Ioan Petrişor
Daniela Stanciu
Liana Stefan
Université Ouest Timisoara, Romanie

CULTURE LIBRE ET HACKING

Introduction

La création de l'Internet, ce nouveau milieu de communication omniprésent et tout-puissant, a engendré des transformations importantes dans tous les domaines de la vie sociale. L'usage de l'Internet est lié au monde quotidien et il annonce l'émergence de cette société en réseau tant annoncée (c'est vrai, sans être uniformément développée à travers le monde). Moyen de relier les êtres humains, de créer un monde virtuel où le partage des informations est, pratiquement, illimité, l'Internet a favorisé la parution du mouvement du logiciel libre (le free software mouvement) et le développement du concept de *culture libre.*

Dans le contexte de la mondialisation, la culture libre représente une aspiration à l'accès égal à la connaissance et à l'information. Elle vise la libre distribution du savoir et son développement grâce à l'enrichissement d'śuvres déjà existantes sans les limites imposées par la protection juridique de la propriété intellectuelle. *Wikipedia,* cette encyclopédie électronique universelle mise en ligne le 10 janvier 2001, est un exemple édifiant de cette philosophie du partage avec plus de 16 millions d'articles rédigés en plus de 270 langues et attirant quelque 78 millions de visiteurs.

Pourtant il ne faut pas confondre (comme il arrive souvent) le terme *libre* avec *gratuit* ou *ouvert*, car la culture libre n'est pas nécessairement gratuite. *Libre* signifie qu'un article, par exemple, puisse être reproduit, modifié, partagé, etc. sans autorisation spécifique de l'auteur original: *ouvert* signifie que l'auteur n'a pas fermé le code source qui peut ainsi être modifié et reproduit alors que le terme *gratuit* implique l'idée d'utilisation de l'article sans avoir à payer de droits.

1. Le monde du libre

Théoriquement, la philosophie du partage des connaissances et leur accessibilité à tous est commune à tous les secteurs qui forment le monde du «libre», mais la réalité varie selon les champs d'application.

L'Informatique. Le secteur de l'informatique est certainement celui où la philosophie du libre est la plus répandue. Le terme «source ouverte» désigne alors un éventail de licences pour logiciels qui rend le code source disponible au public avec peu ou sans restrictions découlant du droit d'auteur. Le logiciel peut ainsi être utilisé, étudié et modifié sans restriction, de même qu'il peut être copié et redistribué dans sa forme modifiée pourvu que les utilisateurs subséquents jouissent des mêmes droits.

Liberté ou infraction. La question se pose si l'on est conscient des limites de cette liberté, si elle envisage aussi le dépassement des limites de la légalité et de la morale. Les «pirates informatiques» utilisent l'ordinateur pour commettre une infraction, un acte qui représente un danger social et qui est sanctionné par la loi. Les infractions informatiques sont multiples et diverses et leur liste est enrichie en permanence grâce à l'imagination et à la créativité des pirates informatiques. La fraude informatique, le faux en informatique, les préjudices pour les données et les programmes de l'ordinateur, le sabotage informatique, l'accès non autorisé, l'interception et la reproduction non autorisée des programmes protégés, l'espionnage informatique, l'emploi non autorisé d'un ordinateur ou d'un programme sont des infractions punies par la loi dans la majeure partie des pays développés. Il y a une recommandation du Conseil de l'Europe, R(89)9, pour combattre la délinquance à l'aide de l'ordinateur. Au plan mondial il y a eu une tentative pour cataloguer les dangers sociaux dans le domaine de l'informatique et ils ont été groupés dans la catégorie «Computer Aided…» à laquelle appartiennent les acronymes connus CAD (computer-aided design), CAM (computer-aided manufacturing), etc. On a proposé alors que les faits criminels commis à l'aide de l'ordinateur soient nommés «Computer Aided Crime». Quel que soit le nom attribué à ces faits, une chose est certaine : on ne peut plus les négliger, car ils évitent que les ordinateurs occupent une place de plus en plus importante dans notre vie quotidienne et que, parallèlement avec leur évolution spectaculaire, malheureusement, une criminalité spécifique se développe de plus en plus.

