly.
FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS, US Department of Justice Criminal Division Office of Professional Development and Training, Judd Robbins JULY, 1994.

[72]|| INTERNATIONAL COMPUTER CRIME CONFERENCE, "Internet as the Scene of Crime", Oslo, Norway, May 29-31, 2000, Remarks of James K. Robinson.

[73]|| SECTION 2 - PROCEDURAL LAW, Article 14 - Search and Seizure of Stored Computer Data, U. S. Department of Justice, Criminal Division, Washington, D.C. 20530, APPENDIX A: SAMPLE COMPUTER LANGUAGE FOR SEARCH WARRANTS.

[74]|| U.S. Department of Justice, United States Attorney, Northern District of Texas, April 12, 2000, SENATE BILL NO. 881, Offered January 13, 1999.
A BILL to amend and reenact §§ 18.2-152.2, 18.2-152.4 and 18.2-152.12 of the Code of Virginia, relating to the Virginia Computer Crimes Act; penalty.

[75]|| ACCESS DEVICE FRAUD STATUTE - 18 U.S.C. 1029, Computer Fraud and Abuse Act - 18 U.S.C. 1030, No-Knock Statute - 18 U.S.C. 3109; Privacy Protection Act - 42 U.S.C. 2000aa, Stored Communications Access - 18 U.S.C. 2701, et seq., Wiretap Statute ("Title III") - 18 U.S.C. 2510, et seq.; 47 U.S.C. 553. SEARCHING AND SEIZING COMPUTERS, Scott C. Charney, Chief, Martha J. Stansell-Gamm,

че при тях **няма категорично мотивирано противоправно намерение**, а действията, които извършват, са по-скоро израз на демонстрация на интелектуално и професионално превъзходство над автора, разработил конкретната компютърна програма. В много случаи те показват своите способности пред познати, колеги и роднини, без да предприемат мерки за укриване на престъплението.

- Втората група престъпници са лица - компютърни специалисти, които страдат от нов вид **психично заболяване,** произтичащо от системни нарушения на техния информационен режим на работа, от информационен глад или информационно претоварване, екстремално превключване от един информационен процес към друг, липса на достатъчно време за адаптиране към нов информационен режим на работа. По същество това е професионално заболяване на специалисти, попадащи в стресови ситуации, което причинява силно главоболие, повишено кръвно налягане, интензивно потоотделяне при работа с компютърната техника. В такова състояние те извършват престъпни действия, насочени към унищожаване на програми или повреждане на технически средства, без да влагат престъпен умисъл.

- Третата група лица, извършители на компютърни престъпления, са **професионалисти**, членове на добре организирани групи, снабдени със съвременна компютърна техника. Тези лица притежават устойчиви престъпни навици, многократно участват в извършването на престъпления и вземат мерки за тяхното укриване. Преобладаващата част от тези лица имат постоянни служебни ангажименти и външно не показват отклонения от общоприетите норми и правила на поведение. Те биват лица, използващи **програмни средства** - счетоводители, касиери, оператори на ЕИМ, оператори на периферии устройства, администратори на автоматизирани информационни системи, програмисти и други; лица, които използват **компютърна техника** - инженери по терминална техника, специалисти по телекомуникационни свръзки, изпълняващи организационно-управленски задачи, ръководители и сътрудници на информационно-аналитични служби, началници на звена по

Computer Search and Seizure Working Group, General Litigation and Legal Advice Section Criminal Division Department of Justice, July 1994, FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS.

[76]|| Пак там.

[77]|| Пак там.

[78]|| Пак там.

[79]|| Пак там.

програмиране, сътрудници от службите по безопасност на труда и т.н.|[80]|

58. Престъпниците от сферата на **външните потребители** са лица, които познават добре съответната компютърна система на потърпевшата страна. Техният достъп е свързан със сервизно обслужване, разработване на програмни продукти на договорна цена, изпълнение на контролни функции от по-горна инстанция, използване на бази данни като клиенти. |[81]|

Обстоятелства, свързани с потърпевшата страна.

59. Причините, поради които голяма част от компютърните престъпления не се разкриват, се дължат на поведението на потърпевшата страна. Различни са факторите, поради които тя не търси съдействие от компетентните органи за разкриване и разследване на компютърните престъпления:

- опасения, че разходите за воденото дело ще бъдат по-големи от нанесените загуби от престъплението;
- опасения от загуба на авторитет в деловите кръгове, респективно загуба на клиенти, които използват компютърната система;
- наличие на фирмени тайни, които в процеса на разследването могат да станат достояние на конкурентни фирми;
- опасения, че разследването ще открие сериозни пропуски в защитата на информацията от посегателства;
- опасения, че разследването на компютърното престъпление може да постави под съмнение професионалната и служебната пригодност на длъжностните лица, и т.н. |[82]|

[80]|| КРИМИНАЛИСТИКА, Бобев К., 2000.

[81]|| Пак там.

[82]|| Пак там.

Глава III
ВИДОВЕ КОМПЮТЪРНИ ПРЕСТЪПЛЕНИЯ. ЗАКОНОДАТЕЛНО РАЗВИТИЕ

60. Не съществува консенсус по отношение на схемата, по която се класифицират компютърните престъпления. С цел хармонизиране на законодателствата международните организации предприемат различни инициативи, с помощта на които се координира развитието на националните правни системи. Законодателството в областта на компютърните престъпления засега се развива в няколко основни направления: **престъпления срещу собствеността, икономически престъпления, престъпления срещу интелектуалната собственост, незаконно и вредно съдържание, наказателнопроцесуални аспекти, правни мерки за осигуряване секретността на информацията.** |[83]|

§ 1. Престъпления против собствеността

61. Първите законодателни реформи в тази област водят началото си от 70-те и 80-те години, като през този период се развиват технологиите, даващи възможност да се събира, съхранява и предава информацията по автоматичен път. Различните законодателства подхождат към проблема, като адаптират съществуващите норми с цел да се гарантира по-ефикасна защита. |[84]|

---

[83]|| Тези инициативи се разглеждат съответно като: *computer-related infringements of privacy, computer-related economic crime, intellectual property protection, illegal and harmful contents, computer-related procedural law, as well as legal regulations on security measures*.
LEGAL ASPECTS OFCOMPUTER-RELATED CRIME IN THE INFORMATION SOCIETY, prepared for the European Commission by prof. Dr. Ulrich Sieber, 1998.

