BLOGGING CRIME

Lecturer **Adriana Iuliana STANCU**[1]

Abstract

The advantages of new technologies are successfully used not only for progress, but also for improving criminal activity. Cybercriminality is currently acquiring new dimensions, such as: increased organization degree of the groups activating in this crime field; greater degree of specialization and technical resources in view of committing crimes by these groups; diversification of operating scope, from card fraud and illegal card operations, to spreading pornographic material, software piracy, illegal accessing of computer systems, and to theft and illegal trafficking of confidential data and blog crime.

Keywords: *blog crime, cross-border character, cybercriminality.*

JEL Classification: K14, K24

1. Frauds, insults, defamations, threats, abetment to terrorism activities, sexual harassments and cyberattacks – on the blog

The Blog/Weblog[2] is defined as a website[3] organized as a hierarchy of texts, images, multimedia objects and/or data, arranged chronologically so that it may be viewed with a browser[4] that reads the HTML language; it is maintained by a person or group, being organized in reversed chronological order, the latest record being displayed first on the page; this hierarchy actually designates an on-line journal[5] or a web journal, but also a content management system (CMS) or an on-line publishing platform.

From a simple curiosity, the blogging fashion has currently become a thorny issue for both sociologists (going to pathological addiction) and law specialists as well.

There are countries where the simple blog might become the main evidence on the basis of which a person might be criminally convicted. For instance, a court from Alexandria (Egypt) condemned in 2007 a young Egyptian (Abdel Karim Suleiman – 22 years) to four years of imprisonment, because, through his personal blog, he allegedly offended Islam and President Hosni Mubarak. The counts consisted in eight materials he had posted on his blog in 2004, and the main arguments of the young man's defence invoked the right to freedom of speech. The trial was condemned by both Amnesty International and the "Reporters without borders".

The charges originating in blogs may easily turn into actual "witch-hunts". For instance, an American professor of history from the Kent State University of Ohio was charged by his colleague from the criminology chair for being behind an Islamic blog. Further to the scandal, even the head of the chair of the accused professor complained to the press about the death threats his Muslim colleague was receiving on the address of the Kent University. On the other hand, the advocates of the freedom of speech in the USA joined in the defence of the accused professor.

Still in the USA, at least half a dozen prosecutors have blogs[6], without being shy of admitting their identity or avoiding references to their daily work. The American prosecutors are protected by the First Amendment, which guarantees their right to freedom of speech like any other American citizens; this right is limited neither by the law of their professional status nor by the non-disclosure agreements (as the CIA members). For instance, an American prosecutor complains about the "cheap journalism" of a Californian publication. The day when a prosecutor uses blog evidence in a case in order to prove he/she and not the newspapers are right, seems very close.

---

[1] Iuliana Stancu - Faculty of Judicial, Social and Political Sciences, "Dunarea de Jos" University of Galati, Romania, adriana.tudorache@ugal.ro.

[2] Cristian Dinu*, Dicționar IT,* Cartea de buzunar Publishing House, Bucharest, 2006, p. 300 – 301.

[3] *Idem*, p. 300.

[4] *Ibidem*, p. 50.

[5] *Ibidem*, p. 191.

[6] www.sfgate.com, consulted on 1.10.2018.

Maybe that is why, a bill or court order definitively condemning prosecutors' blogging is to be expected in the USA.

Directive 2005/29/EC approved by the European Parliament and Council sets out to condemn companies having false blogs, also known as "flogs"[7] (for instance, they post under the identity of ordinary people while actually advertising online some hotels or restaurants, large stores or services suppliers). To this effect, UK announced they shall drastically sanction "misrepresentation as consumer", which has nothing to do with private, online journals, but are true "advertising tricks".

For instance, it was found that on the famous trip advice website, TripAdvisor.com and its blog (http://tripadvisor.typepad.com), certain tourists were actually owners advertising their own business (many times in bankruptcy) and compliment their own offers.