Hackers et crackers. La culture hacker est parue aux années 70-80 et s'est développée dans les décennies suivantes comme une alternative à la culture libre, un réseau informatique délocalisé qui reliait, au début, plusieurs universités américaines. À l'origine, un hacker était un programmateur informatique débrouillard,

une personne curieuse qui adore explorer les détails des programmes et leurs capacités.

Les dernières années, pour la plupart des gens, un hacker est un vilain personnage dont l'activité mafieuse consiste à s'immiscer dans un espace numérique privé pour en usurper le contrôle. La destruction, le vol (de données et d'argent), les infections virales ne sont que quelques méfaits qui lui sont attribués. Mais il y a des voix, de plus en plus nombreuses, qui affirment qu'un hacker est avant tout un débrouillard passionné par la technique qu'il étudie, éprouve et bricole pour en tirer tout son potentiel. Il existe des hackers dans tous les domaines : sécurité informatique, développement web ou logiciel, robotique, mécanique automobile, physique, chimie, etc. Hacker n'est donc pas du tout synonyme de pirate. Ce n'est pas un mot péjoratif, mais plutôt une gratification, une marque d'expérience et de débrouillardise. Pour le verbe *hacker* on indique des synonymes tels *s'approprier, détourner, bricoler* et non pas *voler.*

L'innovation, le peaufinage, l'enrichissement des fonctions sont les résultats du hacking. Mais c'est surtout l'innovation qui motive le hacker. On doit aux hackers la richesse technique et ils ne méritent pas leur mauvaise réputation.

Il ne faut pas les confondre avec les **crackers** qui, n'ayant rien à faire avec les petits biscuits salés, sont des pirates informatiques qui s'introduisent dans un système ou dans un réseau informatique dans le but de perturber son fonctionnement ou de le détruire. Il est un pirate, spécialisé dans la violation de protection ou de bridage, par exemple les mots de passe, les DRM (Digital Rights Management), les pare-feu, les codes PIN, etc.

Il semble que les internautes font la différence entre les bons et les mauvais hackers, qu'il y a ceux que l'on appelle «white hats» (qui sont bien intentionnés), les «black hats» (mal intentionnés) et les «grey hats» (qui sont entre les deux). Ces catégories ainsi que le grand nombre des termes qui désignent les personnes ayant des activités plus ou moins légales sur l'Internet démontrent les dimensions et la complexité du phénomène.

2. Le hacking en Roumanie

Les statistiques montrent que les Roumains sont parmi les plus nombreux et dangereux hackers. Ils représentent une menace permanente pour les systèmes les plus sécurisés. On distingue au moins deux catégories de hackers, selon les articles publiés dans plusieurs journaux que nous avons consultés pour nous documenter sur ce phénomène: les bienveillants (qui donnent des avertissements pour

corriger une erreur ou pour améliorer la sécurité d'un système) et les malveillants (qui, sans être nécessairement des pirates, produisent des dégâts dans les systèmes informatiques). Nous allons citer quelques cas présentés dans les médias et qui illustrent la différence entre ces deux catégories.

Fraudes informatiques roumaines. Un hacker fâché contre les prix en continuelle augmentation chez RomTelecom, a pénétré dans le réseau interne de la société et y a modifié les tarifs : 1 leu pour 5 heures de conversation.

D'autres hackers ont pénétré il y a quelques années le site du Pentagone. Ils n'ont rien obtenu parce que le site n'était pas très important et on les a découverts avant de produire des dégâts. Plus récemment, Răzvan Cernăianu, alias TinKode, étudiant à Timisoara, à l'Université de l'Ouest, a réussi à pénétrer dans les systèmes de la NASA et du Pentagone. Ensuite il s'en est vanté sur son blogue et sur Facebook. Le jeune étudiant en informatique a reçu un prix de Google pour avoir signalé une brèche dans le système de sécurité et la vulnérabilité des logiciels de la compagnie. Son nom se retrouve sur la liste "Google Security Hall of Fame".

