Argument Regarding the Need to Incriminate Computer Data Input Forgery Committed by an Official

Dr. Bogdan Bodea[1]

Abstract

As digital format becomes a necessity, public authorities need to adapt to this concept and the law must follow. Up until now, authorities kept different records in a written form and they conducted their activity exclusively in writing, as the written form provided both certainty of the existence of the act and of its content.

The incrimination under art 325 falls short in offering adequate protection of public confidence in the authenticity of digital documents and the veracity of stipulations recorded in them, as it does not sanction the act of inputting false data committed by a public official acting within his right to input data.

Keywords: *Computer data, forgery, acting without right, fraudulent, public official*

I. General Considerations Regarding the Need to Protect New Social Values

The Global pandemic of 2020 has taken its toll on society through digitalization. More and more we see that working online or in a digital format becomes a necessity, and public authorities need to adapt to this concept.

Nevertheless, in some areas, the law falls short as traditionally all the work of public authorities was done in writing. Up until now such authorities kept different records in a written form and they conducted their activity exclusively in writing, as the written form provided both certainty of the existence of the act and of its content.

Times are changing fast and we believe that they would have changed regardless of the current crisis, as more and more authorities embrace the need of digitalization and as more and more people are accustomed to use modern means of communication on a daily basis.

The technology enters our lives and therefore changes our behaviour thus creating the need to protect new social values, as they arise. In this context, considering the transition from non-digital to digital it proves necessary to incriminate new offences such as data forgery[2]. As society fights cybercrime, such incriminations must be uniform, given the transboundary nature of the offences[3].

Nevertheless, we argue that the Romanian Criminal Code falls short in offering adequate protection, in light of recent cases. We are going to take into consideration

[1] Lecturer, *University of Oradea, Faculty of law.* Contact: avocatbodea@yahoo.com.

[2] S. Bogdan, D.A. Șerban, G. Zlati, *Noul Cod penal. Partea specială. Analiză, explicații, comentarii. Perspectiva Clujeană (New Criminal Code. Special Part. Analysis, explanations, comments. Cluj Perspective),* Ed. Universul Juridic, Bucharest, 2014, p. 557.

[3] C. Miheș, *Infracțiuni informatice: reglementare și investigare (Cybercrime: regulations and investigation)*, Ed. Universității din Oradea, Oradea, 2007, p. 9.

the necessity of incriminating computer data input forgery committed by a public official, a necessity that arose from a case we argued in front of the Romanian Courts.

II. The Point of Origin

On the 28th of April 2020 the prosecutors accused two border policemen of falsely inputting in the border police computer system data they knew not to be real.

The circumstances of the case regarded the situation of Romanian citizens entering the national territory and declaring that they were lorry or truck drivers, which they weren't, a fact easily verifiable by checking the driver's license.

New regulations adopted in the context of the pandemic crisis stipulated that a person, when entering Romania, needs to give a written statement in front of the border policeman in which they have to declare whether or not they have specific symptoms of COVID 19, the place of departure and several other data[4]. They are placed in quarantine, in certain designated places, under police and military supervision.

Under the provisions of art. 4 of Military Order no. 1[5] as supplemented by art. 9 of Military Order no. 2[6], truck and lorry drivers are exempt from the measure of quarantine if they are entering the Romanian territory. They are placed in self-isolation in their homes or in arranged spaces provided by their company or by local authorities. Therefore, some of the people entering Romania thought it better to declare themselves to be lorry drivers in order to avoid the measure of quarantine, mandatory for all other persons that crossed the Romanian border.

In this context 4 individuals who later became denouncers stated in front of border police that they were lorry drivers working in a member state of the EU, and therefore asked to be placed in self-isolation in their own homes.

Leaving aside the debate whether or not the idea came from the border police officer or form the four persons, given the fact that such a debate has to take place in front of the courts and needs to be supported by evidence, we are interested more in the theoretical aspect of the false computer data inputting, working under the presumption that the public official knows that the data he is going to enter into a digital record is false.

The prosecutor office argued that such an input of false data represents the offence of computer forgery stipulated by the Romanian Criminal Code under article 325 NCC[7]. This article incriminates the act of entering, modifying or deleting, without right, computer data or restricting, without right, the access to such data, resulting in data that is untrue, if the crime is committed for using such data to produce legal consequence.

