

# Le Combat contre la Criminalité Informatique dans le Contexte Européen

Nadina Velicu<sup>1</sup>, Marcel Podașcă<sup>2</sup>

<sup>1</sup>*Inspectorat de Police du département de Galați, Police de l'Investigation des Fraudes*

<sup>2</sup>*Inspectorat de Polcie du département de Galați, Police de l'Investigation des Fraudes*

**Abstract.** The article tackles the issue of cyber crime. Moreover, speaks about computer fraud, as a part of criminal activities with cyber crime, generally known as computer crime, e-crime, hi-tech crime or electronic crime too, refers to. It delivers a brief but conclusive definition of fraud involving the computer as the source, tool or target of the crime, presenting the essential characteristics in understanding this phenomenon.

**Keywords:** système informatique, fraude, préjudice, données informatiques

## Le faux informatique et la Fraude informatique

Le développement informatique et l'utilisation à grande échelle des systèmes informatiques a introduit dans l'environnement socio-économique et une série de risques. La dépendance de plus en plus accentuée des agents économiques, des institutions publiques, et même des utilisateurs individuels des systèmes informatiques qui gèrent décidément les ressources, les rendent de plus en plus vulnérables devant l'influence de la criminalité informatique. Par infraction informatique au sens large du terme, on entend: **Toute infraction où un ordinateur ou un réseau d'ordinateurs est l'objet d'une infraction, où dans le cadre de laquelle un ordinateur ou un réseau d'ordinateurs est l'instrument ou le moyen d'accomplissement d'une infraction.** Le contenu de la notion de **fait pénal de nature informatique** est très varié, étant abordé de manières différentes. **Selon le Comité Européen** pour de problèmes criminels, les infractions informatiques sont systématisées comme il suit:

- Infraction de fraude informatique;
- Infraction de fraude en informatique;
- Infraction de préjudice des données ou des programmes informatiques;
- Infraction de sabotage informatique;
- Infraction d'accès non-autorisé à un ordinateur;
- Infraction d'interception non-autorisée;
  - Infraction de reproduction non-autorisée d'un programme informatique protégé par la loi;
- Infraction de reproduction non-autorisée d'une imprimérie;
- Infraction d'altération des données ou des programmes informatiques;
- Infraction d'espionnage informatique;
- Infraction d'utilisation non-autorisée d'un ordinateur;
  - Infraction d'utilisation non-autorisée d'un programme informatique protégé par la loi; Pour une meilleure compréhension de la notion, quelques définitions sans lesquelles la recherche criminalistique de ces faits illicites serait dépourvue de rigueur et précision. Alors:
    - **Par système informatique** on entend tout dispositif ou ensemble de dispositifs interconnectés ou en relation fonctionnelle, dont un ou plusieurs assure l'adaptation automatique des données à l'aide d'un programme informatique;
    - **Par programme informatique** on entend un ensemble d'instructions qui peuvent être exécutées

par un système informatique pour obtenir un résultat déterminé;

— **Par données informatiques** on entend toute représentation de quelque fait, informations ou concepts, dans une forme qui peut être adaptée par un système informatique. Dans cette catégorie on inclut aussi tout programme informatique qui peut déterminer la réalisation d'une fonction par un système informatique;

— **Par mesures de sécurité** on entend l'utilisation des procédures, dispositifs ou programmes informatiques spécialisés à l'aide desquels l'accès à un système informatique est restreint ou interdit pour une certaine catégorie d'utilisateurs;

— **Une personne agit sans en avoir le droit** si elle se trouve dans une des situations suivantes:

- a) Elle n'est pas autorisée, selon la loi ou un contrat;
- b) Elle dépasse les limites de l'autorisation;
- c) Elle n'a pas la permission- de la part de la personne physique ou juridique compétente à l'accorder, selon la loi- d'utiliser, administrer ou contrôler un système informatique ou de développer des recherches scientifiques ou d'effectuer toute autre opération dans un système informatique.

### **Le faux informatique**

L'infraction est prévue dans l'art. 48 de la loi de la criminalité informatique.

