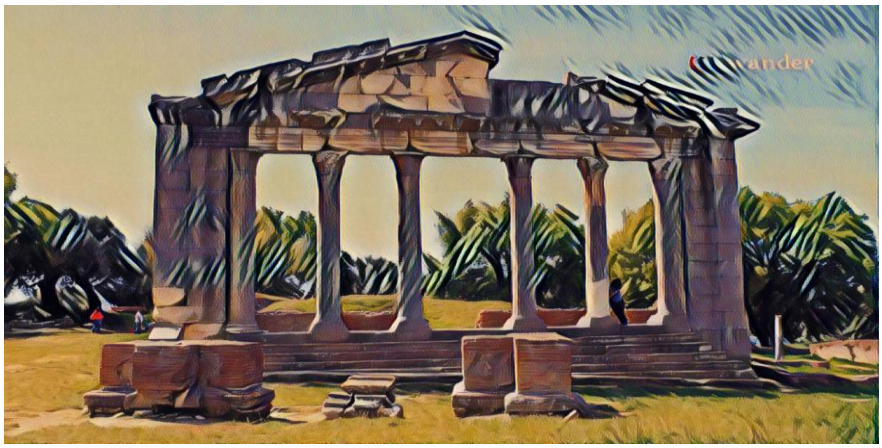
ILLYRIUS

ISSN 2225-2894

International Scientific Review / n. 18 / (I-2022)



Scientific Directors:

Ersi Bozheku – Giorgio Spangher

SPECIAL EDITION
"LEGAL CHALLENGES IN THE DIGITAL ERA"
Essays

edited by
Dorina Hoxha, Jonida Milaj-Weishaar, Ersi Bozheku

In collaboration with

Albanian National Group
Collective Members of Kosovo

Roma – Tirana – Prishtina

Price: 7 euro

Illyrius
International Scientific Review
ISSN 2225-2894

Full Professor of Criminal Law, Dean of Law Faculty, University of Prishtina – Kosovo / Honorary President of '"Association Internationale de Droit Pénal" – Albanian National Group and Collective Members of Kosovo, united in AIDP – Albanian People Group

Prof. Dr. Avv. Ali Abukar Hayo
Professore Ordinario di Diritto Penale, Università di Mogadiscio

Prof. Dr. Mejdi Bektashi
Full Professor of Economics, Vice-Dean of Law Faculty, University of Prishtina – Kosovo

Prof. Assoc. Dr. Avv. Marco Gambardella
Professore Associato di Diritto Penale, "Sapienza" Università di Roma

Prof.assoc. Klodian Skenderaj
Associate Professor of Criminal Procedure Law Faculty of Law, University of Tirana

Prof. Assoc. Dr. Luigi Cornacchia
Professore Associato di Diritto Penale, Università del Salento

Prof. Assoc. Dr. Cristiano Cupelli
Professore Associato di Diritto Penale, Università degli Studi Tor Vergata di Roma

Prof.assoc. Dr. Mirela Bogdani
Associate Professor of Human Rights, Faculty of Law, University of Tirana

Prof. Assoc. Dr. Avv. Nicola Selvaggi
Professore Associato di Diritto penale, Università Mediterranea di Regio Calabria

Prof. Assoc. Dr. Angelo Lalli
Professore Associato di Diritto Amministrativo, "Sapienza" Università di Roma

Prof. Assoc. Dr. Federica Botti
Professore Associato di Diritto Ecclesiastico, Università di Bologna Alma Mater Studiorum

Prof. Assoc. Dr. Fabio Piluso
Professore Associato di Economia degli Intermediari Finanziari, Università della Calabria.

Prof. Assoc. Dr. Andrea Carteny,
Professore Associato di Storia Europa Orientale, "Sapienza" Università di Roma / Direttore del CEMAS Sapienza Università di Roma

Prof. Assoc. Dr. Pasquale Bronzo
Professore Associato di Diritto Processuale Penale, "Sapienza" Università di Roma

Prof. Assoc. Dr. Roberto Flor
Professore Associato di diritto penale dell'Economia, Università di Verona

Prof. Assoc. Dr. Dorina Hoxha
Associate Professor of Criminal Law / Dean of the Faculty of Law, University of Tirana

Prof. Straord. Dr Avv. Giuseppe Saccone
Professore Straordinario di Diritto Processuale Penale, Università "Pegaso" di Napoli

Prof. Straord. Dr. Marco Margarita
Professore Straordinario di Diritto Tributario, Università degli Studi eCampus

Prof. Straord. Dr. Roberto Russo
Professore Straordinario di Diritto Costituzionale, Università degli Studi eCampus

Prof. Aggr. Dr. Avv. Giovanni Stile
Ricercatore, Professore Aggregato di "Economia e Criminalità", Seconda Università degli Studi di Napoli

Prof. Aggr. Dr. Simone Manfredi
Ricercatore, Professore Aggregato di Economia Aziendale, Università degli Studi di Cassino e del Lazio Meridionale

Prof. Aggr. Dr. Marco Cilento
Ricercatore, Professore Aggregato di Sociologia. Direttore del Corso di Laurea in Cooperazione Internazionale e Sviluppo, Sapienza Università di Roma

Prof. Aggr. Dr. Gabriele Natalizia
Ricercatore, Professore Aggregato di Scienza Politica alla Link University – Roma

Dr. Erjon Muharremaj
Docent of International Criminal Law, Faculty of Law, University of Tirana

Dr. Redi Shtino
Già - Vice Ministro dell'Istruzione della Repubblica d'Albania

Cons. Luca Ramacci
Consigliere presso la Suprema Corte di Cassazione

Cons. Eugenio Selvaggi †
Sostituto Procuratore Generale presso la Suprema Corte di Cassazione

Cons. Francesco Brugaletta
Magistrato del Tribunale Amministrativo Regionale (T.A.R.) di Catania / Presidente di Sezione della Commissione Tributaria

Cons. Rosario Aitala
Magistrato. Consigliere del Ministro degli Esteri per le aree di crisi e la criminalità internazionale

Cons. Luigi Pacifici
Magistrato. Sostituto Procuratore della Repubblica presso il Tribunale di Tivoli

Cons. Valerio De Gioia

Magistrato. Giudice presso la Prima Sezione Penale del Tribunale di Roma.

Chief Editors

Editorial and Administrative Responsibles

ISSN 2225-2894

Review of CESIAL – Italo-Albanian Center of Studies, High Formation and Researches of CEMAS "Sapienza" Università di Roma

Reviste e CESIAL – Qendra e Studimeve, Formimit te Larte dhe Kerkimeve Italo-Shqiptare e CEMAS "Sapienza" Universiteti i Romes.

Rivista del CESIAL – Centro Studi, Alta Formazione e Ricerca Italo-Albanese del CEMAS "Sapienza" Univeristà di Roma.

*This review is published twice-yearly and adopts a **double blind peer review** procedure for evaluation ad acceptance.*

*Kjo revistë del në shtyp me një frekuence semestrale dhe përdor procedurat e vlerësimit dhe të pranimit **double blind peer review***

*Rivista avente periodicità semestrale che si avvale della procedura di valutazione e accettazione **double blind peer review***

Ethical code

Illyrius
International Scientific Review
ISSN 2225 – 2894

Introduction
Illyrius is a double blind peer reviewed international research journal aiming to publish qualitative research in the following fields. Its purpose is to act as a meeting place to encourage the sharing of experiences between scholars belonging to different geographical areas and who, thanks to their cultural peculiarities, can contribute to a productive and continuous exchange of scientific and didactic knowledge. In this perspective, the journal is open to welcome contributions from scholars from all over the world on topics such as law, economics, sociology, political sciences, security sciences, international cooperation, communication sciences.
The Illyrius is published by the Italo-Albanian Center of Studies, High Formation and Researches CESIAL of CEMAS "Sapienza" Università di Roma and edited by its components.
Illyrius follows all the standards and best practice guidelines established in the European Charter for Researchers applicable to researchers as well as all the ethical norms and rules established in The European Code of Conduct for Research Integrity . Thus, this Code shall be interpreted in correlation with these legal documents.
This Code aims to disseminate within the academic scholars the values of legality, solidarity, impartiality, as well as aims to apply the principle of equity by reviewing all the contributions through a fair review process based on – at least – two different binding evaluations. In the case of disagreement between them, a third reviewer will be asked.

Research Integrity
Illyrius applies the same standards of integrity applied at the European Charter for Researchers, the European Code of Conduct for Research Integrity.
Authors submitting papers in Illyrius shall apply professional responsibility and the ethical practice. In other words, they shall be aware of the strategic goals of their particular fields. In addition, authors submitting their scientific contributions to Illyrius shall guarantee that their research is relevant for the members of the community by also advancing the current state of the art. Moreover, and more importantly, they shall not infringe the rules of plagiarism and shall not duplicate research carried out or published elsewhere by others or themselves (see Section Plagiarism and Duplication and Redundant Publication (Self-Plagiarism)). In the case of data processing, the data shall be original or explicitly quoted. Additionally, methods of collection and evaluations of the data shall be disclosed, and authors shall not modify them by being honest in reporting the data in a fair, full and unbiased way by also respecting their colleagues, without applying any type of discrimination. Additionally, their research shall be disseminated and exploited according to their personal contractual arrangements. Furthermore, if the work is delegated, authors of the contribution submitted ensure that the person working on them has the competence to carry it out. Last, but not least, the rules regarding intellectual property rights – especially in the case of joint work – shall be respected, also based on the individual agreement between the authors.
Therefore, between others, some of the most important ethical principles that the authors submitting contributions at Illyrius are:
Professional responsibility
Accountability
Professional attitude
Reliability in ensuring the quality of research through the application of design, methodology and analysis and use of resources approved by academia
Honesty in research through the application of the principle of transparency and impartiality
Respect of colleagues as well as research environment and cultural heritage
Application of the principle of equity between all members of the academic community without any type of direct or indirect discrimination based on religion, sex, gender, political or sexual orientation, personal convictions, ethnicity, citizenship, look, language or other types of discriminations since these are only few of the cases and do not exhaustive all of them.
Application of the rules of intellectual property rights

Composition of the board of the journal: their activities and responsibilities.
The scientific directors: take care of the organizational aspects of the journal and its scientific profile. Together with the scientific committee they draw up its guidelines. They decide on eidtorial activities, identify the peer reviewers, maintain relationships with the chief editors and administrative managers. They take the decisions on the articles in the terms which will be discussed below.
The scientific committee: is made up of important figures from the world of science and is the body that carries out the journal's scientific addressing activity. The same indicates to the scientific directors the scientific criteria to be adopted and shares with them the guidelines that the journal will have to follow. The scientific committee evaluates the quality of the journal's activities, offering its own suggestions. Its members may at any time ask the scientific directors for information on the progress of the journal as well as any other useful information and offer their suggestions to the scientific directors. They propose scientific articles for publication. The members of the scientific committee are ex officio peer reviewers, that the scientific directors must contact for the anonymous control of the quality of the manuscripts, taking into account the professional profile of the individual member. They take the decisions on the articles in the terms which will be discussed below.
Editors in chief: In agreement with the scientific directors, they follow the editorial activities of the journal. They take the decisions on the articles in the terms which will be discussed below.

