UDK — 343.3/.7:007
Изворни научни рад

др Ђорђе Игњатовић,
доцент Правног факултета у Београду

ПОЈМОВНО ОДРЕЂЕЊЕ КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА

Тањуг је априла 1983. како, помало злурадо, пише Klaus Tiedemann – не без поноса што се то коначно догодило и нама – свету јавио да су тројица запослених у Истарској банци, у Пули, извршила кривично дело тако што су компјутерском манипулацијом пренели са рачуна штедиша на свој конто милион динара. Сличне појаве забележене су и касније, чак и ових дана, но таква дела нису наишла на посебан интерес, сем у штампи. Игнорисање од стране законодавства и кривично правне теорије може се објаснити њиховим схватањем да систем инкриминација код нас (откуда тај утисак, насупрот искуству многих других земаља?) у потпуности покрива оваква понашања и прописује одговарајуће санкције. Ћутање других кривичних наука теже је разумети. Отуда се овај рад појављује као један од првих покушаја да се у југословенској криминолошкој теорији дефинише по многим цртама особен тип делинквенције – компјутерски криминалитет.

Кључне речи: *Компјутери. – Компјутерски криминалитет. – Злоупотреба компјутера. – Компјутерска превара. – Информатички криминалитет.*

А) УВОД

Тешко је у историји пронаћи пример да је један проналазак у техници у тој мери променио живот човека као што је то случај са средствима за електронску обраду података – компјутерима. Почетак њихове примене у сфери производње често се означава као „трећа индустријска револуција", а окружење које су створили неким ауторима се чини довољним да говоре о рађању тзв. „информатичког, компјутерског друштва".

Скоро да нема области у којој ова моћна средства нису нашла примену. У пословању и индустрији, образовању, здравству, научним истраживањима, чак и у уметности[1]. Свакодневица огромног дела човечанства данас скоро да се и не може замислити без рачунара. Њихова примена учинила је живот лагоднијим, али има и своју другу страну – цивилизација је постала рањивија у свим оним ситуацијама када ове моћне машине откажу. Савремена друштва, и поред свести о постојању тог ризика, нису их се могла одрећи. Због тога се посебни напори усмеравају како би се њихове штетне последице умањиле.

(1) B. Stern N. and R.: *Computers and Society*, Englewood Cliffs, 1983.

Б) КОМПЈУТЕРИ И КРИМИНАЛИТЕТ

Као и у другим областима, и у процесу стварања и примене права, компјутерска техника нашла је своју примену[2]. Примери за то могу се наћи у свим областима права, али ће нас у овом раду пре свега интересовати специфична релација која се може успоставити између криминалитета и примене компјутерских средстава.

Могућности примене рачунарске технике у спречавању и сузбијању криминалитета сваким даном се умножавају. Неслућене могућности ових машина да приме и сачувају огромну масу података и да их обраде у кратком времену, уз касније изванредно брзо претраживање и довођење у корелацију[3], дају криминалистици данас сваким даном све веће могућности у откривању кривичних дела и њихових учинилаца. Такође, аутоматска обрада података нашла је у нашем времену примену и у казненој политици кроз стварање правосудних информационих система, као и у пенитенцијарној пракси за одређивање и евалуацију ресоцијализационих третмана. И поред несумњивог значаја поменутог, пажњу ћемо у овом раду ипак задржати само на специфичном аспекту односа између компјутера и криминалитета – на оним делима чије је извршење у вези са применом електронских рачунара.

Та појава у науци означава се различитим терминима. Неки аутори је називају „злоупотребом компјутера" *(computer abuse)* други „компјутерском преваром"*(computer fraud)*, „деликтима уз помоћ компјутера *(crime bu computer)* и криминалитетом кроз аутоматску или електронску обраду података (АОП одн. ЕОП), а говори се и о „информатичком" одн. „технокриминалитету"[4]. Ми ћемо усвојити термин „компјутерски криминалитет" не само зато што је у литератури доминантно заступљен, већ пре свега због тога што у потпуности одговара оном приступу појави који нам се чини најбољим – криминолошком.