---

[4] Art. 1 par. (2) of the Order no. 414/11 March 2020 of the Health Minister published in Official Gazette, Part I, no. 201 of 12 march 2020 stipulated that: The institutionalized quarantine measure will be imposed on asymptomatic persons entering the territory of Romania coming from the areas with extended community transmission affected by COVID-19 (red zone), for a period of 14 days, in specially arranged spaces provided by local authorities. This order was subsequently amended by Order no. 622/2020 for amending and supplementing the Order of the Minister of Health no. 414/2020 published in the Official Gazette, Part I, no. 315 of April 15, 2020.

[5] Published in Official Gazette, Part I, no. 219 of 18 March 2020.

[6] Published in Official Gazette, Part I, no. 232 of 21 March 2020.

[7] The Romanian New Criminal Code (NCC) was adopted was published and enter into effect on 01.02.2014.

III. The Interpretation of the Provisions of art. 325 NCC

The prosecutor argued that by inputting false data the public official acted "without right" in the sense of the incrimination, given the fact that he has the right to input only data he knows to be true.

Although the case is not yet judged in the arrest proposal that followed the charges, we have fought the charges on the grounds that the incrimination relates to a deed committed without right and in this case the border policeman had not only the right but the obligation to input that data, whether or not he knows it to be true or false.

The Court embraced our opinion and rejected the arrest proposal relating to this accusation on the grounds that the border policemen acted within their right entering the data.

In the Romanian doctrine the offence incriminated under art 325 NCC is presented to be a correlative incrimination to document forgery incriminated under articles 320 and 321 NCC committed in regard to computer data[8] a fact deduced even in relation to the placement of the text in the criminal code among forgery offenses[9].

In fact, under previous legislation[10] the incrimination was identical and derived from the obligation assumed by Romania in accordance with the European Convention on Cybercrime adopted in Budapest on 23 November 2001[11] to incriminate entering, altering, deleting or restricting access to computer data without right.

The legislator opted for a separate incrimination in respect to document forgery, although in France such an action that translates into a data forgery falls within the offence of forgery regulated by article 441.1 French Criminal Code. The French Supreme Court stipulated that modifying computer data in a manner similar to a document is incriminated under this article[12].

The legislator felt compelled to incriminate this offence in order to protect a new social value that is to protect public confidence in the authenticity of digital documents and the veracity of stipulations recorded in them[13] as the crime of illegal

---

[8] S. Bogdan, D.A. Şerban, G. Zlati, *cited above,* p. 559; C. Rotaru, A.-R. Trandafir, V. Cioclei, *Drept penal. Partea Specială II* (*Criminal Law. Special Part.*) Ed. C.H. Beck, Bucharest, 2020, p. 410, G. Antoniu, T. Toader, V. Brutaru, S. Daneş, C. Duvac, I. Griga, I. Ifrim, G. Ivan, G. Paraschiv, I. Pascu, I. Rusu, M. Safta, I. Tănăsescu, T. Toader, I. Vasiu, *Explicaţiile Noul Cod penal Comentat. Vol. IV –art. 257-366 (Explinations of the New Criminal Code. Vol. IV –art. 257-366),* Ed. Universul Juridic, Bucharest, 2016, p. 547.

[9] V. Dobrinoiu, I. Pascu, M.A. Hotca, I. Chiş, M. Gorunescu, C. Păun, M. Dobrinoiu, N. Neagu *Noul Cod penal Comentat. Vol. II – Partea specială. (New Criminal Code Commented. Vol II. Special Part),* Ed. Universul Juridic, Bucharest, 2012, p. 722.

[10] Article 48 of Law 161/2003 regarding measures to ensure transparency in the exercise of public dignity, public office and in the business environment, prevention and sanctioning of corruption stated: *The act of entering, modifying or deleting, without right, computer data or of restricting, without right, the access to these data, resulting in data untrue, in order to be used in order to produce a legal consequence, constitutes a crime and is punished with imprisonment from 2 to 7 years*.

[11] Ratified through Law no. 64/2004 published in Official Gazette, Part I, no. 343 of 20 April 2004.