Butyka Robert, Victor Faur sont d'autres jeunes gens qui ont réussi des performances pareilles sans avoir des études de spécialité. Le premier n'a même pas terminé le lycée, il l'a abandonné en neuvième. L'anglais, il l'a appris à la télé, et le hacking, en autodidacte. La NASA a déclaré à propos de Victor Faur qu'il a compromis 150 servers par ses intrusions illégales dans des ordinateurs qui contenaient des données scientifiques, y compris des logiciels spatiaux et de nouveaux types de technologie, pertes évaluées à 240.000 de dollars.

Le Ministère des Affaires Intérieures, de la Justice et des Finances de la Roumanie ont été attaqués plusieurs fois par des virus qui ont provoqué des modifications majeures aux informations des sites respectifs. Lorsque le gouvernement a annoncé l'augmentation des accises aux boissons alcooliques, sur la page web du Ministère des Finances un hacker a introduit un message de proteste: «Ce site a été pénétré par le Roi de la Bière».

Il y a eu aussi des hackers roumains qui, pour se moquer du gouvernement, ont changé les photos de son site. Un autre a affiché la photo du président Iliescu sur le site du FBI.

En ce qui concerne le commerce électronique, les Roumains se sont spécialisés dans les achats dans les magasins virtuels qui se trouvent à l'étranger (la plupart aux États Unis), en utilisant des cartes de crédit volées ou faussées. Pour cela ils ont utilisé des sites spécialisés dans le commerce électronique et des bases de données avec des numéros de cartes de crédit. Ce genre d'attaques a été favorisépar le fait que le temps qui s'écoule du moment du payement illégitime au moment où le propriétaire de la carte s'en rend compte et refuse le payement, est assez long.

Un autre hacker roumain a bloqué l'ordinateur d'une personne qu'il détestait. Lorsque celui-ci l'ouvrait et entrait dans Word, il écrivait un texte et l'ordinateur se restartait. Évidemment, l'ordinateur est devenu pratiquement inutilisable. Finalement, le hacker a pardonné cette personne et puis il a corrigé lui-même la situation.

Voilà aussi des exemples de hackers qui ont aidé, au lieu de détruire: un de ceux-ci a découvert quelques erreurs (bugs) dans le réseau des ordinateurs d'un citoyen américain qui venait d'ouvrir un Internet café à Bucarest. Il l'a averti plusieurs fois que l'administrateur de ce réseau n'accomplit pas correctement son devoir ou il n'est pas capable de protéger son système. L'Américain a invité le hacker venir travailler à sa firme. Depuis il y est embauché, il touche un salaire décent, il a le taxi de contact et le téléphone payés par la firme.

Un excellent hacker roumain, dans le sens originaire du mot, a trouvé des bogues (bugs) dans le réseau de la société Ericssonet il leur a envoyé ses observations ainsi que la solution pour résoudre le problème. Les patrons de la société lui ont fait cadeau le dernier type de téléphone plaqué d'or.

Bien que les exemples négatifs semblent être plus nombreux, nous supposons plutôt que les journaux préfèrent parler des mauvais sujets pour trouver le sensationnel, l'événement qui assure la vente.

La loi roumaine et les délits informatiques. Au début du mois d'octobre 1999, le Tribunal de Ploieşti (grande ville roumaine tout près de Bucarest) a prononcé une sentence qui condamnait l'administrateur de la firme Andantino à six mois de prison avec sursis. Le 18 septembre 1998, l'accusé avait été surpris par les policiers et par les inspecteurs de l'Office Roumain pour des Droits d'Auteur en train de vendre des CD avec des logiciels au magasin de sa société. «C'est la première sentence pénale dans le domaine de la piraterie software depuis l'adoption en 1996 de la Loi nº 8 des Droits d'Auteur et des Droits Connexes et représente une première preuve concluante que la propriété intellectuelle commence à être respectée en Roumanie aussi» a déclaré un avocat qui représentait la Roumanie dans la Business Software Alliance.

Il faut admettre que la loi roumaine a été longtemps incapable de sanctionner les délits informatiques, que la préoccupation des autorités pour stopper les activités nuisibles des pirates de l'Internet était presque inexistante. Les dernières années des efforts remarquables ont été faits dans ce domaine tout en essayant une harmonisation avec la législation de l'UE. L'activité de la DIICOT (Direction d'Investigations des Infractions de Criminalité Organisée et Terrorisme) dans le domaine du hacking est de plus en plus importante et les résultats se voient dans le grand nombre d'arrestations. Des hackers célèbres ont été arrêtés et leurs inter-

views présentées dans les médias ont dévoilé quelques traits de leur personnalité et la motivation qui les anime.