[84]|| Законодательство России в области информатизации начало формироваться с 1991 года и включало до 1997 года десять основных законов. Это закон "О средствах массовой информации" (27.12.91 г. 2124-I), Патентный закон РФ (от 23.09.92 г. 3517-I), закон "О правовой охране топологий интегральных микросхем" (от 23.09.92 г. 3526-I), закон "О правовой охране программ для электронных вычислительных машин и баз данных" (от 23.09.92 г. 3523-I), Основы законодательства об Архивном фонде РФ и архивах (от 7.07.93 г.

62. Основната група от престъпления срещу собствеността (*crimes against privacy*) се конституира като посегателства срещу правото на собственост и може, в зависимост от развитието на отделните законодателства, |[85]| да включва следните деяния:

- незаконно разкриване, разпространяване, придобиване и/или достъп до данни,
- незаконна употреба на данни,
- незаконно проникване в, изменение и/или фалшифициране на данни с намерение да се причинят вреди,
- незаконно събиране, записване и/или съхраняване на данни,
- съхраняване на неверни данни. |[86]|

5341-I), закон "Об авторском праве и смежных правах" (от 9.07.93 г. 5351-I), закон "О государственной тайне" (от 21.07.93г. 5485-I), закон "Об обязательном экземпляре документов" (от 29.12.94 г. 77-ФЗ), закон "О связи" (от 16.02.95 г. 15-ФЗ), закон "Об информации, информатизации и защите информации" (от 20.02.95 г. 24-ФЗ), закон "Об участии в международном информационном обмене" (от 5.06.1996 г. 85-ФЗ).

[85]|| "Data protection laws" were enacted and have been constantly revised and updated, protecting the citizens' right of privacy with administrative, civil, and penal regulations in 1973 in Sweden, 1974 in the United States of America, 1977 in the Federal Republic of Germany, 1978 in Austria, Denmark, France and Norway, 1979 and 1982 in Luxembourg, 1981 in Iceland and Israel, 1982 in Australia and Canada, 1984 in the United Kingdom, 1987 in Finland, 1988 in Ireland, Japan and the Netherlands, 1991 in Portugal, 1992 in Belgium, Spain and Switzerland, 1995 in Spain, and 1997 in Italy and Greece. Additional data protection laws can be found in many federalistic jurisdictions (e.g. Canada, the Federal Republic of Germany, Switzerland, or the United States of America) as well as in many "sectorial" laws regulating privacy protection in specific areas which today become increasingly important (e.g., in the area of telecommunication, police data or online services). In Brazil, the Netherlands, Portugal and Spain, privacy protection even brought about constitutional amendments.
LEGAL ASPECTS OFCOMPUTER-RELATED CRIME IN THE INFORMATION SOCIETY, prepared for the European Commission by prof. Dr. Ulrich Sieber, 1998.

[86]|| Most of the respective provisions are contained in the general data protection acts cited supra chapter I, fn. See, for Austria, Sections 48 and 49 Data Protection Act; for Denmark, Section 27 (1) No. 1 Private Registers Act and Section 29 (1) No. 1 Public Authorities' Registers Act; for Germany, Section 203 Penal Code and Section 43 Federal Data Protection Act of 1990; for Finland, Section 45 of the Personal Registers Act 1987; for France, Sections 41, 42, 43 and 44 Data Protection Act; for Israel, Sections 2 (5), (9); 16; 23B of the Protection of Privacy Law; for Italy, Article 35 Data Protection Law; for Luxembourg, Articles 33, 34, 35 of the Act Regulating the Use of Nominal Data; for Sweden, Sections 20 (3), (4); 21 of the Data Protection Act; for the UK, Section 15 of the Data Protection Act; for the USA, the Fair Credit Reporting Act 1970 (codified, as

63. С оглед осигуряването на ефикасна защита върху собствеността редица международни институции разработват специални мерки, с които се цели да се намали нивото на компютърната престъпност - |[87]|

§ 2. Престъпления срещу интелектуалната собственост

amended, at 15 U.S.C. §§ 1681-1681t), the Privacy Act 1974 (codified, as amended, at 5 U.S.C. § 552a), the Cable Policy Act of 1984, the Electronic Communications Privacy Act of 1986 (codified at 18 U.S.C. § 1367, 2232, 2510-2522, 2702-2711, 3117, 3121-3127), and the Video Privacy Protection Act of 1988 (codified at 22 U.S.C. § 2000aa) as well as various state laws. See for an overview on State Data Protection Laws in the United States Perritt, Law and the Information Superhighway, 1996, pp. 115 et seq.

[87]|| Contrary to the progress achieved in the field of administrative and civil privacy law, international harmonisation in the domain of criminal privacy law has not really progressed yet. Only first approaches to deal with these questions have been undertaken by the Council of Europe, the United Nations and the Association International de Droit Pйnal.

Council of Europe

The main steps in the field of criminal privacy law have been taken by the Council of Europe. The above-mentioned Data Protection Convention of the Council of Europe of 1981 contains, in its Article 10, a provision stating that "each party undertakes to establish appropriate sanctions and remedies for violation of ... the basic principles for data protection." However, this clause leaves it up to the Member States to determine the nature of these sanctions and remedies (civil, administrative or criminal), as well as their scope of application.