This directive could be integrated into the British legislation in order to refer to the Internet's online domain, which is still not fully regulated and source of many crimes. On the other hand, bloggers fear this practice could be extended on certain untrue postings belonging to regular citizens and not companies, not only in the UK but also in the remainder of the European Union.

Another delicate issue that starts taking shape in blogging is the sexual harassment or blog threatening. Actually, a blogger (Kathy Sierra) became the target of online attacks containing extremely dangerous threats (some included photos of her having a noose and a gag), while another blogger, single mother writing about raising a child alone, was threatened by a "cyber-addict". A writer who wrote on her blog about the pornography industry was threatened with rape. Unfortunately, such examples are not isolated but mark the beginning of a new trend in cybercrime, originating in the much easier possibility to hide the perpetrator's identity in this environment.

Specialty studies showed that women, who stand for almost half of the online community, are much more often victims of threats or harassments. A study on chatting from 2006 of the Maryland University indicated that women received 25 times more messages with explicit sexual content than men. As a result, many of the women having a blog "self-censure" by using pseudonyms, thus resulting into a reduction phenomenon of their online presence.

Internet defamation also moves to the blogosphere. In a similar manner to the press defamation, we are dealing with an extremely fine and controversial line between press liberty and freedom of speech on the one hand, and the right to private life on the other hand, with the obligation of proving one's assertions, this controversy moves in the virtual space as well. It will be interesting to see how the case-law will find a unitary answer to analysing online defamation cases by applying the classical rules, in the absence of a separate regulation for the Internet.

Internet defamation cases become more controversial and serious. For instance, Mahmood Al Yousif, owner of a popular English blog in Bahrain (www.malimodd.tv) a successful businessman, was accused that through his webpage he would have defamed the minister of agriculture. More precisely, he posted on his blog critical remarks regarding the activity of the Ministry of Agriculture and its minister during the 2006 winter floods. Mahmood was called to court on 8 May 2007 and by a special order, his blog was blocked. Mahmood invoked in mass-media a serious breach of human rights. His case is not unique. In Egypt, 13 bloggers were sued because of the critics addressed to the Mubarak regime.

As to the defamation and insult crimes perpetrated via the Internet, and especially via blogs, there is no worldwide, uniform legal approach. Yet, certain approaches started taking shape.

It appears that the first country in the world that wants to legally differentiate bloggers from journalists is Malaysia. The Malaysian minister, Zainuddin Maidin, states in the Malaysian daily The New Straits Times[8]: „There are fears that such blogs are used by calumny spreaders (...) and the classification (between "professionals" and "non-professionals")[9] shall facilitate the taking of measures against those breaking the country's laws. The minister's proposal might be substantiated in measures whereby only "professional" bloggers could be quoted by traditional mass-media, thus

[7] www.prweek.com - PR Week Magazine and www.timesonline.uk - The Times, consulted on 1.10.2018.
[8] www.nst.com, consulted on 1.10.2018.
[9] http://malaysia-today.net, consulted on 1.10.2018.

respecting the freedom to opinion of "non-professionals" who may not be quoted as sources. "Professionals" would have the legal responsibility to assume liability for the truthfulness of their postings, regardless of whether the blogger works in parallel for a newspaper or not. A "professional" blogger might be prosecuted if he/she broke the law.

This distinction between "professionals" and "non-professionals" does not guarantee objectivity. A "professional" might purposely publish fake news by hiding his IP while a "non-professional" might have real and exclusive sources. The issue of qualifying information sources on a blog remains controversial, since many blog owners fear a political restriction of the blogosphere. An increase of blog defamation cases going to trial has been noticed worldwide, because the virtual space is public space by excellence.