Editorial and Administrative Responsibles: take care of the management of the site and of the practical and administrative aspects of the magazine. They manage the email and other communication channels, following the instructions of the scientific directors and editors in chief.

Editorial Process

All authors are guaranteed that the Illyrius applies editorial independence. The journalaims to prevent any type of conflicting interests, fear, or any type of influence coming from corporates, businesses or political parties or other actors. Illyrius is committed to increase diversity, promote inclusion and quality at every state of the publishing process. We support submission from scholars of diverse socio-economic backgrounds and especially woman scholars. The application of the equity principle means that the editorial board does not discriminate, between others, based on race, ethnicity, citizenship, gender, sex, sexual orientation, religion, disability, look, or personal convictions or other reasons.

The decision is based on pure merits of the scholars.The Scientific Directors, the Scientific Committeee and the Editors in Chief decide if the manuscript applies all the ethical standards as well as potentially include academic results that enhances the state of the art of that particular field of research.

The Scientific Directors, the Scientific Committee and the Editors in Chief do not discriminate authors on their personal characteristics as well as on the content of the work, if the scientific work applies all the academic ethical principles.

In particular, the editorial decisions on the scientific contribution submitted to our journal are done based on the anonymous peer review reports, which have a unified format. Before sending to the peer reviewers, previous steps are followed. First, **Editorial and Administrative Responsibles** checks if the contribution submitted follows all the formal criterias for the submission established by the Journal. Second, one of the Editors in Chief reviews if the contribution follows the scope of the journal. Third, the Editor in Chief communicates with a Scientific Directors in order to promote a quick review of the quality. The Scientific Directors make an assessment of the perceived level of qualitative research work, a check on the presence of plagiarism or self-plagiarism parts with technological tools in thier equipment (compilatio system), and suggest either rejection of the manuscript or decide for the review process. If the final decision is that the manuscript does not follow the style of the journal, or does not analyze one of the topics within the scope of the Journal, or the contribution does not pass the plagiarism or self-plagiarism test, or the manuscript is not with a good quality, a quick decision is done and the corresponding author is informed by the editorial and administrative responsibiles using the mail contact editor@illyrius.eu. The Scientific Directors can also delegate this activity to a member of the scientific committee. The delegate comunicates whitin 3 (three) days the result to the Scientific Directors and can not assume the quality of peer reviewer.

During the pre-review phase, which shall be done within two week, the Scientific Directors, or their delegate, will consider the following questions:

Does the contribution fit within the scope of the journal and also applies the same style and formatting and policy requirements of the journal?

Is the contribution without plagiarism or self-plagiarism?

At first reading, the manuscript offers an adequate scientific and methodological level?

If the pre-assessment is positive, the manuscript will be reviewed anonymously by two peer reviewers, experts on the topic.

The Scientific Directos find the peer reviewers, whithin two months. The Scientific Directors look for peer reviewers among the members of the scientific committee, taking into account their academic aptitudes in relation to the topic of the article proposed for publication. In case that the members of the scientific committee do not have an adequate academic profile in relation to the topic of the manuscript, the scientific directors can contact academics who are experts in the area even if they are not members of the scientific committee.

The average time for the first review shall be at most 8 (eight) weeks.

Once the review process is completed, the reviewers shall suggest:

Rejection

Acceptance with major revisions

Acceptance with minor revisions

Full acceptance

Based on the review process, the Scientific Directors and the Editors in Chief will take a decision and inform the corresponding author by also sending the anonymous reports of the reviews. If there is a rejection, authors have the right to re-submit it again by also underlying the fact that the manuscript is re-submitted, after – at least – four weeks from the notification. If there is an acceptance with minor/major revisions, a deadline of four weeks is given. If the manuscript is not re-submitted with the revisions within four weeks, it is presume that the manuscript has been withdrawn by the corresponding author. However, one day before the deadline, a reminder will be sent. If the corresponding author does not respond, or does not submit a justified request for extension, then the manuscript will be rejected.

Peer Review

The peer review process is fundamental to maintain and always increase the standards of our publications. All authors are clearly informed with the rate of acceptance, which will be updated every year. As a result:

The journal uses a unified standard format for the evaluation process, divided in:

Uncovering of the state of the art

Methodology

Content and Innovation

Language standard and Style

Eventual comments

The journal will send to all reviewers is sent the code of ethics as well as the link of the journal with the information regarding scope, quality, and other policies. More importantly, a link with the information regarding the Guidelines for Reviewers, based on Ethical Guidelines for Peer Reviewers, which is also published in the website, is also included. All reviewers are asked and encourage to take knowledge and to familiarise themselves with them. In order to promote quality, they shall sign that they are been familiarized with these documents.

The reviewers are scholars with academic experience and are – in general – members of the Scientific Committee. Only if the members do not experience in this field, other scholars will be contacted.
The journal supports the investigation of cases of manipulation or fraudulent peer reviews.
The journal supports the confidentiality of the authors and of the peer reviewers by guaranteeing their anonymity. Thus, the manuscript is sent to the reviewers without the names of the authors and the comments are sent to the authors without the name of the reviewers.
Only manuscript with potential high level of advance will be sent to for the review process. In order to speed up the review process, the journal applies different policies.
The corresponding author can suggest independent reviewers without conflict of interest; i.e. no current collaboration; no same institute/university; no co-authorship in the last five years; no working on the same institute in the last five years. When there is more than one author, the corresponding author shall take the liability for the absence of interest for all the co-authors. Although all recommendations are considered, the final decision is taken by the Editor in Chief. Third, co-reviewing process is allowed, under the condition that the editorial board is informed. Thus, reviewers can include in the review process other scholars. However, the Scientific Directors shall be informed and the co-reviewer shall declare any relevant competing interests. This will allow the journal to include them in pool of reviewers and ask their evaluations for the following submissions.
At the end of the review process, the Scientific Directors and Editors in Chief taked a decision based on the reviewers' evaluations:
Full Acceptance
Acceptance with minor/major revisions. When the scientific contribution is perceived as a good manuscript and the reviewers as well as the editorial board believes that the author can address the concerns, a deadline – of a maximum four weeks – is given to the authors to revise the manuscript. In this case, the authors shall sende, within the deadline, two documents: a document with the track changes and another document without the track changes.

Authorship
In the case of submission of a contribution with more than one author, an internal agreement between parties will decide the order as well as the parts that they have written individually or jointly.
However, the corresponding author takes the responsibilities for:
Manuscript corrections and proofreading.
Handing the revisions
Agreeing to and signing the Author Publishing Agreement
Sending the Change of authorship request form
Arranging for the payment of the article processing charge.
All co-authors are responding to the queries – such as publishing ethics, availability of data etc.

Affiliations
Each article shall include an affiliation of the author, that represent the institution or institutions where the research was conducted, supported or approved. For the non-research content, any affiliation should also represent the institution or institutions with which each author is currently affiliated.

Plagiarism
The journal applies the same definition of plagiarism included in The European Code of Conduct for Research Integrity. Therefore, "Plagiarism is using other people's work and ideas without giving proper credit to the original source, thus violating the rights of the original author(s) to their intellectual outputs." It is also called as plagiarism the case of applying the same paragraphs in a different language, without duly acknowledging or citing the original author(s) to their intellectual outputs.
Plagiarism can include not only published or unpublished papers but also lessons, presentation and working materials used by others. In addition, plagiarism can occur in text, pictures, illustrations, as well as in the data, in their elaboration as well as in other parts.
All members – editorial team as well as reviewers and co-reviewers – as well as readers are encourage to raise any suspicion of plagiarism by contacting the editorial in the email: editor@illyrius.eu.
With the goal to eliminate plagiarism, all the tools related to plagiarism will be applied. In the case of plagiarism, the paper is directly rejected.

Duplication and Redundant Publication (Self-Plagiarism)
The journal applies the same definition of self-plagiarism included in The European Code of Conduct for Research Integrity. Therefore, "Re-publishing substantive parts of one's own earlier publications, including translations, without duly acknowledging or citing the original." It is also called as self-plagiarism the case of applying the same paragraphs in a different language, without duly acknowledging or citing the original.
It shall be underlined that self-plagiarism is not tolerated, unless it is essential to prove the same theories or concepts by using the same ideas and by correctly citing the original source.
All members – editorial team as well as reviewers and co-reviewers – as well as readers are encourage to raise any suspicion of self-plagiarism by contacting the editorial in the email: editor@illyrius.eu.
With the goal to eliminate self-plagiarism, all the tools related to plagiarism will be applied. In the case of plagiarism, the paper is directly rejected.
At the moment of submission, the manuscript should not be under consideration, accepted for publication or in press within a different journal, although the other journal has explicitly written that it does not have an exclusive submission policy. However, it shall be noted that the publication of the work on the personal or institutional website, or presented in the working seminars organized within the various institutions is not viewed as prior or duplicate publication. However, in the acknowledgment, this shall be mentioned.
Furthermore, it is not considered as prior or duplicate publication, the submission of part of the thesis, although this is published in the institutional or personal website, if it is published under embargo until the moment of publication by the journal. In

addition, the publication of the thesis by a publisher, can be submitted to the journal, if permission is given by the thesis publisher and/or the thesis does not have an ISBN.

Research with Humans or Animals
As stated in The European Code of Conduct for Research Integrity, "researchers handle research subjects, be they human, animal, cultural, biological, environmental or physical, with respect and care, and in accordance with legal and ethical provisions." Moreover, their right to privacy as well as the ethical and legal standards for research shall be respected by also adapting the good practice in that particular field.

Competing Interests and Funding
At the moment of submission, all authors disclose any conflicts of interest and financial or other types of support for the research or for the publication of its results. It is considered as conflict of interest any type of influence that can interfere on the objectivity and impartiality of the work by also impacting on the ethical principles of research. However, it does not constitute a conflict of interest, the funds or grants in the academic research, unless this has influenced the design, the methods, the analysis, and the publication of the results. However, funds or grants shall be declared in the acknowledgment. In addition, the journal is free from undue influence. Thus, also reviewers or editors with a conflict of interest shall withdraw from involvement in decisions on publication or reviewing.
All members – editorial team as well as reviewers and co-reviewers – as well as readers are encourage to raise any suspicion of conflict of interest by contacting the editorial in the email: editor@illyrius.eu.