Further studies on the harmonisation of criminal privacy law were undertaken in the course of the Select Committee of Experts for Computer-Related Crime of the Council of Europe. In his comparative report one of the Committee's Scientific Experts suggested already in 1986 that the harmonisation of law should be extended to the field of criminal law provisions by a two step working plan in order to arrive at an international consensus in this field: First, an appropriate international organisation should aim towards developing certain basic principles which would then be considered by all national legislations in the field of computer-related criminal privacy legislation and which could be presented in the form of a recommendation or convention. Based on these principles, a list of acts of criminal privacy infringements should then be developed. This list of acts could supplement the OECD list mentioned above, should prevent both under- and over-criminalisation, and could be put down in the form of a model law. Following these suggestions, the Committee recommended basic principles which should be taken into account by all Member States when acting in the field of computer-related

64. Неоторизираното копиране и употреба на компютърни програми, наричано **кражба на софтуер** или **софтуерно пиратство,** включва софтуер, който по правило е високостойностен творчески продукт – обект на авторскоправна закрила. |[88]|

65. По отношение на традиционните авторски творби (*cultural works of authorship)*, |[89]| конвергенцията при обработването на данни и комуникацията с данни под формата на цифровизация и разпространение на културни продукти (в т.ч. продажбата на компакт-дискове с музика и видео) показва общия корен на софтуерното,

---

criminal privacy legislation. These basic principles were the following:

"(1) The protection of privacy against offences caused by modern computer technology is of great importance. However, this protection should be based primarily on administrative and civil law regulations. Recourse to criminal law should be made only as a last resort. This means that criminal sanctions should be used only in cases of severe offences in which adequate regulation cannot be achieved by administrative or civil law measures (Ultima ratio principle).

(2) The respective criminal provisions must describe the forbidden acts precisely and should avoid vague general clauses. Precise description of illegal acts, without however resorting to a casuistic legislation technique, can easily be achieved, for example, for specific unfair methods of obtaining data or for specific sensitive data. In cases in which precise descriptions of illegal acts are not possible due to the necessity of a difficult balancing of interests (privacy versus freedom of information), criminal law should decline from incriminating substantive infringements of privacy and adopt a formal approach, based on administrative requirements of notification of potentially harmful DP-activities. Failure to comply with these notification requirements and to obey regulations of the data protection authorities could then be subject to sanctions. These formal offences are in accordance with the principle of culpability as long as they can be considered bans per se (Gefährdungsdelikte, délits-obstacle), which punish the endangering of privacy rights. In many areas criminal privacy infringements, therefore, would presuppose both the infringement of formal requirements, as well as the endangering of substantive privacy rights (Principle of precision in the wording of criminal law).

(3) The criminalised acts should be described as clearly as possible by the respective penal law provisions. Therefore, a too-extensive use of the referral technique (i.e., the technique pursuant to which activities regulated outside the penal law provisions are criminalised by reference) makes criminal provisions unclear and incomprehensible and should be avoided. If implicit or explicit references of the criminal law are used, the criminal provision itself should at least give an adequate idea of the forbidden acts (Clearness principle).

(4) Different computer-related infringements of privacy should not be criminalised in one global provision. The principle of culpability requires a differentiation according to the interests affected, the acts committed, the status of the perpetrator, as well as of his intended aims and other mental elements (Principle of differentiation).

музикалното, видео- и мултимедийното пиратство. |[90]| Връзката между софтуерното пиратство и другите форми на пиратство се доказва с появяването на нови устройства за игри и компакт-дискове, които съдържат компютърни програми, бази данни, книги, музика и филми. |[91]| Въпреки че пиратството не е ново явление, налице са условия, които са причина то да приеме застрашителни размери и да стане сериозна заплаха за системата на авторското право. |[92]|

66. Правата на носителя на авторското право се нарушават, когато някое от действията, изискващи изрично разрешение от носителя им, се извърши от друго лице без неговото съгласие. Такъв

---

(5) In principle, computer-related infringements of privacy should only be punishable if the perpetrator acts with intent. Criminalisation of negligent acts should be an exception requiring a special justification (Principle of intent).

(6) Minor computer-related offences against privacy should be punished only in accordance with recommendation No. (87) 18 on the Simplification of Criminal Justice, on complaint of the victim or of the Privacy Protection Commissioner or of the Privacy Protection Authority (Principle of complaint)."

Especially due to lack of time, the Committee did not discuss further-going proposals concerning guidelines for national legislators in the field of criminal privacy legislation. However, the above-mentioned proposal of the Council of Europe's Scientific Experts had suggested that first it should be clearly decided if the intention of such guidelines was to create either a "minimum list" (to guarantee a minimum protection of privacy in all Member States), an "optional list" (to illustrate additional acts which might be criminalised in Member States), or a "maximum list" (to prevent over-criminalisation and imprecise criminal laws) and/or a model law. The proposal had especially suggested to concentrate criminal privacy law on the following acts:

"(1) The wilful and illegal disclosure of personal secrets committed by public officials, employees of the PTT services and specific holders of professional secrecy (especially medical personnel, lawyers and bank employees) who have obtained the secrets in the course of professional work;

(2) the wilful and illegal disclosure and/or obtainment of automatically-stored personal data, if this act considerably endangers the privacy rights of an individual and infringes upon the formal notification requirements of privacy legislation or infringes upon a (non-appealable or provisionally enforceable) administrative or court decision;

(3) the wilful and illegal obtainment of automatically-stored personal data by false pretences and/or by infringement of security measures;

(4) the wilful disclosure of incorrect (automatically-stored) personal data (if this act endangers the privacy rights of an individual);

(5) the wilful alteration, storage, erasure and/or suppression of (automatically-stored) personal data committed by unauthorised persons (especially by outside parties) with the intent to cause damage to another party or to gain an illegal profit."

United Nations

случай е отразен в хипотезата на софтуерното пиратство: **неразрешеното възпроизвеждане на материали, поставени под закрилата на авторското право, за търговски цели и неразрешеното търгуване с възпроизведените материали се нарича "пиратство".** |[93]|

67. Отличителна черта на пиратството представлява провеждане на неразрешена дейност с цел търговска печалба. Елементът търговска печалба подсказва, че пиратството често се извършва организирано, тъй като то не обхваща само неразрешеното възпроизвеждане на

In 1994, the UN published the "UN Manual on the Prevention and Control of Computer-Related Crime". Among others, the manual contains a chapter on "Substantive Criminal Law Protecting Privacy". The main lines of thinking in the manual follow the above mentioned proposals of the Council of Europe.