[12] see the Decision from 21st of January 2001 in *Bulletin criminal,* apud. G. Zlati, *Unele aspecte în legătură cu infracţiunile informatice din perspectiva legislaţiei în vigoare precum şi a noului cod penal* în Revista Dreptul, nr. 10/2012 (*Some aspects related to computer crimes from the perspective of the legislation in force as well as the new criminal code* in Law Magazine, no. 10/2012) p. 212. The situation is the same in the Dutch criminal system.

[13] S. Bogdan, D.A. Şerban, G. Zlati, *cited above,* p. 558.

accessing of computer data incriminated under art. 362 NCC[14] did not offer sufficient protection.

In conclusion the majority of the doctrine[15] considered this incrimination to be a translation in respect to digital data of both criminal conducts relating to documents, and although stipulating that the action must be done without right, did not stop to analyse this condition in detail with the exception of a reference to the art. 35, paragraph (2) of Law no. 161/2003[16].

IV. Our Perspective and Arguments for the Need of Incriminating a New Offence

We argue that the current incrimination does not cover the input of false data by an official that has the right to access or input such data.

Article 35 paragraph (2) of law no. 161/2003 defines, the person who acts without right as the person who:

a) is not authorized under the law or a contract;

b) exceeds the authorization limits;

c) does not have the permission, from the competent natural or legal person, according to the law, to grant it, to use, manage or control a computer system or to carry out scientific research or to perform any other operation in a computer system.

A person *not authorized* by law or contract is a person who acts without any authorization, a subject that could not, in a legal manner, enter, modify or delete data stored on a computer. This is the case of a particular lacking any authorization, for instance in our example the 4 men trying to cross the Romanian border.

A person who *exceeds the authorization limits* is a person that has an authorization but acts above its clearance. For instance, if there are different levels of security, entering, modifying or deleting data by the person who has a lower access level falls within this incrimination. A person acting within the limits of authorization or clearance (for instance the one that has the right to input such data) cannot commit this offence. Of course, we will not argue that false data are authorized to be inputted, but in general terms, in this case the authorization refers to levels of clearance given, in respect to the nature of the data. Following the reasoning of the legislator, we argue that under letter a) the subject has no authorization and under letter b) the authorization is insufficient.

A person that *does not have the permission* under letter c) is a person that acts without a consent given by the entitled entity, the distinction to the letter a) being that such a right can be given in an informal manner not through an authorization, for instance in the case of a system not protected by password.

---

[14] A similar incrimination in the French Criminal Code is article 323 paragraph 3 that stipulates that fraudulent introduction, deleting or modifying data stored in a computer system constitutes an offence. A distinction is however obvious in the case of the Romanian law as the text still refers to an act done "without right" whereas the French law incriminates fraudulent actions against computer data G. Zlati, *cited above,* page 215.

[15] Including ourselves, see R. Bodea, B. Bodea, *Drept Penal. Partea Specială* (*Criminal Law. Special Part*) Ed. Hamangiu, Bucharest, 2018, p. 513.

[16] C.Rotaru, A.-R. Trandafir, V.Cioclei, *cited above,* p. 411; A. Maxim, *Falsul şi frauda informatică* în Caiete de Drept penal nr. 3/2011 (*Forgery and Computer fraud* in Criminal Law Writings, no. 3/2011), p. 62.

In respect to article 325 NCC we think that through the way the text describes the offence, first of all there needs to be an act of accessing or restricting data *without right* that causes an alteration of the data and renders them untrue[17]. Thus, the incrimination does not cover the situation in which the policeman or any public official for that matter acts intentionally and within his own right inputting false data.

The same opinion was embraced by the Court. Although judge of rights and liberties retained from postulating opinions regarding the typical character of the deed (as it is the attribute of the trial judge to decide whether or not this type of act can be treated as the offence of computer forgery) the proposal was rejected, the judge emphasizing of the lack of the sufficient accuracy regarding the legal framework applicable, insisting upon the existing authorization, as the border policeman had the obligation to input data.

As we have shown, some authors argue that by incriminating this offence the legislator wanted to sanction the corresponding action of the perpetrator in relation to the forgery offence of a written document, either by counterfeiting it or by alteration. In exemplifying the content of the norm, the authors argue that introduction of data resulting in creating the forge electronic document is sanctioned by article 325 criminal code and modifying an existing document falls under the alteration of such an electronic document of electronic data[18].