Libel, Defamation and Freedom of Expression
All authors shall not held any type of behaviour or submit false statements that can harm the reputation of colleagues, students or collaborators. In addition, the reputation of various groups, associations, organizations or individuals is protected.

Retractions, Corrections and Expressions of Concern
As stated in The European Code of Conduct for Research Integrity, the journal will accept corrections made by the authors (corrigendum) or by the publisher (erratum). However, this is limited only to cases where the errors are serious, contain plagiarism or the content is considered as life-endangering. Both authors and publisher are given credit for the corrections post publication.
However, only in extrema ratio, when the content is violating personal rights or confidentiality laws, or it encourages behavior against the public order or health, the journal might decide to remove a published manuscript. It shall be noted that this are only explanatory cases and other cases that are carefully considered by the editorial team might be a reason for this drastic decision.
In all these cases, the corresponding author will be informed. Moreover, the records will be maintained by the journal (see Section Integrity of Records).

Manipulation, Falsification and Fabrication
As stated in The European Code of Conduct for Research Integrity, manipulation, falsification and fabrication are not allowed. In concrete, "fabrication is making up results and recording them as if they were real." In addition, "falsification is manipulating research materials, equipment or processes or changing, omitting or suppressing data or results without justification."
These principles are applied not only in data or contribution but also in imagine. In these cases, correction of the manuscript or its removal could be applied (see Section Retractions, Corrections and Expressions of Concern).

Fraudulent Research and Research Misconduct
The Journal applies all the measures to avoid the fraudulent research and research misconduct. However, if this has not been possible during the pre-review process or review process, as stated in The European Code of Conduct for Research Integrity, fraudulent research and research misconduct are sanctionable. This includes not only the case of corrections, but also the case of removal of the published manuscript (Section: Retractions, Corrections and Expressions of Concern).

Versions and Adaptations
This journal accepts the possibility of adaptation, including also translation in a different language, under two conditions:
Explicit consent by the Journal
Application of the ethical principle in research; in particular regarding self-plagiarism (see Section Duplication and Redundant Publication (Self-Plagiarism)).
The journal retains the right to withhold the approval for publication, if this impacts on professional responsibility, accountability, professional attitude, or intellectual property rights (see Section Research Integrity).

Transparency and Honesty
Researchers apply the principle of transparency and honesty during their research, also in the acknowledgment. Their violation is sanctionable (see Section: Retractions, Corrections and Expressions of Concern).

Data and Supporting Evidence
This Journal applies the policy of open access. This is also included for the data, which can be part of the manuscript or submitted in a different document. These supplementary materials are important for understanding the data uncovered and examined in the manuscript. Depending on the type of manuscript, the supplementary data are only part of the editorial pre-review process or they can also be part of the evaluation process by the reviewers, if the editorial board believes that it is needed for the evaluation process.

Integrity of Record
The journal maintains a record of everything that is published. However, the metadata shall comply with the EU and Italian laws and the Journal will make any effort to make them accessible under the Italian jurisdiction. In the case of modification – i.e. cases

of misconduct of research, such as defamation or retraction (see Section Retractions, Corrections and Expressions of Concern) – a record is kept by the journal.
Moreover, when the manuscript is download, the customer shall respect intellectual property rights as well as copyrights.

Ethical Business Practices

Fair Access
The Journal applies open access system. This guarantees fair access to all contributions. Moreover, in exceptional cases, under justified reasons, the editorial team may reduce or eliminate the payments of Article Processing Charge.

Censorship
The journal respects and protects personal dignity and freedom. The journal encourages and promotes freedom of research. Thus, the Journal does not complicit in any kind of censorship. However, the rules regarding libel, defamation and freedom of expression shall be considered (see Section Libel, Defamation and Freedom of Expression).

Marketing Communication
Marketing will be done through social media, academic media, and email communication. At the moment of submission, the corresponding author shall choose if s/he would like to be sent emails regarding the communication and promotion of the journal. The journal will apply the social media policies as well as the best practice in media use. In addition, on the website, a newsletter will be established. Thus, the Journal will not violate the integrity of the content or of the academic records.

Advertising
The journal does not accept any type of business advising.

PR/ Media
The Journal applies the International Public Relations Association's Code of Conduct. In addition, as stated in The European Code of Conduct for Research Integrity, "authors ensure that their work is made available to colleagues in a timely, open, transparent, and accurate manner, unless otherwise agreed, and are honest in their communication to the general public and in traditional and social media."

Metrics, Usage and Reporting
The journal remains complaint with the industry standard and the COUNTER Code of Practice.
The journal does not influence or control third parties that aim to metric the impact and reception of the content of the Journal. With the goal to promote independency, no agreements with these organizations have been stipulated. However, the Journal actively facilitates the work of these organizations through free access to the data (application of open access to the manuscripts). The Journal is committed to promote best practice in the assessment and impact reporting of scholarly research. This is done through also the involvement of members of the editorial board or of the university partners that are also part of the San Francisco Declaration on Research Assessment (DORA).

Useful Contacts
For all inquiries regarding Illyrius, please contact: editor@illyrius.eu.

Instructions for the Authors and Publishing Conditions

Illyrius
International Scientific Review
ISSN 2225 – 2894

The purpose of Illyrius is to act as a meeting place to encourage the sharing of experiences between scholars belonging to different geographical areas and who, thanks to their cultural peculiarities, can contribute to a productive and continuous exchange of scientific and didactic knowledge. In this perspective, the journal is open to welcome contributions from scholars from all over the world on topics such as law, economics, sociology, political sciences, security sciences, international cooperation, communication sciences. Illyrius seeks to publish original contributions (research papers, book reviews, legislation report, case note) in these areas.
Articles must be written in English. The publisher reserves the right to evaluate any valuable publications in other languages, such as Italian, French, German, Spanish and Portuguese.
In any case, all articles must always have the title and abstract also in English, regardless of the language in which the article is written.
To cover the costs of publication, the editor charge a flat "article processing charge" of 50 EUR and a fee for publishing from 100 to 1000 EUR (Illyrius will be free of charge for the whole year 2022). At the beginning of each year, the cost of the single publication for the current year will be indicated in the journal. The payment of the fee is an indispensable condition for the evaluation and subsequent publication. The publisher reserves the right to indicate and modify the cost of the single publication each year based on the costs that must be incurred by the same for the administration of the magazine. Payments are processed by PAYPAL or IBAN. Bank information is provided to the author by e-mail once the work has been accepted.
For the year 2023 the cost for publication in the magazine will be 200 EUR. Articles submitted by multiple authors will cost € 300 (the publications on Illyrius will be free of charge for the whole year 2022).
The Manuscript, a Cover Letter, and the Title Page shall be sent to: editor@illyrius.eu
Manuscript should not extend recommended extent of:

- 7–25 pages for papers;
- 2–10 pages for book reviews, legislation report, case note, opinions.

Papers: shall include title, name(s) of author(s), affiliation(s) of all author(s), as well as the eventual acknowledgment. abstract (200-250 words), keywords (3-5, not mandatory), introduction, main text (divided to sections), conclusions and list of references in alphabetical order. It shall includes footnotes (in this case the final references ar not mandatory).
Book reviews, legislation report, case note, opinions: shall include title, name(s) of author(s), affiliation(s) of all author(s), as well as the eventual acknowledgment. abstract (200-250 words).
All the manuscript will pass the pre-review process which aims:
the contribution follows all the criteria for the submission – in particular style and extension – established by the Journal.
the contribution fits into the scope of the journal.
the contribution has potential quality.
All the manuscript will pass the double blind review process which aims. Based on that the Editor will choose between:

- Rejection;
- Acceptance with major revisions;
- Acceptance with minor revisions;
- Full acceptance.

Illyrius reserve the right to not start the review process if it does not pass the pre-review process.
Illyrius reserve the right to not start the pre-review process, if there is not a full payment of the process fee.
Illyrius reserve the right to not publish if there is not a full payment of the publication fee.
Illyrius reserve the right to ask for corrections.

Style Sheet for footnotes, references and quotations

Illyrius
International Scientific Review
ISSN 2225 – 2894

Books
E. BOZHEKU, *Infanticidio. Spunti e rilievi di parte generale*. Jovene, Napoli, 2012, p….

Papers and journals
M. ROMANO, *La difesa è sempre legittima?*, in *Illyrius*, 1i, II-2018, p…
M. ROMANO, *Forme di automatismo nell'applicazione delle sanzioni interdittiva*, in Archivio Penale, 1, 2020, p…

Electronic Sources
M. ROMANO, *Recensione a "Diritto penale. Dottrina, casi e materiali"* di Enrico Mezzetti (Zanichelli, 2020, III ed.) in *www.giurisprudenzapenale.com*

Case-Law
It. Cass. Pen., Sez. I, 1 gennaio 2021, n. 3333, p…

Those who are interested in publishing in Illyrius magazine can send their contributions to the following e-mail address: ***editor@illyrius.eu***.

Illyrius

International Scientific Review

ISSN 2225-2894

n. 18/ (I-2022)

SPECIAL EDITION

"LEGAL CHALLENGES IN THE DIGITAL ERA"

Essays

edited by
Dorina Hoxha, Jonida Milaj-Weishaar, Ersi Bozheku

INDEX

ESSAYS

ESSAYS

The right to privacy versus freedom of expression in the Albanian media: Law, practice and lack of oversight on new emerging social media platforms

Prof. Assoc. Dr. Enkeleda Olldashi – Roden Hoxha MSc LLM PhD Cand.[1]

1. Introduction

The right to information and freedom of expression as well as the right to hold opinions and receive and disseminate information and ideas without interference by public authorities are rights guaranteed by international and domestic legal instruments. They are further expanded upon in the context of journalism, with the latter being given a wider margin of appreciation in their exertion. Nonetheless, a journalist's right to freedom of expression is not absolute, with the term "responsibilities" becoming a secondary prerogative pursuant to the ECHR and the case-law of the Strasbourg Court.

In this regard, the term "rights" is construed as journalist's prerogative to exercise their profession, while the term "responsibilities" denoting the obligation to act in good faith and provide accurate and reliable information of public interest, in accordance with the ethics of journalism and the respect and safeguard of the privacy of the subjects of their stories. In recent years, further to the numerous ethical violations committed by journalists and media outlets for the sake of publishing a ground-breaking story, the balance of the right of the public to know and the right of the subject to be shielded from public attention, has been further upset by the advent of social media and the use of these platforms as tools of dissemination and multiplication of news. For the better part, these outlets are either unregulated and operating in a vacuum, or are plainly violating the already set out bylaws and guidelines issued by public institutions such as the Information and Data Protection Commissioner and the Electronic and Postal Communication Authority.