Association International de Droit Pénal

The recommendations of the XVth International Congress on Penal Law Section II on Computer Crimes and other Crimes against Information Technology held in Rio de Janeiro, 4-10 September 1994 also contain a chapter on "Specific Issues of Privacy Protection". The chapter is in line with the above-mentioned principles of the Council of Europe and the UN. With respect to privacy protection the recommendations state:

"12. The significance of protecting privacy interests in the transformed information age against new dangers emanating from the information technology should be recognized. However, the legitimate interests in the free flow and distribution of information within society must also be respected. Privacy interests include the right of citizens to access, by legal means consistent with international human rights, information about themselves which is held by others.

13. The discussion demonstrated that there are significant differences in opinion as to both the means by, and the degree to which protection should be afforded by administrative, civil, regulatory and criminal law. There are also serious disagreements as to the extent to which criminal law should be involved in the protection of privacy. Therefore, non-penal measures should be given priority, especially where the relations between the parties are governed by contract.

14. Criminal provisions should only be used where civil law or data protection law do not provide adequate legal remedies. To the extent that criminal sanctions are used, the AIDP notes the basic principles which should be taken into account by states when enacting criminal legislation in this field, as recommended in Recommendation (89) 9 of the Council of Europe. The AIDP proposes further that criminal provisions in the privacy area should in particular:

be used only in serious cases, especially those involving highly sensitive data or confidential information traditionally protected by law;

be defined clearly and precisely rather than by the use of vague or general clauses (Generalklauseln), especially in relation to substantive privacy law;

establish a difference between the various levels of gravity of the offenses and to respect the requirements of culpability;

съответната творба, но още и продажба или разпространение на незаконно възпроизведената творба, което изисква определена форма на организирана мрежа за разпространение или връзка с евентуалните купувачи. За потребителя е видим често само краят на веригата на такова разпространение - под формата на пункт за продажба, който предлага придобития чрез пиратство продукт. Важно е да се знае, особено когато се разглежда въпросът за средствата за ефективна борба с пиратството, че зад един такъв пункт често се крие организирано предприятие, което незаконно възпроизвежда поставена

---

be restricted primarily to intentional acts; and
permit the prosecution authorities to take into account, in respect of some types of offences, the wishes of the victim regarding prosecution.
15. Further study should be undertaken to attempt, with special regard to public databases, to define a list of acts which should appropriately be criminalised. This could include intentional acts of infringement of secrecy and serious forms of illegal collection, use, transfer and alteration of personal data which create a danger to personal rights. A starting point for this study might be the tentative proposals that were considered by the select committee of experts on computer-related crime of the Council of Europe."
European Union
The above mentioned 1995 general EC Data Protection Directive addresses criminal law questions only globally. Article 24 of the Directive provides that Member States shall adopt suitable measures to ensure the full implementation of the provisions of the Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to the Directive.
LEGAL ASPECTS OFCOMPUTER-RELATED CRIME IN THE INFORMATION SOCIETY, prepared for the European Commission by prof. Dr. Ulrich Sieber, 1998.
[88]|| A German case from 1994 shows the high resulting damages and also illustrates the careless handling of security measures by program distributors and the proneness of new forms of distribution to misuse: During the biggest German computer fair, a software dealer had distributed about 200,000 free copies of a CD ROM, which contained programs worth more than DM 100,000. Each program was code protected which should only allow the CD-user who concluded a contract to gain access to the program. However, young hackers succeeded in "cracking" the code and the program protection of the CD ROM and passed the code on to the visitors on the same fair.
Software piracy in the field of standard programs does not nearly represent a trivial offence of young PC-users. The software industry now increasingly takes legal action against enterprises that use unlicensed software. In these cases, often only a fraction of the installed programs are licensed. For example, during a police search at a company in northern Germany, the police found that only nine out of 58 installed programs of which were licensed. In this case, a fine of DM 100,000 was imposed for further licenses and compensation for damages.

под закрилата на авторското право творба, и я разпространява чрез продажба. |[94]|

68. Днес Интернет играе определяща роля в незаконното разпространение на софтуер. Потребители, които имат достъп до *FTP* или *web servers*, създават скрити директории, за да колекционират или съхраняват огромни количества нелегални копия на комерсиален софтуер. Те употребяват всички видове средства за комуникация, като *e-mail* или *bulletin boards*, да разпространяват, използвайки секретни кодове, съобщения на опциите за даунлоудване. При това софтуерът обикновено се съхранява за кратко време, така че става почти невъзможно да се проследи пътят на разпространението му. |[95]|

69. Ролята на наказателноправната защита на интелектуалната собственост в различните държави еволюира по различен начин. Докато в правните системи с обичайно право много рядко се обръщат към наказателни санкции, в системите с цивилно право нарушенията на "копирайт"а се преследват с такива. Това се отнася поотделно за музикалното, видео и програмното пиратство, като в последните години разликите помежду им се премахват и се създават ефективни и еднородни наказателни механизми. |[96]| За разлика от гражданскоправните мерки, които се вземат по отношение нарушенията на "копирайт"а, в областта на наказателното право обаче все още съществуват значителни различия и е особено важно в преспектива да се извърши съгласуване по тези въпроси. |[97]|

LEGAL ASPECTS OFCOMPUTER-RELATED CRIME IN THE INFORMATION SOCIETY, prepared for the European Commission by prof. Dr. Ulrich Sieber, 1998

[89]|| Обхващането на "копирайт"а от наказателното право е практика в някои държави от 1981г насам. Реформи се правят в Италия – 1981г., Обединеното кралство – 1982г., Швеция и САЩ – 1982г., Финландия – 1984г., Германия и Франция – 1985г., Канада – 1987г., Унгария – 1992г.

LEGAL ASPECTS OFCOMPUTER-RELATED CRIME IN THE INFORMATION SOCIETY, prepared for the European Commission by prof. Dr. Ulrich Sieber, 1998

[90]|| Пак там.

[91]|| Пак там.