Psychologie et motivation des hackers. S'ils envoient des messages ou des mails aux administrateurs de système pour les annoncer qu'ils ont une erreur (bug) dans le système de sécurité, les hackers sont considérés comme des magiciens des ordinateurs. Souvent ils ont offert eux-mêmes des solutions pour enlever les faiblesses de protection des systèmes. D'autres hackers s'amusent tout simplement lorsqu'ils pénètrent les systèmes des autres pour faire des farces telles le changement du background du desktop, la fermeture et l'ouverture du CD-Rom, etc.

Souvent les hackers vérifient la «compétence» des administrateurs du système en les faisant passer de diverses épreuves pour voir s'ils sont ou non capables de tenir les systèmes sous protection. Beaucoup d'administrateurs sont souvent terrorisés tout simplement.

Qu'est-ce que les hackers cherchent dans les ordinateurs des autres gens? D'habitude ceux-ci cherchent un compte, une carte, un mot de passe d'accès, certains cracks, des logiciels ou des licences. Les hackers opèrent souvent sur les connexions des adversaires, «en transférant» de cette manière une grande partie des dépenses pour la communication dans le compte de ces derniers.

Même si leurs intentions sont honorables, comme dans le cas du fameux virus de type «warm» qui s'appelle «I love you» et dont l'existence a été signalée quelques mois d'avance par des hackers, leurs avertissements ont été ignorés. La conséquence: des dommages estimés à 6 milliards USD.

Les hackers avouent qu'il y a certains sites avec des logiciels qui, s'ils sont intelligemment utilisés, personne ne peut les dépister. Et alors comment sont-ils trouvés et arrêtés? Plusieurs ont avoué leurs méfaits sur leurs blogs ou sur Facebook en quittant ainsi l'anonymat. La vantardise ou le désir de faire connaître leurs exploits ont été les principales causes de leur échec. Après des décennies d'anonymats, ils éprouvent le besoin d'avoir un statut, des droits, d'être reconnus par la société.

Les hackers ont constitué des organisations qui demandent des droits, dérivés, surtout, de la «Déclaration universelle des droits de l'homme». *L'éthique du Hacker* est leur livre de chevet. On y trouve des idées telles:

– l'accès aux ordinateurs doit être total et illimité;
– toutes les informations doivent être gratuites;
– les hackers doivent être jugés selon leurs faits, et non pas selon d'autres critères, tels l'âge, les diplômes, la race ou la position sociale;
– on peut créer de l'art et l'on peut apporter de la beauté à l'aide de l'ordinateur;

– les ordinateurs peuvent améliorer la vie.

Il semble que l'effet de ce livre a été bénéfique parce que, après la parution de ce code déontologique, les hackers ont eu moins d'attaques pour gagner de l'argent et ont intensifié leur activité en ce qui concerne les droits des citoyens.

Les hackers sont aussi un festival annuel qui se trouve à sa quatrième édition, un dictionnaire de jargon et un guide, le livre d'Eric S. Raymond, *How To Become A Hacker,* traduit en roumain par Andrei Savu et posté sur son blog.

Hackerville. La ville Râmnicu Vâlcea, située dans le département de Vâlcea, au nord-ouest de la capitale de la Roumanie, a gagné une triste notoriété: le réseau de hackers qui s'y trouve a effrayé toute la planète, comme l'affirme *Le Monde* dans un article repris aussi par Worldcrunch.com.

Râmnicu Vâlcea, avec son quartier Ostroveni, est connu sous le nom de *Hackerville*, parce qu'il est la capitale des vols en ligne. Les clients de tous les pays qui font des achats en ligne – des Français, des Britanniques, des Allemands, des Italiens, mais surtout des Américains, ont été trompés par des hackers roumains. Dans ce quartier tout le monde sait ce qui se passe, mais le code du silence fonctionne sans faute.