Even if we agree that this was the intention of the legislator, we cannot stumble upon the end result. Respecting the idea that the public official cannot by himself enter in good faith data he knows to be false and such a conduct must be prohibited we think that such prohibition is not imposed through article 325 NCC.

First of all, the law does not define the active subject of this incrimination. Indeed, it does not require a special capacity, therefore allowing any person that commits such an act to be punished according to the law, including, in our case the four people that tried to cross the border. The way the text is stipulated tends to incriminate the act of a *foreigner in respect to that system* (a person who has no or insufficient access to such data and that without right enters data to modify the content of the electronic document), whether or not he is a public official.

On one hand, it is true that a public official can commit the offence, *if he has no right*. But we think it would be better if there was a distinction between a stranger and a specialized subject acting without right, in correspondence with forging documents done by a private individual or a public official. This distinction is needed because in most cases persons having a special capacity (for instance a public official) can have an easier physical access to the system (even though they are not authorized or are exceeding the level of authorization). Furthermore, given the nature of their occupation, that involves exercising public authority they should restrain themselves further.

On the other hand, the law needs to cover the situation in which the person *has the right* but opts for inputting forged data. In such a case, despite of any of the legislator's intention, the person who has access to such data cannot be sanctioned, as

---

[17] In the Italian criminal system, the usage of the term "without right" is limited to computer fraud sanctioned under art. 640 (ter.) of the Italian Criminal code; it is placed in correlation with the expression "in any way" and relates to any form of intervention different from the act of alteration of the functioning of computer systems. See F. Mantovani, *Dirrito Penale. Parte Speciale II Seconda edizione (Criminal Law. Special Part II Second edition)*, Ed. Wolters Kluwer – Cedam, Milano, 2018, p. 233.

[18] see S. Bogdan, D.A. Şerban, G. Zlati, *cited above,* p. 559.

his action does not fall within 360 NCC (illegal access to a computer system)[19], art 362 NCC (alteration of computer data integrity)[20] or any other offense against the security and integrity of computer systems and data.

Another interpretation is possible: that such act should fall under art 321 NCC. But that would represent an analogy against the defendant, prohibited as a concept by the constant jurisprudence of the European Court of Human Rights regarding art. 7 of the Convention[21] as the text in question explicitly refers to written official documents.

Therefore recognizing the need to protect computer data or the content of such data even from the persons that have the right to access them, but do so with in ill-faith, the need of incriminating a special crime designated to sanction the deed done by the person who has the right to alter, input or delete such data arises.

Although we could argue the need to re-formulate the text of art 325, we think it is best to set up a new incrimination under paragraph 2 that sanctions the act of inputting false data or fraudulent modifying or deleting data in a manner that alters the content of the electronic data and renders them to be false by the person who has proper authorization. This way paragraph 1 will protect the value against offenders acting without authorization and paragraph 2 against offenders acting with authorization. The Italian legislator had an even wider approach, incriminating under art. 491 (bis) any type of forgery sanctioned by Title VII, Chapter III of the Italian Criminal Code committed in respect to an official digital document. This approach rendered all debates useless as the doctrine insists only upon differences between different types of forgery[22].

If we were to argue that entering data without right means entering false data, like the prosecutor did, we think that there will be an issue regarding the unforeseeable content of the incrimination, due to the way in which the misconduct is described: it refers to an active subject that does not have the *right* of acting in the manner prescribed by law. Therefore, by exclusion if he has such right, the general interpretation of the incrimination is that he cannot commit such a crime.

The prosecutor`s thesis is dangerous seen through another example: if the agent is acting *within his right* inputting *true data* but in a manner that alters the end result, thus creating a legal consequence. Continuing the prosecutor`s reasoning this action would be sanctioned too, as acting without right would mean any improper usage of his right to input data, and would suppress any misconduct of the agent in fulfilling his attributions weather or not they are prescribed by law, an interior order, a work instruction or a recommendation. We cannot accept this thesis as it is simpler and clearer to incriminate the fraudulent inputting false data. In relation to this concept we emphasize that in the UK criminal system it is considered that an instrument is false if it purports to be something it is not or if it 'tells a lie' about its own authorship, origins or history[23].