ц) ДЕФИНИЦИЈЕ И КЛАСИФИКАЦИЈА КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА

Компјутерски криминалитет је вишезначан феномен. Отуда он не оставља исту слику када га посматрамо из различитих углова. Учиниоци, стварне и потенцијалне жртве, истражни органи, тужиоци, компјутерски техничари, криминолози, психолози и социолози, немају о њему исто становиште[5]. И поред тога нужно је дати општу дефиницију ове појаве која би требало да тежи синтези тих концептуалних полазишта.

Одређењу компјутерског криминалитета аутори приступају на два начина. Једни се јасно опредељују и дају његову дефиницију, док се други о овом питању изјашњавају посредно – наводећи која понашања у овај вид делинквенције спадају.

---

(2) Овој проблематици посвећен је посебан број часописа Анали Правног факултета у Београду 1989/2–3.

(3) В. материјале са Међународне конференције *New Horizons in International Crimial Law*, Noto, Italia, May, 1984. објављене у публикацији Association Internationale de Droit Penal, Bordeaux, 1985. с. 117.

(4) Swanson C.R. and Territo L.: *Computer Crime: Dimensions, Types Causes and Investigation*, Journal of Police Science and Administration 1980/3 с. 304–311. и Bequi A: *Technocrimes. The computerization of crime and terrorism*, Lexington, 1987.

(5) Parker D., *Crime by computer*, New York, 1976. s. 13

Пре него што ова гледишта изложимо, потребно је да, бар у најкраћим цртама, укажемо на промене у појавним облицима криминалитета повезаног са компјутерима. Од времана шездесетих година, када су у штампи објављени први случајеви манипулација рачунарима од стране запослених у финансијским установама, преко зачетака криминолошких истраживања у седамдесетим, која су га углавном сводила на вид „криминалитета белог оковратника" и обухватања нових облика угрожавања приватности човека и пиратског умножавања рачунарских програма у осамдесетим годинама, све до најновијих схватања по којима овај вид криминалитета обухвата и нове појаве као што су „хакирање (*hacking*)", „вируси и црви (*viruses and worms*) и „стоно кривотворење (*desktop forgery*)" – ове измене конкретних облика имале су, како ћемо то из приказа који следи видети непосредног утицаја на покушаје појмовног одређења ове појаве.

Пођи ћемо од дефиниције компјутерског криминалитета које су дали несумњиво највећи познаваоци ове материје. У свом раду из 1973. *Donn B. Parker* дефинише „злоупотребу компјутера" као: „сваки догађај у вези са употребом компјутерске технологије у коме жртва трпи или би могла да трпи губитак, а учинилац делује у намери да себи прибави или би могао да прибави корист. Сваки такав случај може бити означен као злоупотреба компјутера ако садржи информације које могу бити коришћене у даљем проучавању тих појава, а циљ тог изучавања је да се убудуће рачунари учине безбеднијим[6].

Други пионир у овој области, такође Американац *August Bequai* дефинише компјутерски криминалитет као „вршење кривичних дела код којих се рачунар појављује као оруђе или као објект заштите" одн. „употреба рачунара при вршењу преваре, утаје и злоупотребе, чији је циљ присвајање новца или услуге, и у вршењу политичке или пословне манипулације, укључујући и радње уперене против самог рачунара[7].

У једном приручнику издатом од америчког Секретаријата за правосуђе, срећемо неколико дефиниција овог вида криминалитета. Он се одређује као „вршење забрањеног дела помоћу рачунара", „облик криминалитета белог оковратника, при чијем се вршењу користе рачунарски системи" и „употреба рачунара при вршењу кривичних дела"[8].