Le texte de la loi prévoit que: Le fait d'introduire, modifier ou supprimer dsans en avoir le droit, des données informatiques, ou de restreindre, sans en avoir le droit, l'accès à ces données, le résultat étant des données qui témoignent pas de la vérité, en vue d'être utilisées pour la production d'une conséquence juridique, constitue une infraction et la punition est de 2 à 7 ans de prison.

La réglementation veut la protection de la sécurité juridique par l'accusation de toutes les actions qui peuvent attirer, par la modification des données trouvées sur support informatique, des conséquences juridiques désagréables pour les personnes qui ont conçu, réalisé et implémenté l'information modifiée.

**L'objet juridique spécial** est constitué par les relations sociales souscrites à la protection de la sécurité du circuit juridique.

**L'objet matériel** est constitué par le support où on trouve toutes les données ionformatiques altérées en vue de la production des conséquences juridiques.

**Le sujet actif** peut être toute personne, le sujet passif étant soit le propriétaire des données informatiques altérées en vue de la production des conséquences juridiques, soit les personnes affectées par ces modifications.

**Le coté objectif. L'élément matériel** est donné par l'action de:

- introduire;
- modifier;
- supprimer;
- restreindre l'accès aux données informatiques dans la vue d'une production des effets juridiques;

**Le côté objectif** est caractérisé par une intention directe.

**La consommation** se réalise au moment de l'initiation du procès d'altération des données.

**La tentative** est punie selon les prévisions de l'art. 50.

**La sanction.** L'infraction de faux informatique prévoit une punition de 2 à 7 ans de prison.

Tout comme le texte législatif le montre, la loi a considéré comme infraction de fraude informatique très dangereuse, avec des activités qui ont comme objet les données informatiques. Après une courte analyse des textes mentionnées par la loi, nous constatons que l'infraction d'altération de l'intégrité

des données informatiques réglemente une forme de cadre des activités illicites qui peuvent être développées avec les données informatiques, et le contenu de l'infraction de perturbation du fonctionnement des systèmes informatiques a réglementé une forme qualifiée, après les suites du développement des activités illicites qui visent le fonctionnement des systèmes informatiques. On peut parler maintenant d'une **nouvelle forme qualifiée, selon les suites du développement des activités illicites qui peuvent être développées avec les données informatiques qui a en vue l'obtention des données fausses pour être utilisées au but de la production d'une conséquence juridique**. On peut observer que la suite qui prévoit l'obtention des données fausses, est traitée par la loi comme une étape intermédiaire et, finalement, elle sera d'intérêt à but explicite- l'utilisation en vue de la production des conséquences juridiques.

Dans le contexte, dans le cadre de l'enquête, l'établissement **du but du développement de l'activité illicite** devient très important. Si on peut essayer le développement des actions incriminées, dans le contenu constitutif de l'infraction, en vue d'obtenir des données fausses qui soit utilisées pour produire des conséquences juridiques, l'enquête insistera sur l'encadrement de l'activité comme faux informatique. Si on ne peut pas essayer ce but, l'activité illicite sera encadrée soit comme altération de l'intégrité des données informatiques, soit, dans la mesure où le résultat est la perturbation grave du fonctionnement d'un système informatique, comme perturbation du fonctionnement des systèmes informatiques. Les recherches dépasseront le niveau d'ignorance qui se manifeste parfois, l'investigation des nouvelles situations étant nécessaire: les conséquences juridiques suivies, les personnes physiques ou juridiques dont les intérêts sont impliqués dans le développement des activités illicites, la nature des préjudices, la mesure où les conséquences liées à l'activité des institutions ou de l'administration de l'état ou des communautés locales apparaissent etc.

Concernant l'activité illicite, elle peut témoigner de l'introduction, de la modification, de la suppression ou de la détérioration des données informatiques ou du restrictionnement de l'accès aux données informatiques- une seule action, deux ou plusieurs, la même action, la même action faite plusieurs fois etc, ayant la possibilité de constater une forme continuée, une forme continue- dans le cas du restrictionnement de l'accès- ou seulement d'une tentative. Comme observation, dans l'énumération des actions considérées comme dangereuses, entre la formule de l'art. 45 et celle de l'art. 48 du Chapitre III de la Loi 161/2003, il y a une différence dans le sens que dans le contenu du faux informatique n'apparaît plus la notion de transmission. Cette modification est raisonnable par la nature des choses- seulement par la transmission des données informatiques on ne peut pas obtenir un résultat du type à celui prévu par l'art. 48, dans le sens de l'obtention des données fausses.