[1] Prof. Assoc. Dr. Enkeleda Olldashi, University of Tirana, enkelejdaboci@gmail.com
Roden Hoxha MSc LLM PhD Candidate, University of New York Tirana, rodenhoxha@gmail.com

International institutions such as the Council of Europe and the European Union have issued general guidelines and standards for the interaction of media with the right to private life and instituted strict legal frameworks for the protection of privacy including here the media context. The Albanian legal framework on the other hand, with the exception of an inadequate set of guidelines and standard setting self-regulation instruments and ethic codes, lacks the appropriate institutional background and oversight for the protection of privacy in the media context, be that on legacy media or new and emerging social media markets.

One must keep in mind that the conflict in balancing freedom of the press and the right to information *vis a vis* the right of a person to his privacy, invariably presents some controversial and challenging legal issues, especially in the media sphere. In addressing the legal dilemmas posed by the competing interests, it is of paramount importance to conduct an in-depth analysis of the conceptual value of these two equally important fundamental rights. Through the exploration of the framework and development of the press and privacy laws and regulations at the international level, as well as in Albania, this article examines the fundamental values enshrined in these two rights. By analyzing the concepts of "public interest," "public figure," and "personal privacy," we will strive to create a balance between the theoretical approaches to the issue and the practical attempts at striking a balance between these interests.

2. The international perspective

As a core principle enshrined in numerous international and domestic legal instruments, the freedom of the press has been widely recognized as a means of enabling the gathering, publishing, and disseminating of news and opinions in a democratic society. As Walter Cronkite has put it, *"Freedom of the press is not just important to democracy, it is democracy."* The crucial role played by the press, which includes but is not limited to print, broadcasting, and electronic media, has for a long time now become a key element for the evaluation and understanding of the democratic standing of a society. The freedom of the press presents the crucial thesis of the "fourth estate" and its role for the wider public.

When privacy and freedom of the press come into conflict most institutions, be they at the international level,[2] or at the domestic level[3] have taken a stance of finding a balance between the two fundamental rights. There is no legal or logical reason to prefer one value over the other. Both privacy and freedom of the press are internationally[4] and constitutionally protected values. Nor is there any commonly

[2] The ECtHR has stated that although the press must not overstep certain bounds, regarding in particular protection of the reputation and rights of others, its task is nevertheless to impart – in a manner consistent with its obligations and responsibilities – information and ideas on all matters of public interest. *Couderc and Hachette Filipacchi Associés v. France*, no. 40454/07, Judgment, Court (Grand Chamber), 10/11/2015.

[3] In a number of its decisions, the Albanian Audio-Visual Authority and its Complaints Commission have ruled that a fair balance must be struck between the rights of the media to disclose information and the rights of the subjects of the stories to their private and family lives.

[4] At the European level, the European Convention on Human Rights, the European Charter of Fundamental Rights and the General Data Protection Regulation play a cornerstone role in setting up the rights and duties of different actors in the field of media and privacy and the tense relationship between the rights of one party and the obligations of the other.

calculated means for weighing *vis a vis* freedom of the press and the right to privacy on a general scale, requesting a case-by-case evaluation of all cases where the two rights come into conflict.

In addition to the general standing of the competing rights of freedom of expression and right to privacy, one must take also a deeper look at the legal concerns stemming from the role of the media as a key player[5] as well as the latter's s behavior as it relates to personal privacy, with some of the issues also straddling the fine line between legal permissions and moral standing of the media. For instance, is it proper for journalists to lie or misrepresent themselves in order to get their story? In the case of Dietemann v. Time, Inc.[6], the court stated, *"one who invites another to his home or office takes a risk that the visitor may not be what he seems, and that the visitor may repeat all he hears and observes when he leaves…". However, the court also reiterated that "The First Amendment has never been construed to accord newsmen immunity from torts or crimes committed during the course of newsgathering. The First Amendment is not a license to trespass, to steal, or to intrude by electronic means into the precincts of another's home or office. It does not become such a license simply because the person subjected to the intrusion is reasonably suspected of committing a crime."* To this day, American courts have not changed their attitude towards deceptive conduct in the media's newsgathering process.

Tradition endows the press with a special mandate to be the "watchdog," or "guardian" of the government, represent public interests of the governed, and contribute to the democratization processes of society. To date, this fundamental value of the press has been enshrined in the constitutional documents of numerous countries,[7] and in international instruments like the Universal Declaration of Human Rights.[8]

On the other side of the same coin, the "right to privacy" is a term used frequently in the realm of law and everyday life as a shield to protect individuals from undesirable exposure and to protect private information.[9] Nevertheless, the exact meaning of the term is not self-evident. Different legal instruments provide different interpretations of the core right. In developed countries, the right to information privacy is acknowledged as a universally accepted human right, mainly as a basis for individuals' freedom and autonomy.[10]

---

[5] The European Court for Human Rights has asserted the essential role played by the press as a "watchdog" in a democratic society, and its task in imparting information and ideas on all matters of public interest to the public's right to receive them *in Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland [GC], § 126; Bédat v. Switzerland [GC], § 51; Axel Springer AG v. Germany [GC], § 79; The Sunday Times v. the United Kingdom (no. 2), § 50; Bladet Tromsø and Stensaas v. Norway [GC], §§ 59 and 62; Pedersen and Baadsgaard v. Denmark [GC], § 71; News Verlags GmbH & Co.KG v. Austria, § 56; Dupuis and Others v. France, § 35; Campos Dâmaso v. Portugal, § 31).*

[6] *A.A. DIETEMANN, Appellee, v. TIME, INC., a New York corporation*, United States Court of Appeals, Ninth Circuit 449 F.2d 245 (9th Cir. 1971).

[7] U.S. Const. amend. I, *"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press;"*. France. The French Constitution, adopted by the Referendum of September 28, 1958 and Promulgated on October 4, 1958. French Text and English Translation. New York: French Embassy, Press and Information Division, 1958, Article 4.

[8] Universal Declaration of Human Rights, GA Res. 217(III), 10 December 1948, Article 19.

[9] Balancing Freedom of the Press and the Right to Privacy: Lessons for China By Zhendong Sun, 21, URL: https://central.bac-lac.gc.ca/.item?id=TC-QMM-99152&op=pdf&app=Library&oclc_number=892076602, last accessed 28.05.2021.

[10] Rachels, J. (1975), "Why privacy is important", Philosophy & Public Affairs, Vol. 4 No. 4,

Despite the large discussion in literature on the definition and key aspects of privacy, a common definition has hardly been reached. Weinstein has described privacy as a condition of "*being-apart-from-others*" very closely related to alienation,[11] or as Fried puts it *"a form of power and control we have over information about ourselves*"[12], or the individual's ability to control the circulation of information relating to him"[13] or defining it as a form of "*control over when and by whom the various parts of us can be sensed by others"*.[14] A legal and commonly accepted definition of privacy, which is directly applicable at the domestic level has been provided by the European Court for Human Rights in the case of X and Y v. the Netherlands,[15] where it remarked that the concept of "private life" is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person […]. It can sometimes embrace aspects of an individual's physical and social identity,[16] gender identification, name and sexual orientation and sexual life,[17] as well as, but not limited to, the right to personal development, and the right to establish and develop relationships with other human beings and the outside world.[18]

Although the right to privacy can guarantee one's authority to regulate one's personal and intimate information, such a right, however, is not absolute and unconditionally protected by the legal instruments in force. The right to privacy has an inevitable tension with the freedom expression and the role of the press, which is derived from the natural desire to have access to new information about the world surrounding us. This strain between the two rights requires individuals to compromise their rights to privacy, whether willingly or unwillingly, for the sake of other competing interests in a democratic society.[19] Thus, the right to privacy may concede to the freedom of the press if a higher legitimate interest is served by the latter, where common well-being prevails over the individual's interest. Needless to say, the interests served by the press, depending on the newsworthiness of the information falling into the private sphere, will in most cases outweigh the latter, including cases where priority is automatically endowed to the freedom of press such as when a public figure is involved, [20] or if no reasonable expectation of privacy exists.

Under Article 8 of the EU Charter for Fundamental Rights,[21] everyone has the right to the protection of personal data concerning him or her, as well as access to data which has been collected concerning him or her, and the right to have it rectified.

---

pp. 323-33.; Introna, L.D. (1997), "Privacy and the computer: why we need privacy in the information society", Metaphilosophy, Vol. 28 No. 3, pp. 259-75.

[11] M. Weinstein, "The Use ofPrivacy in the Good Life" in 1. Roland Pennock & John W. Chapman ed., Privacy: Nomos XIII (New York: Atherton Press, 1971), p 94.

[12] Charles Fried, An Anatomy of Values (Cambridge, Mass.: Harvard University Press, 1970) p 140).

[13] Alan F. Westin, Privacy and Freedom (New York: Athenaeum, 1968).

[14] Richard B. Parker, "A Definition ofPrivacy" (1974) 27 Rutgers L. Rev. 281.

[15] *X and Y v. the Netherlands*, 26 March 1985, ECHR, Series A no. 91.

[16] *Mikulić v. Croatia*, no. 53176/99, § 53, ECHR 2002-I.

[17] B. *v. France*, judgment of 25 March 1992, ECHR, Series A no. 232-C, pp. 53-54, § 63.

[18] *Burghartz v. Switzerland*, judgment of 22 February 1994, ECHR, Series A no. 280-B, p. 28, § 24.

[19] HÄMÄLÄINEN v. FINLAND, no. 37359/09, 65, ECHR (GC) 16/07/2014.

[20] Lingens v. Austria, 8 July 1986, ECHR Series A no. 103.

[21] European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

The European Commission put forward its EU Data Protection Reform[22] in January 2012 as a means of advancing data protection in the European sphere following the big shift of data collection and processing in the digital age. The regulation put forward and accompanying instruments was seen as an essential step to strengthen the citizens' fundamental rights in the new digital age and simplify the rules for business in the European digital single market.

On 15 December 2015, the European Parliament, the Council and the Commission reached an agreement on the new data protection plan,[23] establishing a modern and harmonized framework across the EU. On 8 April 2016 the Council adopted the regulation and the directive, following their adoption by the European Parliament on 14 April 2016. On 4 May 2016, the official texts were published in the EU Official Journal in all the official languages, with the regulation coming into force on 24 May 2016 and applying to the concerned parties from 25 May 2018, Regulation (EU) 2016/679[24] on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and Regulation 2018/1725[25] on the rules applicable to the processing of personal data by European Union institutions, bodies, offices and agencies.