Познати немачки стручњак за ову област *Urlich Sieber* дефинисао је 1977. компјутерски криминалитет као „противправне повреде имовине код којих се рачунарски подаци с предумишљајем мењају (манипулације рачунаром), разарају (рачунарска саботажа), до њих се неовлашћено долази и користи (рачунарска шпијунажа) или се користе заједно са хардвером (крађа времена)"[9]. У свом најновијем раду, овај аутор усваја другу дефиницију по којој у овај вид криминалитета спада „свако противправно, неетичко или недозвољено понашање које је у вези с аутоматском обрадом података и/или преносом података". Он сматра да ширина ове дефиниције дозвољава употребу разних хипотеза за све врсте криминолошких, криминалистичких, економских, превентивних или правних студија, при чему сваки од ових приступа има одређено поље примене.

---

(6) Parker D., Nycum S. and Oura S.: *Computer abuse*, Sprinfield, 1973.

(7) Bewuai A.: *Computer crime*, Lexington, 1978. s. 4.

(8) *Computer Crime, Criminal Justice Resource Manual, National Criminal Justice* Information and Statustics Service LEAA, U.S. Depariment of Justice, Washington, 1979, s.4—5.

(9) Sieber U.: *Computerkriminalitat und Strafrecht*, Köln 1977. и Goldmann G.: *Computer — Kriminalitat und ihre Bekmpfung*, Kriminalistik,1989/8—9 s. 445.

Као најплодотворнију поделу компјутерског криминалитета, он издваја ону која, заснована на криминолошком и правном критеријуму, разликује: имовинска кривична дела, повреду права на приватност и угрожавање осталих правно заштићених интереса која су извршена употребом компјутера[10].

Један други немачки аутор, *Klaus Tiedeman*, под криминалитетом извршеним уз помоћ компјутера подразумева „сва противправна или друштвено штетна понашања која су у бити одређена употребом средстава за електронску обраду података, без обзира да ли се она користе као средство извршења или објект напада[11]. На првом месту ради се о нападима на сферу резервисану за приватност појединца, а затим о повредама имовине проузрокованим коришћењем средстава за аутоматску обраду података.

На плану казуистике, *Tiedeman* сматра да је (када се изоставе случајеви коришћења компјутера при вршењу „обичних" имовинских кривичних дела – као фалсификовање биланса или порески деликти) могуће разликовати четири групе криминалних радњи: а) манипулације *input — output*. Ради се о уношењу, обради и давању лажних података; б) индустријска шпијунажа у области рачунарства („информатичка шпијунажа"); ц) случајеви саботаже у области компјутера, који су интересантни како због проузроковане штете, тако и због начина извршења; д) такозвана „крађа компјутерског времена" – недозвољено коришћење рачунарских система и мрежа, од непоузданих сарадника или лица са стране. Најзад, као специфичан вид са компјутерима повезаног имовинског криминалитета (конкретно „компјутерске преваре"), аутор истиче злоупотребу шалтера за подизање готовог новца[12].

Неки писци сматрају да при дефинисању компјутерског криминалитета треба сићи на практични терен; – по њима, треба испитати, да ли би дело уопште могло бити проузроковано, као и да ли би по интензитету и ширини било подведено под наведени појам, да компјутер није коришћен при извршењу[13].

Италијански аутор Carlo Sarzana у компјутерски криминалитет сврстава „свако криминално понашање у које је рачунар умешан или као материјално средство извршења или као објект криминалне активности или као симболичко средство". Код овог последњег, реч је о злоупотреби погрешног

---

(10) У исто време, он критикује традиционално схватање о компјутерском криминалитету као искључиво имовинском деликту које ја заступао раније –Sieber U.: *General report on „Computer crime"* — The emergence of Criminal Information Law, International Academy of Comparative Law, XIII th International Congress, Montreal, 1990.

(11) Tiedemann K.: *Phénoménologie des ifractions économiques* u Aspects criminologiques de la délinquance d'affaires. Strasbourg, 1978. c. 231.