[92]|| Пак там.

[93]|| ИНТЕЛЕКТУАЛНАТА СОБСТВЕНОСТ, СОИС, 1988, 237-239.

[94]|| Пак там.

[95]|| LEGAL ASPECTS OFCOMPUTER-RELATED CRIME IN THE INFORMATION SOCIETY, prepared for the European Commission by prof. Dr. Ulrich Sieber, 1998.

[96]|| Пак там.

[97]|| GENERAL COPYRIGHT PROTECTION

§ 3. Икономически престъпления

70. Следващата вълна от реформи в законодателствата включва опитите да се предотвратят компютърно-относимите икономически престъпления, които набират ръст още през 80-те. За разлика от класическите престъпления те включват неосезаеми обекти (например компютърни програми и данни) или нови методи за извършване на

The protection of intellectual property in computer and communication systems is also influenced by various, more general initiatives in the field of copyright law.
European Community
In 1992 and 1993, especially the following Directives have been adopted:
Council Directive 92/100/EEC on rental and lending rights and certain rights relating to copyright;
Council Directive 93/83/EEC on copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission;
Council Directive 93/98/EEC on terms of protection of copyright.
Further initiatives of the Commission were described in the Green Paper on copyright and related rights in the information society published by the Commission in July 1995. Following the consultation process of this Green Paper, on 10 December 1997 the Commission adopted a proposal for a European Parliament and Council Directive on the harmonisation of certain aspects of copyright and related rights in the Information Society. The proposed Directive aims to harmonise reproduction rights, rights of communication to the public, and distribution rights as well as exceptions to the restricted acts. It also provides for obligations concerning technological measures and rights management information. As far as "sanctions and remedies" are concerned, Article 8 (1) of the Directive proposal requires that "Member States shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in this Directive and shall take all the measures necessary to ensure that those sanctions and remedies are applied. The sanctions thus provided for shall be effective, proportionate and dissuasive".
World Intellectual Property Organisation
In addition, there are various WIPO initiatives to up-date the copyright framework. Between 1993 and 1995, WIPO held a series of world-wide symposia and fora on the challenges of the new information technologies to copyright. In December 1996, the WIPO diplomatic conference on Certain Copyright and Neighbouring Rights Questions adopted the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT). The treaties contain provisions for copyright protection of copyrightable contents disseminated through global networks. The treaty obliges the contracting parties to provide legal remedies against the circumvention of technological measures (e.g. encryption) used by authors in connection with the exercise of their rights and against the removal of altering information, such as certain data that identify the work of their authors, necessary

престъпления (например въздействие върху машина, вместо върху човек). |[98]|

а) "Хакерство" - основен престъпен състав

71. Преди навлизането на компютрите достъпът до информацията се регулирал от институтите на секретността на

---

for the management of their rights.
GENERAL PRODUCT PIRACY
Further international initiatives of the Council of Europe, the European Union and the WTO do not specifically aim at computer-stored values, but protect them in a more general context.
Council of Europe
Based on the work of the Council of Europe's Steering Committee on the Mass Media, the Committee of Ministers of the Council of Europe adopted the "Recommendation on Measures to Combat Piracy in the Field of Copyright and Neighbouring Rights" in 1988. Among other aspects the recommendation declared that authors of computer software should benefit from copyright protection and suggested both civil and criminal remedies for infringements.
European Union
In the European Union, a similar approach was followed by the Council Regulation (EC) No. 3295/94 of 22 December 1994 laying down measures to prohibit the release for free circulation, export, re-export or entry for a suspensive procedure of counterfeit and pirated goods. The Regulation deals with
definitions especially with respect to counterfeit goods and pirated goods;
application for action by the custom authorities;
conditions governing action by the customs authorities and by the authorities competent to take a substantive decision;
provisions applicable to goods found to be counterfeit or pirated goods.
Article 11 of the Regulation requires that "each Member State shall introduce penalties to apply in the event of infringements of Article 2. Such penalties must be sufficiently severe to encourage compliance with the relevant provisions."
World Trade Organisation
Trade related aspects of intellectual property rights were especially dealt with by the World Trade Organisation (WTO). The mandate of the WTO includes the Agreement on Trade in Goods (especially GATT), the Agreement on Trade in Services (GATS) as well as the Agreement on Trade-related Aspects of Intellectual Property Rights (TRIPS). The TRIPS Agreement was negotiated in the context of the Uruguay Round in order to reduce distortions and impediments to international trade and to take into account the need to promote effective protection of intellectual property rights. It requires compliance with the substantive provisions of the Bern Convention for Protection of Literary and Artistic Works. With respect to new

кореспонденцията, секретността на телефонните комуникации и професионалната тайна. Днес обаче не може да се гарантира защита срещу незаконния достъп до съхраняваните в компютрите данни чрез традиционните наказателни норми. |[99]|

72. Терминът "**компютърно хакерство**" ("*computer hacking"*) традиционно се описва като проникване в компютърните системи не с цел манипулиране на данните, саботаж или шпионаж, а с цел постигане на удовлетворение от преодоляването на техническата защита. |[100]| Диференциацията е съществена - собственикът на

---

technologies, the agreement addresses the relevant copyright questions especially relating to computer programs and databases. Section 5 Article 61 of the TRIPS Agreement obliges Member States to provide criminal procedures. It states:
"Members shall provide for criminal procedures and penalties to be applied at least in cases of wilful trademark counterfeiting or copyright piracy on a commercial scale. Remedies available shall include imprisonment and/or monetary fines sufficient to provide a deterrent, consistently with the level of penalties applied for crimes of a corresponding gravity. In appropriate cases, remedies available shall also include the seizure, forfeiture and destruction of the infringing goods and of any materials and implements the predominant use of which has been in the commission of the offence. Members may provide for criminal procedures and penalties to be applied in other cases of infringement of intellectual property rights, in particular where they are committed wilfully and on a commercial scale."
LEGAL ASPECTS OFCOMPUTER-RELATED CRIME IN THE INFORMATION SOCIETY, prepared for the European Commission by prof. Dr. Ulrich Sieber, 1998.