This regulation was further complemented by Directive (EU) 2016/680[26] on the protection of natural persons regarding processing of personal data connected with criminal offences or the execution of criminal penalties, and on the free movement of such data, as well as safeguarded by a number of national[27] and supranational institutions such as the Data Protection Board[28] and European Data Protection Supervisor[29] and Data Protection Officer.[30]

Concurrently with the EU regulations in force for the protection of personal data, which are gradually being included and adapted into the Albanian legislation as part of the EU Association and Stabilization Process, one key international instrument directly enforceable at the national level is Article 8 of the European Convention for Human Rights and the ensuing case law adopted by the ECtHR. Pursuant to the European Court for Human Rights, in interpreting the European Convention on Human Rights, the notion of private life is a broad term with no strict definition,

[22] https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46, last accessed 28.05.2021 – Last accessed 28.05.2021

[23] https://www.consilium.europa.eu/en/press/press-releases/2015/12/18/data-protection/, last accessed 28.05.2021- Last accessed 28.05.2021.

[24] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[25] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

[26] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[27] https://edpb.europa.eu/about-edpb/about-edpb/members_en - Last accessed 28.05.2021.

[28] https://edpb.europa.eu/edpb_en - Last accessed 28.05.2021.

[29]https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_en - Last accessed 28.05.2021.

[30] https://ec.europa.eu/info/departments/data-protection-officer_en - Last accessed 28.05.2021.

covering a plethora of issues and elements constituting the right. The general principles deriving from the Court's case-law with regard to the protection of private life in the context of its relation to the freedom of expression and the rights of the press are set out in paragraphs 83 to 87 of the *Couderc and Hachette Filipacchi Associés v. France* [GC] judgment, stating that:

> *"…the notion of private life is a broad concept, not susceptible to exhaustive definition. It extends to aspects relating to personal identity, such as a person's name, photograph, or physical and moral integrity. This concept also includes the right to live privately, away from unwanted attention … The guarantee afforded by Article 8 of the Convention in this regard is primarily intended to ensure the development, without outside interference, of the personality of each individual in his or her relations with other human beings."*

> "…Moreover, whilst a private individual unknown to the public may claim particular protection of his or her right to private life, the same is not true of public figures …Nevertheless, in certain circumstances, even where a person is known to the general public, he or she may rely on a "legitimate expectation" of protection of and respect for his or her private life…"
>
> "…Publication of a photograph may thus interfere with a person's private life even where that person is a public figure. The Court has held on numerous occasions that a photograph may contain very personal or even intimate "information" about an individual or his or her family. It has therefore recognized every person's right to protection of his or her own image, emphasizing that a person's image constitutes one of the chief attributes of his or her personality, …"

As a general rule, personal information should not be made public without the consent of the concerned person consent being an important element in determining whether a publication of a detail from private life interferes with the right to privacy. However, as under other legal instruments, public interest poses an enormous weight on whether a case falls under the umbrella of privacy or the latter defers to the right to information.

Public interest relates to matters affecting the public to such a degree that it may legitimately take an interest in them, attracting its attention or concerning the public significantly.[31] Areas of public interest, under the Court's case law may include, but are not limited to misuse of public office[32], improper use of public funds,[33] protection of public health,[34] safety and environment, protection of national security,[35] crime and social behavior and similar political and socioeconomic topics, and many more. In determining public interest, what the Court takes into consideration is whether the news report is capable of contributing to the public debate and not whether they will manage to fully achieve that objective.[36]

[31] *Bladet Tromso and Stensaas v. Norway*, 21980/93, Judgment, (GC), 20/05/1999, §§ 59 and 62.
[32] *Medžlis Islamske Zajednice Brčko and Others v. Bosnia and Herzegovina* [GC], §§ 80-84.
[33] *Matúz v. Hungary*, no. 73571/10, ECHR, 21 October 2014.
[34] *Mamère v. France*, no. 12697/03, ECHR 2006-XIII.
[35] *Gîrleanu v. Romania*, no. 50376/09, ECHR, 26 June 2018.
[36] *Erla Hlynsdóttir v. Iceland* (No. 2), 54125/10, ECHR, 21/10/2014.

3. Albanian legal framework and ongoing problems

These international instruments, as well as the case law deriving from their interpretation, have one way or another been juxtaposed and integrated into the domestic legal system of Albania. From the outset of the conception and later introduction of the Albanian Constitution, Parliament saw the right to privacy and the right to freedom of information as cornerstone values of a new and emerging democracy. However, in contrast with the European instruments where the right to privacy and freedom of information are distilled into two single articles, the Albanian Constitution provides for a series of norms which encompass the rights which were developed by the ECtHR into different interpretations of the norms stemming from single, multifaceted articles. The Constitution, in Article 23 provides for the freedom of expression. At the same time, the rights encompassed under Article 8 of the Convention with regards to privacy and family life, are laid down in a number of norms such as the right to secrecy of correspondence,[37] the right to residence,[38] and chapters dedicated to social and political rights,[39] under which fall a number of legal concepts and interpretations of the right to privacy. With the amendments to the Constitution introduced through law 96/2016, a number of personal civil rights for the subjects undergoing re-evaluation due to their inclusion or current standing in the judicial system have either been limited or abrogated altogether.[40]

Further to the Constitution, with regards to the right to privacy, one key instrument in force in Albania is the Law on the protection of personal data,[41] which has intermittently been amended for the purpose of falling in line with the latest developments in the international and European sphere, as well as the case-law of the ECtHR. For the purposes of this law, personal data encompasses any information relating to a natural person, whether identified or identifiable, directly or indirectly, in particular with reference to an identification number or more specific factors for his physical, physiological, mental, economic, cultural or social identity.[42] The law sets the main guidelines for the processing of personal data,[43] their transfer[44] their protection,[45] as well as going into detail with regards to the duties, obligations and rights of individuals, state actors as well as data processing parties. The law has further been complemented by a number of bylaws and normative acts relating to specific issues of personal data processing and protection.[46]

With relation to the duties and obligations of the media towards the protection of personal data in the process of publication of news, the Personal Data Protection

[37] Constitution of the Republic of Albania, amended by law no. 9675, dated 13.1.2007; no. 9904, dated 21.4.2008; no. 88/2012, dated 18.9.2012, no. 137/2015, dated 17.12.2015 and no. 76/2016, dated 22.7.2016, Article 36.
[38] Ibid Article 37.
[39] Ibid, Chapters III, and IV.
[40] Ibid, ANNEX Transitional re-evaluation of judges and prosecutors, Article A Restriction of the rights provided by the Constitution.
[41] Law no.9887, dated 10.3.2008, "On personal data protection".
[42] Ibid, Article 3.
[43] Ibid, Articles 6 and 7.
[44] Ibid, Articles 8 and 9.
[45] Ibid Article 5.
[46] https://www.idp.al/per-kontrolluesin-te-tjera - Last accessed 28.05.2021.

Commissioner has issued a comprehensive instruction on the fundamental rules in connection with the protection of personal data in written, visual and audio-visual media[47] This instruction sets forth the ground rules for the safeguard of the legal and ethical standards in the newsroom, ranging from issues related to protection of minors,[48] the role and behavior of the media during the coverage of criminal proceedings,[49] the prohibition of interception as well as use of information pertaining to close personal interests such as health and sexuality,[50] the publication of photographs,[51] consent from the subjects of the stories, as well as the duty to balance newsworthiness taking into account public interest and personal rights of individuals.[52]

The Instruction, as a deterrent for unlawful and unethical behavior by part of the media outlets has prescribed financial penalties to violators of the rules of the law as well as norms of the Instruction therein, prescribing fines ranging from m 10,000 up to 50,000 ALL.[53] However, despite the harsh nature of the financial penalties and obligations provided for in the law and the specific instructions, to date, the Commissioner has only issued a total of 20 administrative Decisions, Orders and Recommendations on issues of protection of Personal Data and Privacy in the Media Context,[54] and all the aforementioned instruments having been issued in the timespan of 2013-2016, lacking any decision since. Of all these decisions 1 (one) sole decision issued a 300.000 ALL fine due to the failure of the media outlet to delete the personal information of the complainant from their publications;[55] 9 (nine) orders to delete personal data from publications, and 10 (ten) recommendations to follow the provisions of the aforementioned Instruction. The low number of administrative actions undertaken by the Commissioner towards any media outlets, especially the online outlets, which are entirely unregulated with regards to their content and behavior, be that from the standpoint of the National Electronic Communication and Postal Authority, or that of the Audio-Visual Media Authority, is a cause of concern, since the former, at present fall solely under the purview of the Data Protection Commissioner.

Further to the Instruction of the Commissioner, the relationship between the freedom of the press and the right to privacy is regulated by the Law on audio and audio-visual media services in the republic of Albania,[56] designating the Audio-Visual Authority (AMA) as the sole institution regulating the behavior of television outlets and radio stations in the entirety of the territory of Albania.[57] The law, among others,

[47] Instruction no. 9, dated15/09/2010, URL: https://www.idp.al/wp content/uploads/2016/11/udhezimi_nr_09_i_perditesuar.pdf (Albanian) - Last accessed 28.05.2021.
[48] Ibid, Chapter II.
[49] Ibid, Chapter III.
[50] Ibid, Chapter V.
[51] Ibid, Chapter VI.
[52] Ibid, Chapter IX.
[53] Ibid, Chapter X.
[54] https://www.idp.al/hetimi-administrativ/ - Last accessed 28.05.2021.
[55] (Decision No. 02, dated 24.01.2013, "On the administrative contravention of the controller Gazeta Shqiptare) (Albanian), URL: https://www.idp.al/wp-content/uploads/2016/11/Vendim-nr-02-Gazeta-Shqiptare-1.pdf - Last accessed 28.05.2021.
[56] Law no. 97/2013 "On the Audiovisual Media Service".
[57] Ibid, Chapter II, Article 6 "Audiovisual Media Authority (AMA)".

provides for the duties of the audio-visual service providers,[58] as well as the right of interested subject to appeal near the AMA for cases where they perceive that their rights under the law have been violated by the former, including here cases where their right to privacy has been breached by media outlets,[59] initiating in this way an examination procedure near the Complaints Committee, culminating in a decision of the latter ranging from recommendations, to decisions to compel to retract to financial penalties, temporary suspension of the license and/or the authorization, reduction of the license time and/or the authorization and withdrawal of the license and/or the authorization.[60] In any case, these administrative actions are subject to appeal to the AMA itself, as the head authority and ultimately the District Court. From the time of formation of the Complaints Committee in 2016, rarely has the latter issued punitive verdicts towards violators of the broadcasting code, an instrument partly juxtaposing the instructions issued by the Data Protection Commissioner, as well as including further chapters on issues such as persons with disabilities, advertisements, best commercial practices, etc. The table below indicates that it is in the modus operandi of AMA that perpetrators of violators of the Broadcasting Code be either cited for their behavior, or be issued decisions for retraction and apology towards the subjects of their story, rarely issuing fines for repeated offend behavior, indicating that the media behavior towards privacy rights of individuals is fairly regulated, and requires little intervention by part of the regulating authorities.