(12) Tiedemann K.: *Criminalita da computer u Trattato di criminologia*, medicina criminologica e prichiatria forense a cura di Ferracuti F. vol. X, Milano, 1988. s. 16—19.; Carsten P. and Trichardt A: *Computer crime by means of the Automated Teller Machine — just another face of fraud?* South African Journal of Criminal Law and Criminology 1987/2 s. 122— 134.

(13) Leibholz — Wilson: *User's Guide to Computer Crime*, Radnor, Pensylvania, 1974. c. 14. Интересантно је да је захтеву практичне примењивости приближила и дефиниција коју је дао E. Bunge (Kriminalistik 1987/2), по коме компјутерски криминалитет обухвата „сва чињенична стања код којих је електронски рачунар средство извршења и (или) објекат дела, а основана је сумња да постоји неко кривично дело. „Немачка полиција користи ову дефиницију у свакодневном поступању –в. Водинелић В: *Методика откривања, доказивања и разјашњавања рачунарског криминалитета*, Приручник 1990/4 с. 323–338

верована жртве у непогрешивост ових средстава, што делинквенту даје психолошку предност и олакшава преварну радњу[14].

У нашој, иначе изузетно оскудној литератури, дате су следеће дефиниције криминалитета у вези са компјутерима: „Кривична дела код којих се криминалитет појављује као средство (оруђе), предмет или објекат напада, за чије је извршење или покушај неопходно извесно знање из рачунарства или информатике"[15] и „злоупотребе у коришћењу рачунара и извршење различитих претњи и недозвољених радњи у раду рачунара[16].

Како је то већ поменуто, у низу радова садржај појма компјутерски криминалитет одређен је на један индиректан начин – набрајањем конкретних облика у којима се овај вид друштвено опасног понашања појављује. Навешћемо неке примере. Тако је у Криминолошком речнику[17] за компјутерски криминалитет наведено да обухвата: 1) крађу одн. одузимање делова централне јединице или периферних уређаја; 2) уништење или оштећење (из пакости, ината или освете) система; 3) уношење лажних података како би се олакшала превара (мењањем програма одн. датотека) и 4) коришћење информација из рачунарских база података у криминалне сврхе (крађа, уцена).

M. Leepson[18] само наводи да у ову категорију спадају: саботаже и вандализам запослених, електронска крађа, превара и проневера, а законодавне комисије Шкотске, Енглеске и Велса, на основу Извештаја о компјутерском криминалитету, израдиле су радни документ у коме сва дела из ове области разврставају у пет група: 1) компјутерска превара, 2) надозвољено коришћење рачунарских података (продирање „хакера", компјутерско прислушкивање, недозвољена употреба рачунара у личну корист), 3) недозвољена промена или деструкција меморисаних података, 4) одбијање приступа овлашћеном кориснику и 5) недозвољено уклањање таквих података[19].

Италијански аутор *F.Mucciarelli*[20] сматра да у „информатички криминалитет" треба убројити: понашања којима се коришћењем рачунара угрожава приватност појединца, имовинске деликте извршене на исти начин, и дела код којих се рачунарски систем појављује као објекат напада.

У нашој литератури В.Водинелић[21] прави разлику између „рачунарског криминалитета" у ужем (рачунарска превара, саботажа и шпијунажа) и у ширем – неправом смислу (сва остала дела). Компјутерски криминалитет одређују набрајањем дела која ту спадају и М. Папрић[22] и Д.Басић[23].

И поред начелне (само условно и научне) прихватљивости оваквог казуистичког приступа, сматрамо га мање погодним од оног код кога се чини

---

(14) Sarzana K.: *Criminalita e technolia: il caso dei „Computer — crimes"*, Rassegna pentitenziaria e criminologica, 1979/1–2 c. 53–89.

(15) Brvar B.: *Pojavne oblike zlorabe računalnika*, Revija za kriminalistiko in kriminologijo 1982/2 c. 92 – 104.

(16) Цикота Д.: *Заштита података информационих система посебно са становишта овлашћења у коришћењу података*, Безбедност, 1988/3 с. 229–241.