---

[19] Art. 360 NCC incriminates the unauthorized access to a computer system, but as we have seen the offender is authorized to access the system.

[20] Art. 362 NCC incriminates the act of modifying, deleting or damaging computer data or restricting access to this data, without right. A similar incrimination that also refers to an unrightful act.

[21] See F. Streteanu, *Tratat de drept penal. Partea Generală* (*Criminal law treatise. General Part*), Ed. C. H. Beck, Bucharest, 2008 p. 48.

[22] S. Preziosi in A. Fiorela (a cura di) *Questioni fondamentali della parte speciale del diritto penale. Terza edizione* (*Fundamental issues regarding the special part of criminal law. Third edition*), Ed. G. Giappichelli, Torino, 2019, p. 607-650.

[23] See H.r.l.j. H.D. Ormerod (General editor) *Blackstone`s Criminal Practice*, Oxford University press, 2012, p. 476.

V. Conclusions and *de Lege Ferenda* Proposals

As a conclusion the need to protect public confidence in the authenticity of digital documents and the veracity of stipulations recorded in them is undisputed. Article 325 NCC responds to this need in relation to subjects acting without right. We think that the text should be left untouched and a new incrimination should follow in the same article under paragraph (2) sanctioning the act of inputting false data or fraudulent modifying or deleting data in a manner that alters the content of the electronic data and renders them to be false, by the person who has the proper authorization.

Furthermore we would argue for a separate new aggravated incrimination under a proposed paragraph (3), that sanctions the act stipulated in paragraph (1), committed a public official that acts *without right*, a distinction that should be made in a similar manner to the one made in relation to forgery of written documents.

References

1. Antoniu, G. *et.all., Explicațiile Noul Cod penal Comentat. Vol. IV – art. 257-366 (Explanations of the New Criminal Code. Vol. IV – art. 257-366),* Ed. Universul Juridic, Bucharest, 2016.

2. Bodea, R., Bodea, B., *Drept Penal. Partea Specială* (*Criminal Law. Special Part*) Ed. Hamangiu, Bucharest, 2018.

3. Bogdan, S., Şerban, D.A., Zlati, G., *Noul Cod penal. Partea specială. Analiză, explicații, comentarii. Perspectiva Clujeană (New Criminal Code. Special Part. Analysis, explanations, comments. Cluj Perspective),* Ed. Universul Juridic, Bucharest, 2014.

4. Dobrinoiu, V. *et.all., Noul Cod penal Comentat. Vol. II – Partea specială. (New Criminal Code Commented. Vol II. Special Part),* Ed. Universul Juridic, Bucharest, 2012.

5. Mantovani, F., *Dirrito Penale. Parte Speciale II Seconda edizione (Criminal Law. Special Part II Second edition)*, ed. Wolters Kluwer – Cedam, Milano, 2018.

6. Maxim, A., *Falsul și frauda informatică* în Caiete de Drept penal nr. 3/2011 (*Forgery and Computer fraud* in Criminal Law Writings, no. 3/2011).

7. Miheş, C., *Infracțiuni informatice: reglementare și investigare (Cybercrime: regulations and investigation)* ed. Universității din Oradea, Oradea, 2007.

8. H.r.l.j. H.D. Ormerod (General editor) *Blackstone`s Criminal Practice*, Oxford University press, 2012.

9. Preziosi, S. in Fiorela, A. (a cura di) *Questioni fondamentali della parte speciale del diritto penale*. *Terza edizione* (*Fundamental issues regarding the special part of criminal law. Third edition*), Ed. G. Giappichelli, Torino, 2019.

10. Rotaru, C., Trandafir, A.-R., Cioclei, V., *Drept penal. Partea Specială II* (*Criminal Law. Special Part*), Ed. C. H. Beck, Bucharest, 2020.

11. Streteanu, F., *Tratat de drept penal. Partea Generală* (*Criminal law treatise. General Part*), Ed. C. H. Beck, Bucharest, 2008.

12. Zlati, G., *Unele aspecte în legătură cu infracțiunile informatice din perspectiva legislației în vigoare precum și a noului cod penal* in Revista Dreptul, nr. 10/2012 (*Some aspects related to computer crimes from the perspective of the legislation in force as well as the new criminal code* in Law Magazine, no. 10/2012).