[58] Ibid, Chapter III, Article 30 and following.
[59] Ibid, Article 51 "Procedures for handling complaints".
[60] Ibid, Article 132 "Measures for violations".

Grievance Redress Bulletin

Decisions of the Albanian Audivisual Authority on the Complaints of the public on the behaviour of media outlets for the years 2016-2021

Bulletin No.	Year	Complaints on the subject "Violation of children's rights"	Complaints on the subject "Violation of the rules of ethics and dignity"	Complaints on the subje"Prohibited commercial communications"	Other Complaints	Rejected Complaints	Fining of Entity	Obligation to Publish Response/Respond to Complainant	Citation/Prior to Fining	No Action Undetaken	Follow-Up of the Case	Product Removal / Retraction / Prohibition fo Continuationn of Publicationn
1	2016	10	4	0	0	4	0	2	6	4	1	1
2	2017	6	5	0	3	1	0	1	7	0	1	1
3	2017	5	6	3	2	1	1	1	7	1	0	4
4	2018	3	3	3	2	1	0	0	4	3	0	3
5	2019	4	6	3	5	1	0	0	7	2	1	3
6	2020	5	12	2	1	2	3	2	8	5	0	3
7	2021	3	11	0	7	2	0	0	2	9	1	2

Source: Audiovisual Authority of Albania • Created with Datawrapper

Fig.1 Grievance Redress Bulletin summary of Complaint Commission decisions for the years 2016-2021

However, the same cannot be said about online publications and broadcasting, the latter being entirely unregulated by the laws in force.[61] The lack of supervision or regulation by any national authority has led to many cases of violation of privacy of victims of violent and sexual crimes,[62] children and teenagers,[63] as well as other sensitive cases in the eyes of the wider public. To add to this issue, there is no definitive number of online media outlets or their operational structure. There are no official figures on how many online portals, news magazines, newspapers or active blogs are operational in Albania, with only partial figures being delivered by the Union of Journalists with more than 800 online portals active, with over half of them being unregistered with an objective inability to discern their administrators.[64]

For the rectification of this situation, the Government introduced a slew of legal initiatives aimed primarily at the registration of these outlets[65] as well as for the amendment of the Law on Audiovisual Service in Albania,[66] with regards to the inclusion of online media, as well as written press into the purview of AMA, in order to regulate their behavior in line with the Broadcasting Code, however, with significant changes to the procedural guarantees for the subjects of the law. [67]

From their inception, due primarily to the lack of public consultation, as well as the rushed approval procedure under which the amendments were presented to Parliament, they lacked public support due to their perceived censuring effect,[68] as well as the institutional support of the President, who vetoed the amendments passed by parliament,[69] the Ombudsman, who viewed the new instrument as rushed and incomplete,[70] as well as international institutions such as the OSCE.[71] The final nail in the coffin for the new amendments was the Opinion of the Vince Commission,[72] deeming the initiative as having major inconsistencies with spirit of the Constitution and international legal instruments, pertaining to the independence of the ruling

[61] The Law on the audiovisual service in Albania, in article 2, provides that it applies to linear audiovisual broadcasts, non-linear audiovisual broadcasts and their support services. This law does not apply to the print media. The law altogether does not provide in any of its articles the application towards online service providers.
[62] http://www.shkodranews.org/ndodh-edhe-kjo-ne-tirane-adoleshenti-perdhunon-mamane-e-tij/ - Last accessed 28.05.2021.
[63] https://www.oranews.tv/shkon-per-te-festuar-krishtlindjen-rrembehet-dhe-perdhunohet-17-vjecarja-shqiptare - Last accessed 28.05.2021.
[64] https://top-channel.tv/2019/03/18/fake-news-shtohen-per-zgjedhjet-mbi-400-portale-pirate/ - Last accessed 28.05.2021.
[65] Draft law on some additions and amendments to Law no.9918, dated 19.5.2008, "On electronic communications in the Republic of Albania", amended, dated 10.07.2019.
[66] Draft law on some amendments and additions to Law no. 97/2013, "On audiovisual media in the Republic of Albania", amended, dated 10.07.2019 URL: http://www.parlament.al/Files/ProjektLigje/20190715110745NDRYSHIME%2097-2013%20-%20AMA.pdf.
[67] Ibid, Article 21.
[68] https://www.reporter.al/ligji-antishpifje-mund-te-dhunoje-fjalen-e-lire-pa-e-luftuar-shpifjen/.
[69] Decree for the return of Law no. 91/2019 "For some amendments and additions to Law no. 97/2013 "On audiovisual media in the Republic of Albania", amended, URL: https://www.parlament.al/Files/ProjektLigje/20200120145223Dekreti%20i%20PR,%20nr%2011413%20date%2011%201%202020.pdf.
[70] https://fjala.al/2019/12/18/avokati-i-popullit-i-shqetesuar-per-paketen-anti-shpifje-ligj-jo-korrekt/
[71] https://abcnews.al/osbe-kunder-rames-per-ligjin-antishpifje-niveli-i-gjobave-presion-indirekt-qe-con-ne-mbylljen-e-mediave/.
[72] European Commission for Democracy though Law, CDL-AD(2020)013-e Albania - Opinion on draft amendments to the Law n°97/2013 on the Audiovisual Media Service.

body,[73] the professional qualifications of said body,[74] the right to anonymity in the internet,[75] the complaint examination procedure (ref 50-58) stating that *"The administrative procedure for reviewing complaints, as it stands, does not provide the necessary procedural guarantees, in order to protect the right to freedom of expression in the internet."*, as well as the penalties, procedure and *"severely punitive and debilitating nature of the fines"* to be issued by the Complaints Committee in case of finding of a breach of the law,[76] noting that in the interest of the freedom of expression of the media and pluralism in Albania, it considered that the proposed amendments to the law were not ready for adoption in their current form. The law suffered from debilitating vagueness and was very likely to have a *"chilling effect"* on the freedom of speech and media activities, suppressing free discussion and political speech in the Albanian sector of the internet.

Following the issuance of the Opinion in June 2020, the Government has yet to reflect the suggestions and criticism into an updated package, leaving the internet media sector, be that of any form, in a legal vacuum and free to behave beyond the commonly accepted ethical and legal standards with regards to the rights of the subjects of their news stories, with only the Civil Code[77] being to some degree a deterrent to unethical action by part of the latter, however with the plaintiff being burdened with all the procedural obligations stemming from a civil court process.

It is clear from this paper that the current legal and regulatory framework relating to privacy protection is quite truncated when compared to the media's right to information and dissemination of the latter. The absence of well-established regulations in this market segment allows it to flourish in total anarchy. That the new legal initiative's obligation to comply with both, the domestic constitutional framework and basic international requirements, has yet to be addressed by the government. Other options for intervention in this matter have been seen as crucial by local freedom of information activists and civil society organizations. At the same time, institutions tasked with protecting these fundamental rights have failed to enforce the law, or at least provide adequate resolution, with only a few cases evaluated and decided in over a decade. With no regulatory oversight and no accountability for their actions or their impact on the lives of the subjects of the stories, the media market, particularly online, is ripe for abuse and unethical practices.

4. Concluding remarks

In view of the current situation, where the number of online portals continues to rise exponentially from year to year and there is no objective means for an aggrieved citizens to identify the owners or administrators of a media outlet, and where it is impossible for state authorities, either due to the legal vacuum or lack of capacities to enforce their decisions or recommendations, new means of regulation are crucial to the healthy development of the press, especially with regards to the conflicting rights of the media and the subjects of the news.

[73] Ibid, para. 35-36.
[74] Ibid, para. 37.
[75] Ibid, para. 43-46.
[76] Ibid para. 60-63.
[77] Article 625 (Amended by law no 17/2012, dated 16/02/2012, Article 2).

The Kosovo Press Council[78] example is one possible avenues of remedy of the situation, with soft law as a means of regulating the behavior of the media, with blemishes on the reputation of the outlet having a higher degree of incentive for better behavior than the financial disciplining of the latter, an initiative that has been mirrored in Albania through the Alliance for Ethical Media,[79] a voluntary group of Albanian media dedicated to rigorously implementing the Code of Ethics for Journalists.[80]

Further to soft law, already existing institutions need to be strengthened, with the Data Protection Commissioner, despite having the purview of oversight on the issues, lacking significant decision-making since 2016, and the already existing legal framework having to be amended to adapt to the information technology society that has emerged in the later years, however, abiding to the best international standards and integrating the findings and opinions of the Venice Commission.

One final point of consideration is the need for depolitization of the already existing oversight institutions, per the findings of the European Commission for Democracy Through Law, as well as the regulation of media ownership in Albania, especially for online media and internet portals, as a means of remedy for potential plaintiffs to have the possibility of identifying likely respondents for civil suits. In tangent, the justice system needs to be reformed in order for libel, defamation and non-pecuniary claims to be examined within an acceptable timeframe.

[78] https://presscouncil-ks.org/?lang=en.
[79]https://www.coe.int/sq/web/tirana/-/albanian-alliance-for-ethical-media-establishes-self-regulation-mechanisms.
[80] https://kshm.al/kodi-i-etikes-se-gazetarit/.

The challenge of incorporating legal rules into digital applications: a theoretical exploration of article 25 GDPR

Efstratios Koulierakis Ph.D.[1]

1. Introduction

Nowadays, the improvement of computers' abilities, new means of storage of information and the wide use of internet have rendered the creation of 'digital dossiers' about almost every individual practically feasible (Solove, 2004). More recently, the use of smart phones and other smart items, such as televisions or watches, expose their users to a constant monitoring of their every-day life (Article 29 WP, 2014a, pp. 5-6).

The EU's General Data Protection Regulation (GDPR) pursues to address the threats for the rights of the data subjects in the digital era. According to article 25 GDPR, data controllers should adopt 'technical and organisational measures', in order to comply with the GDPR, 'by design and by default'. This legislative choice of the EU pursues to shape digital applications in such a way that they encompass data protection rules and principles into their architecture or their *code* in the famous formulation of Lawrence Lessig (2006). The idea of digital architectures incorporating data protection principles pre-existed the GDPR (see for example Cavoukian 2010).[2] The novelty of the article 25 GDPR is that it is a legally binding provision, obliging data controllers to encompass the data protection principles into technological applications, in general terms.

The present contribution explores this provision of EU law. The main research question is *how article 25 GDPR pursues to shape digital technology*. In order to answer this question the present paper first explores, *which are the addressees of article 25 GDPR and how this obligation relates to the role of product designers in the tech-industry*. Subsequently, it elaborates on the question of how far the obligation of article 25

[1] PhD researcher at the Faculty of Law, University of Groningen (The Netherlands), and member of the Security, Technology and e-Privacy Research Group, e.koulierakis@step-rug.nl. The author is an Early Stage Researcher within the KnowGraphs Project, the work of which is supported by the European Union's Horizon 2020 Research and Innovation Programme under the Marie Skłodowska-Curie Innovative Training Network, grant agreement No 860801. The ideas herein reflect only the author's view.