Paradoxalement, les hackers ont accepté de donner des interviews aux journalistes français, tant que leur anonymat soit respecté. Nous reproduisons quelques aveux dont la traduction du roumain nous appartient.

"Il est plus facile avec les Américains car ils achètent tout en ligne, même leur pain, ils sont habitués à tout faire sur Internet". Le jeune homme qui a fait cette déclaration soutient qu'il donne 4 ou 5 coups par semaine et finalement il lui reste quelques dizaines ou centaines de milliers de dollars.

"Nous vivons dans un grand monde, plein d'imbéciles, qui sont prêts à tout faire en ligne. Nous vendons des produits fictifs, nous clonons d'autres sites et nous volons les données des cartes de crédit. En Europe, pour s'emparer de l'argent, nous utilisons les soit nommées «flèches» ou les «porteurs d'argent» qui redirigent l'argent envoyé dans un certain compte. Les porteurs gardent 30% de l'argent et ils nous envoient le reste par Western Union", explique le hacker. L'affaire est assez rentable si l'on regarde les transactions faites sur Western Union.

Les hackers roumains ont compris aussi qu'il vaut mieux travailler en équipe, ce qui leur donne un pouvoir plus grand par rapport à d'autres hackers. Les porteurs sont les plus exposés des hackers, et, pour la plupart du temps, ils utilisent des ID faux. Ils savent tout sur le monde complexe de l'Internet.

"Nous avons invités tous nos voisins devant les ordinateurs. Nous avons utilisé des enfants de 14 ans pour nous aider. Nous avons utilisé aussi des enfants des orphelinats et nous les avons faits travailler pour nous", raconte le hacker.

Victor Faur, alias SirVik, connaît très bien le système, car il est un des hackers les plus connus de Roumanie. Il a été pris et condamné à 6 mois de prison avec sursis et à payer une amende de 240.000 dollars. Il a cassé les serveurs de la NASA pour leur démontrer la faiblesse de leur système de sécurité. "Je leur ai attiré l'attention de réparer leur système de sécurité, mais j'ai fait l'erreur de me vanter sur un site qu'ils surveillaient", dit le hacker.

Selon Ice Man, un autre hacker renommé en Roumanie, qui s'appelle Robert Butyka, voler sur l'Internet est très simple. Mais il ajoute aussi que pénétrer de divers sites n'est pas la même chose avec voler parce que les hackers sont attirés surtout par le défi.

Râmnicu Vâlcea est le centre de la criminalité en ligne de la Roumanie et les actions des hackers qui y habitent ont frappé quelques continents. Le phénomène a débuté en 1996 et il a eu l'effet de la boule de neige dans la ville. Les autorités de Bucarest ont commencé à suivre ce phénomène en 2003, sous la pression des États-Unis.

Pour neutraliser les hackers, un groupe des professionnels du FBI, spécialisés dans les fraudes informatiques, est venu à Bucarest pour préparer 600 policiers roumains pour le combat contre la criminalité. Dans la police roumaine on a créé une unité spéciale avec 200 membres détachés dans tous les départements du pays.

Conclusion

Dans les déclarations que les hackers roumains ont faites sur l'Internet ou dans les journaux des dernières années, nous avons pu constater que le hacking est devenu une véritable culture qui a son propre code, même son éthique. Si au début de leur activité ils étaient une espèce d'anarchistes qui voulaient changer l'ordre social pour permettre l'accès libre à l'information ou aux richesses de ce monde, leurs efforts actuels montrent un désir de se faire entendre, une aspiration vers la légitimité.

Le temps est venu de nous demander si ces hackers, qu'ils soient Roumains ou d'autre nationalité, ne représentent pas les éléments de la «destruction créatrice». La crise actuelle, inhérente à la logique interne du capitalisme comme toute autre crise, peut engendrer elle-aussi des innovations en bousculant les positions acquises. L'exploration des idées nouvelles et l'ouverture vers des opportunités deviennent ainsi possibles. L'ordre économique et social, qui caractérisent les pé-

riodes de non-crise, bloque les initiatives or les hackers qui nient cette ordre ne font que libérer les flux des innovations.