[98]|| Laws against computer-related economic crime were enacted since 1978 in the United States of America (in state legislation) and in Italy, since 1979 in Australia (state law), 1981 in the United Kingdom, 1984 in the United States of America (federal level), 1985 in Canada and Denmark, 1986 in the Federal Republic of Germany and in Sweden, 1987 in Austria, Japan and Norway, 1988 in France and Greece, 1990 in Finland and the United Kingdom, 1992 in the Netherlands, 1993 in Luxembourg, 1994 in Switzerland, 1995 in Spain and again in Finland, and 1997 in Malaysia. In countries such as Denmark, the Federal Republic of Germany or Finland, the respective laws also included new provisions for trade secret protection. While some countries operate under the legal provisions enacted since the early 1980s, other countries such as, e.g., Canada are currently amending these provisions again to reflect new challenges to computer-related criminal law posed by the fast developing computer technology.
LEGAL ASPECTS OFCOMPUTER-RELATED CRIME IN THE INFORMATION SOCIETY, prepared for the European Commission by prof. Dr. Ulrich Sieber, 1998.

[99]|| Пак там.

[100]|| In a Dutch statistic of 1991, the cases of hacking amount to approximately one fifth of all computer crimes. Cf. Kaspersen, in: Sieber (ed.), Information Technology Crime, 1994, p. 347 (with explanations about the groups of crimes on p. 345). The twilight zone of hacking is very large, because the respective attempts

компютърната система не е увреден, а само застрашен. Значителни щети обаче са налице в случаите, когато престъпниците употребят получените по този начин знания за извършване на шпионаж, саботаж или измама. |[101]|

73. Техниката на хакването зависи до голяма степен от вида на комуникационните системи. "Традиционната" форма на хакването се развива през 80-те въз основа на използване на паролите за защита, които не се сменят често от компютърните потребители. |[102]|

74. Основният престъпен състав тук е познат като "неправомерен достъп". **Неправомерен достъп до компютърна система е налице, когато деянието е причинило унищожение, блокиране, изменение или копиране на информация, или нарушение на работата на изчислителната система.** |[103]|

75. Престъпното деяние се състои в неправомерен достъп до охранявана информация чрез проникване в компютърна система по пътя на използването на специални технически или програмни средства, на действащи пароли или маскировка като законен ползвател, позволяващи успешно да се преодолее системата за защита при условие, че са били приети такива мерки за защита, ако това деяние води до унищожаване, промяна или блокиране на информацията. За неправомерен се счита достъпът до защитена информация от лице, не притежаващо права за получаване или работа с дадената информация или компютърната система. |[104]|

---

of getting access often cannot be registered and traced back.

[101]|| One of the most severe cases of sophisticated "hacking" involved a group of German teenagers in the late 1980s. They had managed to get access to various American computer systems and then sold the knowledge obtained in their data journeys to the former Soviet secret service KGB. The case was discovered because one of the hackers sought help at the author's former Bayreuth chair, leading to a deal with the prosecution authorities: The hacker revealed his knowledge and the investigation against him was turned down. The case was of particular interest because information on new techniques of computer manipulation were revealed in the course of this proceeding.
LEGAL ASPECTS OFCOMPUTER-RELATED CRIME IN THE INFORMATION SOCIETY, prepared for the European Commission by prof. Dr. Ulrich Sieber, 1998.

[102]|| Пак там.

[103]|| Пак там.

[104]|| Състави на компютърни престъпления в руското законодателство са отразени в 28 главе УК, която е озаглавена "Преступления в сфере компьютерной информации" и съдържа три текста: "Неправомерный доступ к компьютерной информации" – "Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в

76. Неправомерният достъп до компютърната система трябва да е бил осъществен умишлено. Извършвайки това престъпление, лицето трябва да съзнава, че неправомерно влиза (използва) в компютърната система, да предвижда възможността или неизбежността от настъпването на указаните в закона последствия, желае и съзнателно ги допуска, или се отнася към тях безразлично. |[105]|

77. Мотивите и целите за това престъпление могат да бъдат различни. Това може да бъде користен мотив цел да се получи някаква информация, желание да се причинят вреди, желание да се проверят собствените професионални способности. Мотивите и целта обаче не са включени като съществен елемент от състава на престъплението.|[106]|

78. Хипотезата на неправомерния достъп е конкретизирана в британския *Computer Misuse Act 1990* по следния начин: лицето извършва престъпление, когато: 1) осъществява достъп до компютър, 2) достъпът е неоторизиран, и 3) лицето знае, че достъпът е неоторизиран. |[107]|

79. Тези три елемента трябва да са дадени в **кумулация.**

- За да е налице престъпление, се изисква повече от осъществяване единствено на достъп до хардуера; необходимо е още да се накара компютърът да извърши определени функции. Такива могат да бъдат например актовете на изменяне или изтриване на програма или данни, както и резултатът да бъде показан или по друг

электронно - вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети." (ст. 272); "Создание, использование и распространение вредоносных программ для ЭВМ" - "Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами." (ст. 273), и "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети" - "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред." (ст. 274).

[105]|| LEGAL ASPECTS OFCOMPUTER-RELATED CRIME IN THE INFORMATION SOCIETY, prepared for the European Commission by prof. Dr. Ulrich Sieber, 1998.

[106]|| Пак там.

[107]|| COMPUTER LAW, Chris Reed, 1992.