Un problème d'intérêt est **l'établissement de la personne physique ou juridique préjugée comme suite du développement de l'activité illicite**. Il n'est pas suffisant qu'on identifie la personne qui a un droit légal d'opérer avec les données informatiques, personne préjugée, bien évidemment, par la personne des criminels. Il est nécessaire l'identification des personnes qui subissent les conséquences juridiques suivies par les criminels par l'obtention des données fausses, conséquences fondementées par une réalité fautive caractérisée justement par l'existence des données fausses, mensongères. Il est probable que ces personnes ont le plus à souffrir parce qu'elles fondent leur comportement social sur une réalité mensongère qui détermine des actions erronées qui ne peuvent déterminer, à leur tour, que des pertes pour le patrimoine des personnes face auxquelles les conséquences juridiques se manifestent et pour d'autres personnes qui ont des relations patrimoniales avec celles-ci.

Il est à remarquer le fait que le **préjudice** apparaît dans le cadre de l'infraction de faux informatique comme quelque chose d'implicite, inhérent, mais pas comme quelque chose de manifeste. Les conséquences juridiques qui ont à la base des données fausses, par la nature des choses, produisent des préjudices. Au centre de la démarche législative se trouve l'accomplissement de quelques activités illicites ayant comme but l'obtention des données fausses, c'est vrai, pour être utilisées en vue de la production d'une conséquence juridique.

On peut observer que le but doit être suivi et pas réalisé effectivement, la réalisation étant éventuelle. Le criminel qui développe l'activité illicite obtient la suite caractéristique et peut commencer à utiliser les données fausses, peut ajourner leur utilisation ou il peut y renoncer. Il est important pour la consummation de l'action le développement de l'activité illicite et l'obtention des suites

caractéristiques- pratiquement l'infraction est consommée au moment où on obtient les données fausses.

### **La Fraude informatique**

L'infraction est prévue dans l'art. 49 de la loi de la criminalité informatique.

Le texte de la loi prévoit que: le fait de causer un préjudice patrimonial à une personne par l'introduction, la modification ou la suppression des données informatiques par la restriction de l'accès à ces données-là ou par l'entravement du fonctionnement d'un système informatique en vue d'obtenir un bénéfice matériel pour soi-même ou pour quelqu'un d'autre, constitue une infraction et elle est punie de 3 à 12 ans de prison.

**L'objet juridique spécial** est constitué par les relations sociales qui protègent le patrimoine d'une personne.

**L'objet matériel** est donné par les systèmes informatiques qui contiennent des données informatiques altérées ou qui sont empêchées à fonctionner comme suite de l'activité du criminel.

**Le sujet actif** peut être toute personne et **Le sujet passif** peut être toute personne physique ou juridique dont le patrimoine est affecté par des actions sur les systèmes informatiques qu'elle détient ou qu'elle utilise.

**Le côté objectif. L'élément matériel** est constitué par l'action de:

- introduire des données informatiques;
- modifier des données informatiques;
- supprimer des données informatiques;
- restreindre l'accès aux données informatiques;
- entraver le fonctionnement d'un système informatique.

**Le côté subjectif** est caractérisé par l'intention.

**La consummation** est réalisée au moment de l'action qui a comme résultat la création du préjudice patrimonial.

**La tentative** est punie conformément aux prévisions de l'art. 50.

**La sanction.** L'infraction de fraude informatique est sanctionnée avec la prison de 3 à 12 ans.

**La fraude informatique** est une autre infraction qui traite des activités illicites qui ont comme objet des données informatiques auxquelles on ajoute, à cause de la nature de l'environnement, les systèmes informatiques. On a à faire à une nouvelle forme qualifiée d'après le résultat du développement de l'activité illicite- le préjudice patrimonial. Ce résultat devient si important qu'il constitue le centre de la démarche législative. Pour des raisons de technique législative, l'activité illicite, considérée comme très dangereuse, est liée à la création d'un préjudice, l'introduction, la modification ou la suppression des données informatiques, le restrictionnement de l'accès à ces données ou l'entravement du fonctionnement d'un système informatique deviennent des modalités par lesquelles on peut causer un préjudice.