[2] A notable example is article 17 of the previous Directive 95/46 on data protection, which also referred to 'technical and organizational measures'.

GDPR reaches: *does article 25 GDPR require full, automatic compliance in every possible scenario or should the appropriate measures of compliance be identified on case-by-case basis*?

In section II, the present paper first examines article 25 from a doctrinal perspective. It elaborates on the rationale of article 25, it identifies the addressees of the provision and the moment in which this legal obligation applies. Section III examines how far the obligation of article 25 GDPR reaches and whether it is possible for controllers to achieve full automatic compliance, by design and by default. Section IV focuses on data protection by design (article 25(1) GDPR) and it elaborates on the guiding principles for the identification of the appropriate means of compliance with this particular provision. As a conclusion, the paper proposes a new approach on identifying means of shaping the design of digital applications.

2. Article 25 GDPR as a controller-obligation

A. An obligation to act

Article 25 GDPR, contains a positive obligation, in the sense that it is an obligation to act. The controllers should not only abstain from specific acts violating data protection rights, but they should also actively adopt data protection measures so as to comply with the Regulation.[3]

As it has been pointed out by Jasmontaite and others, article 25 GDPR is an obligation of result (2018, p. 174). In that sense, article 25 GDPR does not prescribe specific forms of actions for the controller. Instead, the provision sets a target: the legal obligations of the GDPR should be embedded in technological applications by design and by default.

The Regulation does not describe the means under which the controller may attain that target. Article 25 GDPR mentions methods of pseudonymisation as a means towards the desired outcome. However, means of pseudonymisation are one out of many techniques available to the controller. Furthermore, it is not mandated that all controllers should use data pseudonymisation techniques indiscriminately. Instead, it is up to the controllers to decide the appropriate methods to achieve the objectives of article 25. In other words, even though specific actions are defined indicatively, the emphasis remains on the end state (Westerman, 2018, p. 33). Article 25 GDPR primarily defines a result that ought to be achieved, not particular actions that should be performed.

B. An obligation ex ante

Although data controllers fall under the scope of the Regulation if they process personal data, article 25 GDPR introduces an obligation that applies earlier. More specifically, article 25 introduces protection of personal data ex ante. The controller should take into account the obligations deriving from the GDPR not only during processing but also at the time of determination of the means of processing. In other words, the controller should choose the appropriate technical and organisational measures, *before* the commence of data processing.

It can be mentioned at this point that article 25 GDPR is not the only example of an obligation ex ante in the Regulation. Article 35 GDPR, adopts the same logic,

[3] For the definition of the term 'controller', see GDPR article 4(7).

with regard to the data protection impact assessment (DPIA). According to that provision, when the processing is likely to result in a high risk for the data subjects' rights, the data controller is under the duty to undertake a DPIA, prior to the commence of the processing. It has to be clarified, that data controllers fall under the scope of the Regulation, from the moment that they begin to process personal data (GDPR, arts 2(1), 4(2)). However, if a controller fails to comply with GDPR's obligations ex ante, the moment that the processing starts, the data controller is already in breach of the Regulation.

Under this logic, if a data controller begins to process personal data, by the use of a digital application, the architecture of which fails to meet the requirement of article 25, the controller violates the Regulation, as early as the first moment of processing. Without the implementation of the data protection principles in the stage of development, the subsequent use of the application will not meet GDPR's requirements.

C. The question of responsibility

An interpretative issue relating to article 25 GDPR is the question of who should be responsible for the implementation of data protection by design and by default (Jasmontaite et al., 2018, pp. 171–172). If the data controller is the designer of a technical application, the answer to the question is straight forward: the controller-developer is under the duty to comply with article 25 GDPR. However, the answer is not that simple, if the data controller is not the one who designs the application. The legal obligations of the GDPR are formulated as controller obligations or processor obligations. Product designers fall outside of the scope of the GDPR as long as they do not process personal data themselves, either as controllers or as processors.[4] The persons or legal entities who design digital applications, without undertaking processing operations, are not obliged to comply with the pre-requisites of the Regulation (GDPR, arts 1, 4(1), 4(2), 4(7)). Therefore, data designers are the ones determining the architecture and the default settings of digital applications, whereas they do not necessarily fall under the scope of the Regulation.

Although the GDPR does not impose obligations to data designers directly, it is clear that it pursues to bring them into play, indirectly. According to recital 78, the GDPR pursues to 'encourage' the 'producers' of 'services and applications' to 'take into account the right to data protection when developing and designing such products, services and applications and […] to make sure that controllers and processors are able to fulfil their data protection obligations'.

Recital 78 is not legally binding and it cannot be a legal basis to impose obligations for persons, falling outside of the scope of the GDPR. However, recital 78 offers valuable guidance, as to the objectives of the Regulation. It clarifies that the GDPR aims at creating incentives for data designers to incorporate data protection principles into digital applications.

The underlying idea of article 25 GDPR is to place the burden of compliance on data controllers, in a way that they will only opt for digital solutions that comply with the Regulation by design and by default. This way, software and hardware designers

[4] For the definition of the term processor, see GDPR article 4(8); the scope of application of the GDPR is defined in art. 2(1); The term 'processing' is defined in article 4(2).

can be indirectly forced to incorporate data protection rules, into their digital products. Alternatively, product designers who produce applications incompatible with article 25, will not have their products purchased by data controllers. As Lee A Bygrave mentions, article 25 GDPR envisages a market where data controllers purchase products that incorporate data protection principles, and thus they stimulate the production of such products (Bygrave, 2017, p. 119).

It can be mentioned at this point that the previous Directive 95/46/EC on the Protection of Individuals with Regard to Personal Data Processing, failed to give incentives for incorporation of data protection technologies that predated the GDPR. This was pointed out by Peter Hustinx, who opined on the draft text of the GDPR, in his capacity as the European Data Protection Supervisor. In his view, data protection principles would become relevant for developers and producers of hardware and software, if data controllers were to be held accountable for adopting them (EDPS, 2012, p. 30).

Hence, designers of digital applications do not fall under the scope of the GDPR, as long as they are not controllers or processors. However, article 25 pursues to bring them into play indirectly. Since the GDPR forces data controllers to opt for digital solutions meeting the criteria of article 25, digital designers are forced by market incentives to meet the criteria of article 25. Otherwise, data controllers should not (and hopefully will not) purchase products of digital designers who do not take data protection and in particular article 25 GDPR seriously.

D. The moment of determination of the means of processing

Another interpretative question that arises in this point is when exactly is the moment of 'determination of the means of processing', mentioned in article 25 GDPR. Once again, there is a distinction to be drawn between cases where the data controllers design the digital application by their own means and cases where the designer is a person or entity other than the data controller.

In the first case, the 'moment of determination' of the means of processing coincides with the process of development of the digital application. In this scenario, the moment that the controller-product designer decides the structure of the programme, at that moment they determine the technical means of the processing. For example, if a start-up company designs a data processing phone application, that they aspire to operate themselves, the company is under the obligation to take into consideration article 25 GDPR, already at the stage of designing the application.

However, when the controller acquires the technical applications from a third party, it is not clear, how the controller falls under the scope of article 25. In the second example, the question of the moment of determination of the means of processing is not that simple.

In that regard, recital 78 can be a useful tool for the interpretation of the notion of 'the moment of determination of the means of processing'. As it was argued in the previous sub-section, the objective of article 25 GDPR is to influence the conduct of designers indirectly. By considering article 25 as a form of indirect regulation of the conduct of product designers, one can adopt an interpretation of the 'moment of determination of the means of processing', based on the purpose of article 25 GDPR.

More specifically, in a case where the data controller acquires the means of processing from a third party, the moment of determination of the means of processing, under article 25 is the moment of acquisition of the relevant product or service. According to this interpretation, data controllers are obliged to purchase products and services complying with article 25 GDPR. If data controllers fail to acquire means of processing that implement the rules and the principles of the GDPR, the data processing activity will be in breach of the Regulation.

By adopting this interpretation of article 25 GDPR the burden of compliance remains on data controllers, whereas product designers are given the incentive to incorporate data protection principles into their digital applications. If digital products do not meet article 25 requirements, data controllers should simply avoid them.

3. Delimitating the scope of article 25 GDPR

It has been argued so far that article 25 GDPR imposes a positive obligation for controllers to actively incorporate the rules and the principles of the GDPR into the architecture of their applications. The question that rises in relation to article 25 GDPR, is how far this obligation reaches. More specifically, it is clear that article 25 requires automatic compliance with GDPR requirements but it is a matter of interpretation, which requirements are subject to automatic compliance and to what extent there should be human intervention in the system for ensuring compliance with the Regulation. It should be clarified at this point that a complete technological fix, in a way that software automatically complies with every aspect of EU data protection legislation, without the need of subsequent intervention is conceptually impossible for the following reasons.

First, not all provisions of the GDPR are subject to compliance by design and by default. There are actions that data controllers should undertake, that are necessary for the legitimacy of the processing, whereas these actions do not affect processing operations as such (Koops and Leenes, 2014, p. 163). One such example is the obligation to conduct a DPIA. Other examples are the obligation to declare data protection breaches to the data protection authority and to the data subjects, as well as the obligation of prior consultation with the Data Protection Authority, where the DPIA indicates a high risk for the data subjects. These are examples, where the GDPR does not regulate the processing as such, but it imposes additional obligations to the data controller. Such legal requirements are not subject to compliance via technical and organisational measures.

Second, complete automatic compliance is impossible as designers cannot predict all possible occasions that may come up at the stage of data processing. More specifically, data controllers cannot apply the GDPR without identifying the context of the processing. On the contrary, data controllers should envisage data protection issues that may arise during the data processing and determine how such issues will be addressed, by prescribing ways of compliance. These ways of compliance are often referred to as 'policies'. These policies, should subsequently be transposed into code, in order to be automatically executed (De Vos et al., 2019, p. 49). According to Koops, the process of encoding legal rules into software can be described as 'identifying the

legal norm, moving from legal norm to techno-rule, and deploying the techno rule in practice' (2011, p. 190). This mental process requires that designers of digital applications predict all the possible ways in which the applications could be used. It is also necessary that designers pre-determine how every data protection issue conceptually possible, should be resolved in the form of policies. Even if there are examples where the uses of the product and the compliance methods can be pre-determined, this is a statement that definitely does not hold truth for all digital applications.