начин изведен на изхода на компютъра. |[108]| Не се изисква извършителят на престъплението да осъществява достъп до точно определен компютър. Обикновено хакерът случайно попада на адрес на една или друга своя жертва. Следователно първото условие за наличието на престъпление ще бъде налице, ако неговите усилия за осъществяване на достъпа са реализирани, дори той да няма представа за идентичността на компютъра – жертва. |[109]|

- Вторият елемент от фактическия състав на престъплението изисква достъпът да е неоторизиран. Такъв е налице, когато достъпът не е одобрен от лицето, което има правото да го контролира. На въпроса дали достъпът е оторизиран или не, трябва да се отговаря при всеки отделен случай. Операторът на *bulletin board* например може да позволи на всеки да разглежда определена информация, обаче може да запази друга такава за по-ограничен кръг потребители. |[110]|
- Накрая, за да има престъпление, е необходимо потребителят да е наясно с това, че достъпът е неоторизиран. Само умишлени деяния са наказуеми според наказателното право. Тук съществува една особеност: ако при работа с компютърна система потребителят бива питан за идентификационен код, от това той би трябвало да направи извода, че достъпът е нежелан. Трудно е обаче да се установи *metis rea* в случай, в който един оператор на компютърна система не взима мерки за индициране за неоторизираните потребители, че техният опит за достъп не е желан. Друг пример може да се даде за случай, в който потребител А получава легално парола за достъп от собственика на компютъра. А обаче разкрива своята парола на Б и съдейства на Б да употреби паролата, за да придобие достъп до този компютър. В този случай достъпът на Б до компютъра ще бъде неоторизиран; въпреки че А е упълномощен с достъп до компютъра; той не е упълномощен да "контролира" достъпа и в този смисъл не може да прехвърля права на трета страна. |[111]|

(последващите глави - в книгата)

---

[108]|| Пак там.

[109]|| Пак там.

[110]|| Пак там.

[111]|| Пак там.

Част пета

КОМПЮТЪРНО ПРАВО - ИЗВОДИ

Особености на компютърното право.

80. Явленията в областта на информационните технологии са качествено различни от явленията в другите области на технологията. |[112]| Днес под "информационни технологии" се разбират и компютърните технологии, но се обхващат и начините, по които информацията се предава - посредством телекомуникации и радиопредаване. Т.е. сходният термин "информационно право" е твърде широк. Поради тази причина се явява нуждата да се обособи ново правно направление, което да отграничи материята в тази област, и което понастоящем носи наименованието **компютърно право** (***computer law***).

81. Основните особености, които отличават компютърното право от други направления в правото, включват неговия предмет, обект и съпътстващите ги правоотношения.

82. **Предметът на компютърното право** е във връзка с обекта на правно регулиране. Предмет на компютърното право са обществените отношения, появяващи и развиващи се във връзка с компютъра като обект на правно регулиране. В тази връзка може да се даде следното примерно определение за компютърно право: **компютърното право е направление в правото, имащо за предмет регулирането на обществените отношения във връзка със създаването и използването компютърните системи, както и закрилата на правата върху тях.**

83. **Обектът на компютърното право** е точно определен - **компютър** (или **компютърна система**). Тази особеност е може би най-съществената отлика на компютърното право от другите правни направления. За разлика от останалите правни области, които разглеждат сложни съвкупности от родове и видове обекти, компютърното право се занимава с един единствен обект – **компютъра**. Тази тясна специализация му дава принципната

---

[112]|| COMPUTER LAW, Chris Reed, 1992.

възможност да обхване в пълнота всички обществени отношения, свързани със създаването и употребата на компютърните продукти.

84. Предвид спецификата на **правоотношенията**, които чертаят мястото на компютъра като обект на правото, могат да се отграничат три основни области на приложение на правните норми: **1) Правни норми, регулиращи процесите по създаването на компютърните продукти.** Създаването на компютърните продукти е творчески процес, резултатите от който следва да бъдат защитени от специфични правни материи. Такива сега се явяват патентноправната и авторскоправната материя; **2) Правни норми, регулиращи правоотношенията във връзка със законосъобразната употреба на компютърните продукти.** В областта на законосъобразната употреба на компютърните продукти правоотношенията се регулират по правилата на онези нормативни актове от националното и международното право, които регламентират всички отношения, свързани с употребата на сходни продукти. Например в областта на облигационното право компютърът се третира като обект на покупко-продажба, в областта на вещното право той се явява движима вещ, и т.н. **3) Правни норми, регулиращи правоотношенията, създавани във връзка с нарушенията и престъпните посегателства върху компютърните продукти**. Тук приоритет следва да се даде на онези правни норми, които имат задача да регулират всички правоотношения, свързани с нарушенията и престъпните посегателства върху компютърните продукти и правата върху тях. Те могат да бъдат от гражданскоправен, административноправен или наказателноправен характер.

85. Въз основа на горното може да се извлекат някои от по-характерните особености на компютърното право, които да бъдат систематизирани в следната последователност:

- **Компютърното право е ново направление в правото**. Неговото появяване е следствие от развитието на компютъра като техническо устройство. История - кратка, а практиката, свързана с регулирането на обществените отношения в тази област – не особено богата. Това обаче не е недостатък, а предимство – компютърът е революционен технологичен феномен, което е гаранция за прогресивното развитие на този клон от правото.
- **Компютърното право е последица от развитието на научно-техническия прогрес**. За разлика от традиционните правни направления, които градят своите институти в продължение на дълги исторически периоди и остават относително непроменени също дълго време, което дава основание да се говори за т. нар. “консервативност”

на правото, компютърното право е следствие на научно-техническия прогрес и има задача да съдейства за най-добра правна обезпеченост на този прогрес.

▪ **Компютърното право е сложно, съставно право – то включва институти от различни правни отрасли.** Спецификата на неговия обект изисква то да заимства отделни правни институти от авторското и изобретателско право, административното право, гражданското право, търговското право, облигационното право, наказателното право, международното право. Тенденцията да разширява своето поле на действие предполага още по-силното му проникване в тези, а и други правни области.

86. Към момента компютърното право не е кодифицирано, няма собствена "територия" и включва материя от разнородни правни области. Компютърното право обаче е ново направление в правото и законодателната власт би трябвало да провъзгласи система от норми, имащи "компютърен" статут – кодекс, закон, съвкупност от отделни законови текстове, или подобни. |[113]|

Отграничения от сходни правни направления.

87. Компютърното право регулира обществени отношения в областта на информационите технологии. Но то не е единственото направление, което решава тези задачи. Със сравнително развита нормативна уредба са някои нови направления в правото, намиращи се в тясна връзка с компютърното право: т. нар. интернет-право и кибер-право. |[114]| Затова се налага да се направят необходимите отграничения.