Sometimes, these defamations received civil sanctions, such as the case of the French language professor who received a 1,000-Euro fine for using his blog in order to defame his former headmistress. In France, this case was commented by a lawyer for Le Monde, concluding that a person may write whatever he/she wants in an intimate/private journal, but on a blog, he/she assumes the "liability of an editor on the publishing moment" (Le monde). Such a blogger would be legally liable, as an editor, even if he/she does not fill this position in its economic-traditional sense. In the states where the "cascading liability" principle operates, the first to bear the liability is the website editor or the blogger himself/herself, then, if the same is anonymous, the server host or even the internet provider.

According to a decision of the US Supreme Court (quoted by Le Monde as well), it was ruled that the person republishing a fact, even a defamatory one (originating in mass-media or other websites), cannot be held liable for calumny. The victim must identify the primary calumny author and go against him/her. The decision was grounded on the fact that the federal laws cannot allow calumny liability sharing between the main author and the one subsequently distributing the information.

The Communications Decency Act of 1996 offers total immunity against calumny trials to those persons publishing information taken over from other sources via the Internet. Only the United States Congress may rule the review of the current legislation.

Nevertheless, it appears that the majority of the legal opinions in the USA support the fact that individual bloggers should be suable for purposeful republishing of a calumny. To this effect, a law amendment by the Congress is expected.

The issue of the new technologies against the right to freedom of speech[10], as an essential personal right, remains controversial both legally and morally.

2. Transforming a blog into a cyberattack gate

Generally speaking, blogs are interactive, providing amateur readers with the possibility to post their own comments besides the blogger's. There have been cases when behind an apparently harmless post a malicious code (virus, worm, trojan etc.) was hidden, which in reality "stole" email addresses and even passwords of that blog's visitors. The stolen data was used in the most varied purposes, going from socially moderate crimes to computer crimes having a high social danger.

As to these new types of cyberattacks, the best solution is to secure blogs. To this effect, two situations occur:

I. The blogger called to a company or specialist to host his online journal (the blogger only updating the content) or

II. The blogger, having advanced web knowledge, administers on his/her own his/her blog on a server.

In the first case, Gecad experts recommend the following measures:

- choose a hosting services provider who could ensure blog security measures against cyberattacks that might bring prejudices;

[10] S. Davies, „*Big Brother: Britain's Web of Surveillance and the New Technological Order*", London, Pan Book, 1996, p. 10 et seq.

- the blog administration password should be complex (both small and capital letters, figures and special characters);

- blog protection against automatic posting of unwanted comments or spam (protection can be achieved by CAPTCHA – cases where various figures and letters are written, which the visiting poster should introduce before adding content);

- the blog owner should not forget to close the update content session (by log out/off), especially if this operation is performed in public spaces such as internet cafes or hot spots.

In the second case, the blogger buys from a provider only the server space[11], but he/she needs to take additional safety measures:

1) to use the latest versions of the blog platform (PHP[12], MySQL etc.), because hackers can speculate certain vulnerabilities, accompanied by the adequate configuration of the used software;
2) to develop the application the blog is built on (blogware) with the maximum security level, in order to avoid "SQL injections" (when a visitor, instead of a comment, inserts a script through which he/she could find out other email addresses and passwords;
3) to filter all inputs (filtering other files than the administrator's files);
4) to use widespread blog applications that are well monitored from the security point of view.

It's an already known fact that potential attackers prefer focusing on a company rather than a home-user, but any attack may lead to damages, if not material, at least image damages.

Bibliography

1. Cristian Dinu, *Dicționar IT, Cartea de buzunar* Publishing House, Bucharest, 2006.
2. S. Davies, „*Big Brother: Britain's Web of Surveillance and the New Technological Order*", London, Pan Book, 1996.
3. http://malaysia-today.net, consulted on 1.10.2018.
4. www.prweek.com, consulted on 1.10.2018.
5. www.sfgate.com, consulted on 1.10.2018.
6. www.timesonline.uk, consulted on 1.10.2018.
7. www.nst.com, consulted on 1.10.2018.

[11] Cristian Dinu, *op. cit.*, p. 250.
[12] *Idem*, p. 205.