**Le résultat du développement de l'activité illicite** doit nécessairement représenter **la création d'un préjudice patrimonial**. Comme nous avons montré auparavant, normalement, toute conséquence juridique basée sur une réalité fautive, est vouée à créer des préjudices patrimoniaux avant tout. Dans le cas de la recherche de l'infraction de fraude informatique, les enquêteurs vont vérifier plus que la simple existence et, éventuellement, le développement d'un préjudice causé par le développement d'une activité illicite avec des données ou des systèmes informatiques. **On ne peut pas parler d'un préjudice quelconque qui, par ses principaux éléments caractéristiques, est suivi par les criminels.**

L'infraction est consommée au moment où on réalise le préjudice dans le patrimoine d'une personne physique ou juridique et pas au moment du développement de l'activité illicite. Si l'activité illicite a

lieu sans créer le préjudice en cause, on peut parler de l'investigation d'une tentative. Dans le cas des préjudices qui se développent dans le temps- des situations fréquemment rencontrées dans la pratique- j'apprécie qu'il n'est pas nécessaire d'établir les conditions qui permettraient une évaluation certaine de l'étendue du préjudice pour considérer l'infraction comme consommée. Il suffit d'investiguer l'existence d'un préjudice, l'infraction est consommée pratiquement avec le début de la manifestation du préjudice. L'enquête sera intéressée d'évaluer, bien évidemment, le préjudice tout entier, ou au moins d'établir les éléments spécifiques qui aideront à l'évaluation du préjudice, mais ce problème ne doit pas influencer le moment où l'infraction est consommée.

L'infraction est susceptible d'une forme continuée, au cas où on investigate le développement des activités illicites avec des données informatiques et des systèmes informatiques dans le temps, avec la création des préjudices épisodiques, à évaluer séparément.

Une précision est nécessaire, concernant la liaison entre préjudice et une personne physique ou juridique déterminée. **Par le but suivi par le développement de l'activité illicite**, les criminels veulent la création et le développement d'un préjudice qu'ils exploitent pour eux-mêmes ou pour une autre personne- pour obtenir un bénéfice pour leur propre patrimoine ou celui d'une autre personne. Pour que cela arrive, il faut que le préjudice puisse être contrôlable.

En analysant la situation avec attention, on peut observer que, comme suite du développement de l'activité illicite avec des données et des systèmes informatiques, des conséquences de nature patrimoniale et non-patrimoniales sont générées. Dans le cas de la présente démarche, nous sommes intéressés par les conséquences de nature patrimoniale qui peuvent être exploitées- dans le sens de la création des préjudices dans le patrimoine d'une personne physique ou juridique en liaison directe avec la génération des gains dans le patrimoine du criminel ou des autres personnes- ou qui ne peuvent pas être exploitées- le cas de ces préjudices qui échappent à tout contrôle parce qu'ils ne peuvent pas être transformés en gains qui servent à un patrimoine déterminé. Alors, l'enquête devra prouver justement l'existence d'un préjudice dans le patrimoine d'une personne physique ou juridique déterminée qui soit constituée par un élément qui facilite par une relation directe le fait qu'il puisse être contrôlé et qu'il soit un bénéfice matériel pour le criminel ou pour toute autre personne.

**L'identité des personnes impliquées** est un problème important, à part les éléments d'intérêt commun à toute enquête, on a à faire à des éléments particuliers qui témoignent de la relation patrimoine-personne. Le ou les criminel(s), selon la situation, sont intéressés à obtenir un bénéfice matériel dans leur propre patrimoine ou dans celui des autres personnes. Il serait intéressant d'établir quelle devrait être la nature de la relation entre le criminel et la personne pour laquelle il veut obtenir un bénéfice matériel. S'il s'agit de mettre fin à une obligation, de la couverture d'une garantie, de toute autre situation qui suppose une relation patrimoniale, je pense qu'il faut observer un certain effet sur le patrimoine du criminel. Une situation spéciale serait celle des libéralités, situation où le criminel voudra un bénéfice dans le patrimoine d'une autre personne sans y impliquer à diminuer son propre patrimoine, par compensation avec le développement des activités illicites.