(17) *A Dictionary of Criminology*, ed, by Walsh and Poole A., London, 1983. c. 43.

(18) *Op. cit.* c. 91–95.

(19) Wisik D.: *Law reform proposals in computer crime*, Criminal Law Review, April 1989. s. 257—270.

(20) *I computer — crimes nel disegno di lagge* 1657/188984, Ravista italiana di diritto e orocedura pénale 1985/3 s. 785—791)

(21) *Op. cit.*

(22) *Употреба компјутера и криминалитет*, Приручник, 1984/6 с. 593–597.

(23) *Нешто више о компјутерском криминалу и тероризму*, Југословенско банкарство, 1988/12 с.50–53.

напор да се ова појава јасно дефинише. Због тога ћемо на крају овог одељка указати на дефиницију компјутерског криминалитета која би прецизно, али и на општи начин, одредила овај појам. Дакле, она би требало да буде и довољно одређена како бисмо у пракси могли поуздано знати када се суочавамо са овим видом криминалитета, али и тако широка да може покрити и евентуална нова друштвено опасна понашања у овој области. Да бисмо до ње дошли непходно је критички размотрити решења наведена у литератури.

Пре свега, будући да се ради о типу криминалитета, све оне дефиниције које у категорију сврставају и сва „неетичка, недозвољена и друштвено опасна" понашања у вези са компјутерима требало би сматрати прешироким. Уколико се ради о криминалитету, ту могу спадати само оне радње које су и иначе кажњиве према одредбама кривичног права (овде по страни остављамо питање да ли норме ове гране права на прави начин санкционишу оваква понашања)[24]. Ако и постоје дела из ове области која носе посебан степен опасности, а ни широким тумачењем кривично-правних норми не потпадају под постојеће инкриминације, то може бити само сигнал законодавцу да приступи инкриминацији таквих радњи.

Даље, ни сва дела која су покривена инкриминацијама, а у вези су са рачунарима, не могу се подвести под појам компјутерског криминалитета. Као особен вид делинквенције, овај облик људског деловања мора на специфичан начин бити повезан са системима за електронску обраду података и то тако да му њихова употреба, својства ових технолошких средстава и црте самих учинилаца дају за право да се издвоји као особена врста антидруштвене делатности у криминолошком смислу. Тиме би се отклонили приговори, који долазе најчешће од лаика да би се, следећи логику најширег приступа дефиницији овог вида делинквенције, могли издвојити и други облици повезани са новим технолошким средствима као што су „телефонски" или „криминалитет телекомуникација".

Када се анализирају у раду наведене дефиниције, јасно је да у литератури доминира овакав приступ. У већини радова, наведени су додатни услови да би се једно кривично дело повезано са рачунарима могло подвести под појам компјутерског криминалитета. Отуда би те услове требало размотрити и определити се у којој мери они одговарају стварању адекватне (у неведеном смислу) дефиниције.

Тако, захтев да проучавање оваквих дела има практичну корист за изградњу поузданијег обезбеђења компјутерских система, на чему инсистира Паркер, представља по нашем мишљењу уношење у дефиницију елемента који се подразумева. Истина, он говори о „злоупотреби компјутера", а не о криминалитету. Уколико је реч о овом другом, треба подсетити на основни криминално политички постулат по коме свако криминолошко проучавање недозвољених активности има само један крајњи циљ – да нам пружи знања која ће нам помоћи у спречавању и сузбијању оваквих појава. Због тога се уношење овог практичног елемента у дефиницију чини сувишним.

Захтев који се истиче у нашој литератури – да учинилац поседује одређено знање из рачунарства или информатике одн. свест о начину рада, могућностима и конкретној намени компјутерских система, је логичан и неспоран, али је дискутабилно да ли је неопходно да буде садржан у самој дефиницији овог вида криминалитета. Како се ради о кривичним делима, по

---

(24) В.детаљније Tiedemann K.: *Criminalita da computer*, Milano, *op. cit.* s. 1., Leepson M.: *op cit*, с. 90—91. и Backer W.R.: *Crimes with no laws: Telecomunications & computer crime*, Police Chief 1988/5 s. 44—45.