Dans la logique de «la veille anticipative» dont l'objet, pour les entreprises et les collectivités, est la gestion de l'information de leur environnement extérieur afin d'anticiper les changements importants, actuels et futurs, pour leur devenir, les hackers ne font qu'anticiper les dangers qui menacent les systèmes informatiques. Ils attirent l'attention des veilleurs (administrateurs) sur les faiblesses des logiciels et des codes. Grâce à leur activité, les décideurs ne peuvent plus négliger l'anticipation et ignorer les signes d'une difficulté future. Les hackers apportent une aide aux responsables de ce monde en les obligeant de faire attention aux «signaux faibles» annonciateurs de changements pertinents.

Les hackers mènent une guerre de longue haleine par la ré-information de leurs concitoyens et pour la reconquête des réseaux et des structures institutionnels. Avec leurs armes silencieuses mais extrêmement efficaces, ils envisagent un renversement graduel des rapports de force. Ils sont en guerre et les armes utilisées ne sont pas matérielles. Leur message est facile à déchiffrer : l'intelligence et la créativité n'ont pas de limites, elles peuvent ouvrir n'importe quelle porte. Ceux qui ont découvert ces vérités ont transformé les black hats en white hats en les embauchant à leurs firmes.

Bibliographie

Blanc S., Noor O.: *Hackers:Bâtisseurs depuis 1959.* Owni Editions, Paris 2012.

Lesca H., Lesca N.: *Les signaux faibles et la veille anticipative pour les décideurs.* Hermès-Lavoisier, Paris 2011.

Schumpeter J.A.: *Capitalism, Socialism and Democraty.* Routledge, London and New York 1994.

Mad: *Desprehackingşi cum gândeşte un hackerde fapttot ce se poate şti,* [Online] Available http://voodootutorials.3x.ro/tutorials/desprehacking.htm (25.01.2013).

Raymond E.: *Cum să devii un hacker,* [Online] Available http://wiki.lug.ro/Cum_s%C4%83_devii_un_hacker (25.01.2013).

Stallman R.: *Culture libre – une définition* [Online] Available http://www.ciac.ca/fr/culture-libre-une-definition-fr (21.01.2013).

http://www.gandul.info/stiri/.

http://www.incont.ro/social-media.

http://jurnalul.ro/stiri/.

CULTURE LIBRE ET HACKING

Résumé

L'Internet représente un moyen de relier les êtres humains, de créer un monde virtuel où le partage des informations est, pratiquement, illimité. Le mouvement du logiciel libre (le free software mouvement) a créé aussi le concept de culture libre et même un courant de pensée qui se fonde sur des valeurs telles la liberté d'expression ou le partage du savoir. La culture hacker est parue aux années 70-80 et s'est développée dans les décennies suivantes comme une alternative à cette culture libre, un réseau informatique délocalisé qui reliait, au début, plusieurs universités américaines. À l'origine, un hacker était un programmateur informatique débrouillard, une personne curieuse qui adorait explorer les détails des programmes et leurs capacités. De nos jours ce nom est devenu péjoratif et synonyme avec „pirate informatique". Nous nous proposons une réflexion sur l'activité de ces personnes, sur leur éthique, à partir de nombreux cas de la Roumanie. Pour le déroulement de notre recherche nous avons utilisé les données secondaires extraites de quelques interviews publiés dans les journaux roumains, puis nous avons fait appel à l'analyse de leur contenu pour découvrir les stratégies relationnelles pratiquées, les tactiques et les comportements usuels adoptés. Exceptant l'aspect pénal de certaines activités des hackers, ceux-ci mettent l'accent sur leur désir d'accès libre à l'information, de transparence. Le hacking est une infraction, mais est-ce qu'il pourrait représenter une conception nouvelle qui considère le savoir comme un bien public? L'śuvre de l'esprit est produite et appartient à la communauté mondiale, la communauté est en droit d'avoir un accès universel à ce savoir et c'est la coopération des individus qui stimule la création de nouveaux savoirs. Est-ce qu'on pourrait considérer le hacking une espèce de „destruction créative" (J. Schumpeter) qui déclencherait „la veille anticipative" (H. Lesca) des organisations ou des personnes visées par l'activité des hackers? Sont-ils les anarchistes de la société postmoderne?

Mots-clés: culture, libre, hacking