88. Под "**Интернет**" се разбира глобална (в световен мащаб) мрежа от неопределен брой свързани помежду си компютри. "Интернет-мрежата представлява глобално обединение на компютърни мрежи и информационни ресурси, принадлежащи на множество хора и организации. Това обединение е децентрализирано, и единни общозадължителни правила (закони) не са устновени. Съществуват обаче общоприети норми за работа в Интернет, насочени към това, щото действията на всеки ползвател на мрежата да не пречат на действията на другите ползватели. Правилата за използване на които и да са ресурси в Интернет (от пощенската кутия до канала за свръзка) се определят от владелците на тези ресурси и само те." |[115]|

---

[113]|| LEGAL PROBLEMS OF NANOTECHNOLOGY Frederick A. Fiedler & Glenn H. Reynolds,: An Overview, Southern California Interdisciplinary Law Journal, 1994.

[114]|| INTELLECTUAL PROPERTY RIGHTS SYMPOSIUM PANEL DISCUSSION, Q. TODD DICKINSON, Tokyo, Japan November 16, 1999.

89. "Компютърна мрежа" е свързани помежду си два или повече компютъра или компютърни системи чрез сателити, кабелни линии или друга комуникационна среда със способност тя да бъде проводник на информация между компютрите. |[116]| Подобна компютърна мрежа се нарича *network* - система от свързани помежду си компютърни системи и терминали. |[117]|

90. В зависимост от задачите, които решават, комуникационните мрежи могат да имат **локален** характер. Компютрите могат да бъдат свързани посредством **локална мрежа** (*LAN*) – чрез нея се осъществява обмен на данни между ограничен брой компютри, обикновено в рамките на едно учреждение. "Интранет" е пример за подобна система – свързани помежду си компютри в локална мрежа с цел между тях да се осъществява комуникация. Отличава се от Интернет с ограниченията, наложени върху всеобхватността на връзките и броя на компютрите, обхванати от нея. От своя страна *LAN*-мрежите могат да бъдат свързани в глобална мрежа (*GAN*), |[118]| и да имат **глобален** характер. Последните са известни като **световната информационна мрежа - Интернет**. |[119]|

---

[115]|| ПРАВО И ИНТЕРНЕТ: ОЧЕРКИ ТЕОРИИ И ПРАКТИКИ, В. Б. Наумов, Москва, 2002.

[116]|| TEXAS PENAL CODE, TITLE 7. OFFENSES AGAINST PROPERTY, CHAPTER 33. COMPUTER CRIMES, 33.01.

[117]|| 47 U.S.C. 553. SEARCHING AND SEIZING COMPUTERS, Scott C. Charney, Chief, Martha J. Stansell-Gamm, Computer Search and Seizure Working Group, General Litigation and Legal Advice Section Criminal Division Department of Justice, JULY 1994, FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS.

[118]|| Пак там.

[119]|| За мнозинството изследователи началото на компютърните мрежи се слага на 2 септември 1969 г., когато в лабораторията на Лен Клайнрок в университета на Калифорния, Лос Анжелис (*UCLA*), са свързани с кабел два компютъра. Първоизточник на идеята е агенцията *ARPA* (*Advanse Research Projects Agency*) към министерството на отбраната на САЩ. Постепенно техниката се усъвършенства и през 1972 г. се появява първото полулярно приложение на мрежата - електронната поща.

В най-ранните дни от развитието на Интернет, като се започне приблизително от 1973 г., активността в това направление се дължи на изследователска програма, спонсорирана от *ARPA*. *ARPANET* била принципната основа на системата, използвана от университетски изследователски групи и различни индустриални изследователски организации. В 1975 г. *ARPA* превръща *ARPANET* в Отбранителна комуникационна аагенция (*Defense Communications Agency to operate*.)

91. С оглед **разграничението между компютърното право и интернет-правото и особено кибер-правото** може да се каже, че комуникациите межу компютрите, макар че са зависими от компютърните системи, самите те не са условия за съществуването на последните. |[120]| Компютрите са самостоятелни и независими устройства. Комуникацията между тях е допълнителна функция, която те притежават. Самите комуникации, разглеждани като средства за обмен на информация, до голяма степен също са възможни без употребата на компютри (например телефонните, спътниковите, кабелните, радио и телевизионните комуникации). **Предмет на настоящата работа са изключително правоотношенията, свързани с компютрите като устройства сами по себе си.**

(ПРОДЪЛЖЕНИЕТО - В КНИГАТА)

Системата се употребявала единствено за изследвания и за отбранителни цели. След 1981г. и други агенции са заинтересовани от употребата на *ARPANET*. *NATIONAL SCIENCE FOUNDATION* (*NSF*) слага началото на *COMPUTER SCIENCE NETWORK* (*CSNET*), която използва *TCP/IP*, за да свърже университетите чрез ARPANET, както и чрез телефонната система *PHONENET* (за е-майл). В 1986 г. *NSF* използва своята *NSFNET*, за да свърже суперкомпютърни центрове към *ИНТЕРНЕТ*. От 1988 г. насам *ИНТЕРНЕТ* се превръща в политика, сложена от изследователските агенции и университети по целия свят.

В 1988 г. *US Federal Networking Council* предлага да се свържат *MCI Mail* с Интернет. Това променя основно политиката на употреба на *ИНТЕРНЕТ* за комерсиални цели. През 1990 г. *ARPANET* е оставена и *NSFNET* поема задължението на основна опора на глобалната информационна мрежа. В началото на третото хилядолетие *ИНТЕРНЕТ* става първа стъпка към глобална информационна структура и виждането за нейното приложение и прана защита се нуждае от по-нататъшно развитие.

[120]|| Пример може да се даде с процеса срещу фирмата *Microsoft*, относим към вграждането на програмата *INTERNET EXPLORER* в операционната система *WINDOWS*. Съдът приема, че е налице вместване в управляващата хардуера програма на едно "приложение", което няма съществено значение за работоспособността на компютърната система.