La personne dont le patrimoine serait enrichi par un bénéfice matériel, sera identifiée pour investiguer l'ensemble des éléments constitutifs de l'infraction et pour récupérer le préjudice dans le cas où le bénéfice matériel recherché par le criminel est réalisé effectivement, pouvant constater une augmentation, un enrichissement du patrimoine de cette personne. Au cas où les investigations prouveront des actes de participation, une commande éventuelle, une sollicitation voulue de cette troisième personne, le traitement judiciaire sera adapté, dans le sens que cette personne sera inculpée tout comme dans un autre cas où une infraction est réalisée, la résolution infractionnelle du criminel est influencé décidément par la demande d'une troisième personne<sup>1</sup>.

---

<sup>1</sup> N.A. – à voir les décisions de la Cour Suprême concernant le vol commandé lié au traitement judiciaire de la personne qui passe l'ordre.

**De l'analyse des données concernant la criminalité informatique, on peut mettre en évidence les tendances d'évolution suivantes:**

- Les infractions informatiques deviennent de plus en plus fréquentes. La société informationnelle dépend de plus en plus des ordinateurs. Les composantes importantes de la vie sociale sont des coordonnées des systèmes informatiques. Comme une conséquence, le nombre des attaques par l'intermédiaire et sur ceux-là augmentera.
- Les infractions informatiques peuvent être commises de nos jours par toute personne et elles peuvent atteindre virtuellement toute personne. Si les systèmes informatiques constituaient, à leur apparition, un attribut des environnements scientifiques, militaires et gouvernementales, aujourd'hui, à cause des performances liées à la réduction des prix, elles sont disponibles à tout le monde.
- Les infractions informatiques ont un caractère de plus en plus mobile et de plus en plus international. La procession électronique des données est de plus en plus convergente au domaine des télécommunications. Les infractions informatiques sont, encore plus de nos jours, commises par l'intermédiaire des réseaux de télécommunications.
- Les infractions informatiques et le réseau internet constituent spécialement une attraction pour les organisations du crime organisé. L'anonymat offerte par les réseaux mondiaux d'ordinateurs, tout comme les méthodes de transmission des messages par leur aide, liés à l'impossibilité des forces de maintien de l'ordre public de contrôler le flux d'information, présente des avantages spéciaux pour les groupes du crime organisé, y compris celles à caractère transnational.

**Bibliographie:**

LOI nr.161 / 2003 concernant quelques mesures pour assurer la transparence dans l'exercice de la dignité publique, des fonctions publiques et dans l'environnement des affaires, prévention et la sanction de la corruption, Titre III, Prévention et combat contre la criminalité informatique,  
Boroi – „Drept penal, partea specială”, Editura Cermaprint, București, 2006;  
DIRECTIVE 2000/31/EC – concernant le commerce électronique, établit le cadre pour les législations nationales concernant les services informatiques destinés au marché interne, surtout concernant le régime des transmissions commerciales et des contrats, la responsabilité des intermédiaires, la solution des litiges, la coopération entre les états membres concernant ce problème.  
Vasile Bercheșan – „Metodologia investigării infracțiunilor”, Editura „Paralela 45”, Pitești, 1998;  
Maxim Dobrinoiu – „Infracțiuni în domeniul informatic”, Ed. C.H. Beck , București 2006;  
Tudor Amza, Cosmin-Petronel Amza – „Criminalitatea informatică”, Ed. Lumina Lex, București, 2003,  
Gabriel Ion Olteanu – „Metodologia criminalistică – Cercetarea structurilor infracționale și a unora dintre activitățile ilicite desfășurate de acestea”, Ed. AIT Laboratories s.r.l., 2005,  
[www.legi-internet.ro/articole-drept-it/provocari-constitutionale-ale-internetului.html](http://www.legi-internet.ro/articole-drept-it/provocari-constitutionale-ale-internetului.html)  
[adi.ro/pub/scoala/Master/SemI/SecDate/Materiale%20CURS%202007/00.3%20Introducere.doc](http://adi.ro/pub/scoala/Master/SemI/SecDate/Materiale%20CURS%202007/00.3%20Introducere.doc)  
[www.euroavocatura.ro/articole/cat/61/Infracțiuni\\_Informatic](http://www.euroavocatura.ro/articole/cat/61/Infracțiuni_Informatic)