нашем мишљењу, наведени захтев већ је садржан у свести о самом делу као једном од услова кривичне одговорности.

У погледу мишљења да рачунар може бити и „симболично средство" извршења оваквих дела (за ово се залаже *C. Sarzena*), такође се може рећи да уношење овог елемента у појам компјутерског криминалитета представља усложавање овог појма за које би се тешко могло наћи оправдање. „Херојско доба" информатике, у коме су грађани беспоговорно веровали у тачност свега што је резултат рада рачунара, углавном је прошло. Њихово свакодневно искуство је, напротив да (како се то обично каже) „ и компјутер може да погреши", због чега је могућност манипулације позивањем на ауторитет модерне технологије све мања.

Најзад, из свих наведених разлога, чини нам се прихватљивом следећа дефиниција: *компјутерски криминалитет представља посебан вид инкриминисаних понашања код којих се рачунарски систем (схваћен као јединство хардвера и софтвера) појављује или као средство извршења, или као објекат кривичног дела, уколико се дело на други начин, или према другом објекту, уопште не би могло извршити или би оно имало битно другачије карактеристике*[25].

Ово би била дефиниција компјутерског криминалитета у ужем, правом смислу. У ширем значењу, он би се могао означити као: *вршење било ког кривичног дела повезаног са употребом или функционисањем рачунара.*

Криминалистичка феноменологија бави се проучавањем овог типа криминалитета у оба ова значења, али би пратила и друга понашања која представљају противправну, или чак само друштвено штетну манипулацију средствима за аутоматску обраду података, зато што нека од њих имају непосредне везе са криминалитетом или због могућности да, услед своје посебне друштвене опасности, процесом инкриминације касније буду уврштена у круг понашања која подлежу кривично-правној репресији.

Д) ЗАКЉУЧАК

Компјутерски криминалитет представља особену врсту криминалне активности која у наше време због својих битних карактеристика – степена друштвене опасности, средстава извршења дела, објеката заштите, карактеристика учинилаца и тежине последица – захтева посебан приступ. Лажна слика о изузетном карактеру оваквих понашања не даје нам за право да игноришемо појаве за чије истраживање не поседујемо још одговарајућу методологију. Да бисмо указали на реалне димензије ове појаве навешћемо само речи једног од највећих ауторитета у овој области *Bequi-a* да је „шанса за откривање дела из ове области и у најразвијенијим земљама", (уз постојање специјализованих агенција које се искључиво тиме баве) „само један према сто, а да учинилац буде кажњен – још пет пута мања". Он констатује да је данашњи правни систем већине држава немоћан да се на одговарајући начин супротстави оваквим понашањима.

Отуда се пред субјекте криминалне политике постављају бројни захтеви. Уместо умирујућег игнорисања оваквих дела, потребно је повећати

(25) *„Компјутерски систем"* схваћен је овде као функционална јединица која се састоји из једног или више рачунара и припадајућег софтвера; под „хардвером (*hardware*)" се подразумева укупност машинске, физичке опреме (коју чине нпр. централни процесор, монитори, штампачи, магнетне траке и дискови, скенери, плотери и сл.), а под „софтвером (*software*)"скуп компјутерских програма који садрже инструкције које управљају радом рачунара – в.Parker D. *op cit.* s. X и *Енглеско – српскохрватски речник рачунарства*, Београд, 1988.

ризик њиховог откривања оспособљавањем органа кривичног прогона. Претпоставка за то је систематско научно проучавање компјутерског криминалитета и адекватно иновирање кривичног законодавства, како би се норме ове гране права прилагодиле појавним облицима друштвено опасних понашања у овој области. Уколико већ сада не усвојимо овакав начин размишљања, већ у блиској будућности доћи ћемо у апсурдну ситуацију да један од најопаснијих видова криминалитета, чији се даљи раст са извесношћу очекује, нећемо бити у стању да предупредимо и сузбијемо.

(Примљено 10.01.1991)

Dr Đorde Ignjatović,
Assistant Professor of the Faculty of Law in Belgrade

DETERMINING THE NOTION OF COMPUTER CRIMINALITY

Summary

This is one of the scarce attempts in Yugoslav literature to analyze a specific problem of criminal phenomenology, namely the type of criminality connected to the use of computers. The definition of computer criminality is both distinguishing and general, and followed by a distinction between the narrow and wide conception of that notion.

Computer criminality in its narrow sense is a specific kind of criminal conduct where the computer system conceived as an entity of hardware and software appears either as the means of committing or as the object of criminal offence. The conditions is that such offence could not be committed against some other object at all, or, in the contrary case, that it would have essentially different characteristics. In the wider sense, this covers the committing of any criminal offence which is related to the use or functionning of computers.

In the conclusions it is emphasized that the small nubner of computer criminality which is discovered must not deceive us. This is a criminality whose dark numbers are exceptionally high. Also, all forecasts speak to the fact that this is one of the rare types of criminality whose rise in future development has never been challenged. This is why this new type of criminality should be studied in a systematic way. The results of such studies should serve Yugoslav law - makers to introduce finally amendments which would help preventing such offences. On the other hand, it is necessary to begin immediately with professional training of the corresponding authorities and services in order to prosecute the perpetrators.

Key words: *Computers. - Computer criminality. - Misuse of computers. - Computer fraud. - Informatics criminality.*

Dorde Ignjatović,
Chargé de cours à la Faculté de droit de Belgrade

LA DEFINITION CONCEPTUELLE DE LA CRIMINALITE INFORMATIQUE

Résumé

Le présent travail est une des rares tentatives dans la littérature yougoslavie d'analyser un problème spécifique de la phénoménologie criminelle. L'auteur part de l'assertion qu'il existe un type spécial de criminalité lié à l'utilisation des ordinateurs. Cette criminalité est désingée par le terme de criminalité informatique et outre la description des formes sous lesquelles elle apparaît, l'auteur donne une définition qui, selon son avis, definit ce type de criminalité de manière précise, mais aussi suffisemment généralisée. Il établit aussi une distinction entre le concept plus large eta le concept plus restreint de cette notion.

La criminalité informatique au sens plus restreint, proprement dit, est une forme spécifique de comportements criminels chez lesquels le système de l'ordinateur (compris comme unité du matériel et du logiciel) apparaît ou bien comme moyen d'exécution ou bien comme objet d'un acte criminel, dans la mesure où cet acte ne pourraît pas être commis autrement ou envers un autre objet, ou bien il aurait alors des caractéristiques essentiellement différentes. Dans un sens plus large, ce comportement implique l'exécution d'un acte criminel lié à l'utilisation ou au fonctionnement des ordinateurs.

Et enfin, dans la conclusion de son travail, l'auteur souligne l'évaluation que le nombre modeste des actes de criminalité informatique officiellement découverts ne devrait pas nous tromper. Il s' agit d'un type de criminalité dont le chiffre noir est extrêmement élevé. De même, toutes les prévisions disent que c'est un des rares types de criminalité dont la croissance à l'avenir ne fait pas de doute. Ce sont là autant de raistons pour lesquelles la criminalité informatique doit être étudiée de manière systématique. Les résultats de ces recherches devraient servir aux législateurs yougoslaves pour effectuer enfin des changements par lesquels le système des incriminations s'adapterait à la lutte contre ces actes criminels. D'autre part, il est nécessairae d'amorcer tout de suite la formation des cadres dans les organes dont la tâche est la poursuite des actes criminels et de leurs auteurs en vue que le risque de leur dépistage soit accru.

Mots clés: *Ordinateurs. - Criminalité informatique. - Abus des ordinateurs. - Fraude informatique.*