Third, even if the text of the GDPR remains the same, our understanding of the Regulation changes over time. Due to this 'dynamic' element of legal norms, compliance requires human intervention for the re-interpretation of the GDPR and the re-formulation of compliance policies (Koops and Leenes, 2014, p. 166). The understanding of a legal text requires references to legal documents that are not statutory laws. In EU data protection law, the case law of the CJEU and opinions of the EDPB are of extreme importance. The use of case law and soft law texts is very important for the interpretation of laws in general. However, such materials are even more significant when it comes to the GDPR, which is a piece of legislation that relies upon abstract formulations. The abstract formulations of the GDPR pursue to grant breathing space for the regulation to deal with a wide spectrum of activities and the unpredictable technological improvements.

4. The guiding principles for the identification of the means of compliance

A. Effective protection

Turning to article 25(1) GDPR, it is mentioned that the controller should adopt technical and organisational measures that will implement data protection principles in an 'effective manner'. This term indicates that article 25 prescribes results, not 'best efforts' or particular ways of conduct (Jasmontaite et al., 2018, p. 177). As the EDPB has opined in relation to the principle of effectivity in article 25(1): 'Article 25 does not require the implementation of any specific technical and organizational measures', as long as the implemented measures and safeguards achieve the desired effect (EDPB, 2020, p. 7).

Hence, article 25(1) GDPR defines effective implementation of data protection as a desired end-result but it prescribes no particular actions for the controller to achieve the end state. The controller should decide among the available methods of compliance and eventually build a compliance framework of technical and organisational measures that lead to effective data protection.

The question that arises at this point is what qualifies as effective protection. It should be clarified that article 25 GDPR does not go as far as requiring that the data controllers automatically comply with every legal provision of the Regulation. As it was argued in the previous section, such automatic compliance with every legal provision in the Regulation is impossible. However, the question of 'how much is enough?' requires further clarification.

In that regard, article 25(1) GDPR enlists certain elements that must be considered, for the determination of the means of processing. The elements that are mentioned in article 25 are: (a) the state of the art; (b) the cost of implementation; (c) the nature the scope context and purposes of processing; (d) the risks of varying

likelihood and severity for rights and freedoms of natural persons posed by the processing. These elements can function as the guiding principles for the identification of what constitutes effective data protection in relation to article 25 GDPR.

B. A risk-based approach

Article 25 GDPR adopts a risk-based approach to data protection (Bygrave, 2020, p. 576; EDPB, 2020, p. 9; Jasmontaite et al., 2018, p. 177). According to that provision, the controller should take into account 'the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing'. CNIL identifies data protection risks as, 'composed by one feared event (what do we fear?) and all the threats that make it possible (how can this occur?)' (2012, p. 6).

The idea of a risk-based approach can be better understood in juxtaposition with a harm-based approach (Article 29 WP, 2014b, p. 4). A harm-based approach is a legislative option, where the law responds to situations where a harmful event (or the 'feared event' that is to be avoided in CNIL's formulation) has already occurred. On the contrary, a risk-based approach moves the protection of persons a step further. More specifically, a risk-based approach does not only react to an adverse effect that has occurred, but it also pursues to prevent it or mitigate the harm potentially caused by the event, in advance. A risk-based approach requires the identification of possible harms for the persons' rights and enforces measures for the harmful event to be avoided.

It should be mentioned that there is no general agreement between theorists, as to what constitutes a harm in the domain of data protection (Kuner et al., 2015, p. 97). However, it is generally agreed that this notion includes both physical harms and intangible harms (Kuner et al., 2015, p. 97).

The idea of a risk-based approach to data protection appears in many aspects of the Regulation (EDPB, 2020, p. 9). Most notably, a DPIA is a process for identifying in advance the possible harms, deriving from data processing. At this point, it becomes apparent that there is a close connection between the DPIA and the risk based approach of article 25 GDPR. The DPIA is a method of identification of risks, whereas article 25 requires measures against those risks. The same principles for identification of dangers in relation to DPIA, apply in relation to article 25 (EDPB, 2020, p. 10).

According to the risk-based approach of Article 29 WP, the higher the risk for the data subjects, the stricter the measures that should be implemented by the controller. There are less safeguards required in small-scale, simple and low-risk data processing (Article 29 WP, 2014b, p. 3). However, this conclusion does not imply by any means that the GDPR accepts the violation of data subject rights if such violation is less harmful (Article 29 WP, 2014b, p. 4; Kuner et al., 2015, p. 97). On the contrary, the risk-based approach requires the adoption of additional measures in relation to data processing, with the idea of providing extra layers of protection, if a violation to data subject rights is more harmful.

In that sense, the risk-based aspect of article 25 calls for a balancing exercise: on the one hand there are the legitimate aims pursued by the data controller and on the other hand there are 'the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing'. The higher the risk for the data subjects, the more measures of compliance by design the controller should implement.

C. The nature the scope, the context and the purposes of processing

Article 25 GDPR requires that the controller considers the 'nature, context, scope and the purposes of the processing'. The 'nature' of the processing, should be distinguished from the nature of personal data and whether such data belong to special categories of data, under article 9 GDPR. The nature of the processing refers to the 'intrinsic features' of data processing, such as the technical means of the processing, whether the individuals are subject to profiling or whether the data are aggregated with data from different sources (Jasmontaite et al., 2018, pp. 178-179). Different technical environments require different technical solutions for compliance. Hence, effective protection under article 25 is not a fit-for-all solution but a solution that should be re-adjusted in relation to a specified technical environment. For example, when it comes to techniques of profiling or aggregation of data from multiple sources, effective protection under article 25 GDPR requires stricter safeguards of compliance by design.

The 'scope' and the 'context' of the processing refer to wider environment in which the data are processed (Jasmontaite et al., 2018, p. 179). To that effect, the controller should take into account whether the data fall under the scope of article 9 GDPR or whether such data may reveal intimate aspects of a person's life. In these examples the data controller is expected to adopt stricter technical and organisational measures for the protection of the data subjects rights.

When it comes to the 'purposes' of the processing, this aspect of article 25(1) is closely connected to the principle of purpose limitation under article 5(1)(b) GDPR. This aspect of article 25(1) obliges data controllers to determine the purposes of the processing in advance and use such applications that their structure limits the data processing to the initially specified purposes.

D. The state of the art

The 'state of the art' element of article 25 GDPR is concerned, it refers to both technological applications of data processing but also to organisational measures (EDPB, 2020, p. 8). In that regard, the controller should be constantly updated in relation to technical means posing threats to the data subjects. Furthermore, the controller should be aware of data protection technologies, available in the market in order to address those threats (EDPB, 2020, p. 8; Jasmontaite et al., 2018, p. 176). Especially in relation to organisational measures, article 25 requires up-to-date training of the employees with regard to processing technologies (EDPB, 2020, p. 8). Article 25 further requires that the controller keeps up with new ideas in the domain of data protection policies and implementing them if necessary (EDPB, 2020, p. 9).

E. The cost of implementation

Article 25 also refers to the cost of implementation for the controller, when deciding the appropriate technical and organisational measures. More precisely, the controller should make the budgetary commitments for the adoption of the relevant data protection measures. In its opinion on article 25, the EDPB clarifies that the cost for the controller, should not only be perceived in terms of money spent for acquiring

the tools for compliance, but also '[the] resources in general, including time and human resources' (2020, p. 8).

The economic considerations of article 25 should not be understood as a right of the controller to conduct a cost-benefit analysis before determining the appropriate means of processing. In other words, this expression does not refer to a balancing between the economic interests of the controller and data subject rights, with the purpose of identifying the appropriate technical and organisational measures.

On the contrary, this formulation is all about the controller's obligation to make an economic planning with the purpose of complying with the GDPR prerequisites. As the EDPB puts it, the economic incapacity is not an excuse for the controller to circumvent compliance by design (2020, p. 8). The reference to the cost of implementation in article 25, is not a reason not to implement data protection measures but something that the controller *should* consider in advance.

It is to be clarified at this point that the GDPR does not disregard the economic interests of the controller. On the contrary, the legitimate interest of the controller is one of the legal grounds for data processing, as long as it is not overridden by the rights of the data subjects (GDPR, art 6(1)). As the CJEU has clarified, EU data protection law, 'precludes a Member State from excluding, in a categorical and generalised manner, the possibility of processing certain categories of personal data, without allowing the opposing rights and interests at issue to be balanced against each other in a particular case' (*ASNEF*, 468/10 para 48; see also *Asociația de Proprietari*, C-708/18, paras 52-53; *Breyer*, C-582/14, para 62). It becomes apparent that domestic legislation and domestic courts should take into account the legitimate interests of the controller (*ASNEF*, C-468/10, paras 46-47).

As AG Jääskinen has opined, the controller's right to conduct business can be balanced against the data subject's fundamental rights to private life and data protection (CFREU, arts 7, 8, 16; Opinion of AG Jääskinen in Google Spain and Google, C-131/12 para 95.). For example, in *Asociația de Proprietari*, the CJEU uphold that the GDPR did not (in principle) preclude the property owners in the case, to establish a video surveillance system with the purpose of protecting their property (para 60).

It becomes apparent that the GPDR may require a balancing exercise, between the economic interests of the data controllers and the data subject rights. On that basis, there can be an evaluation of whether data processing is legitimate or not. Subsequently, there has to be an evaluation of what are the necessary measures with the purpose of achieving compliance by design. After the appropriate measures have been identified, the controller should plan and expend for the implementation of those measures. In that regard, the data controllers may not make discounts in compliance by design, with the claim that the measures constitute an excessive economic burden.

As Jasmontaite and others convincingly point out, '[t]he exact amount that is invested in these measures should depend on the nature, scale, context of the processing as well as on information sets that are going to be processed' (2018, p. 178). Hence, one cannot determine a percentage that controllers, in general, should commit to data protection compliance. This percentage varies from controller to controller, as the necessary safeguards are different. It should be clarified however, that article 25 does not impose an obligation for the controller to opt for the most expensive means of compliance. As EDPB mentions, '[t]he cost element does not require the controller

to spend a disproportionate amount of resources when alternative, less resource demanding, yet effective measures exist' (2020, p. 9).

5. Conclusion

Article 25 GDPR constitutes an indirect means of regulation of innovation: It places an obligation on data controllers with the purpose of influencing the conduct of multiple stakeholders in tech-industry. It does so by obliging data controllers to opt for digital applications that comply with the GDPR, when they design or acquire means of processing. This way, the GDPR aspires to influence the design of digital applications, in a way that they incorporate data protection values into their architecture.

This obligation of compliance ex ante does not go as far as requiring full automatic compliance with every legal provision in the Regulation. On the contrary, it is about incorporating certain safeguards that pursue automatic compliance with processing rules and protection of the data subjects' rights.

In that regard, article 25 GDPR offers guidance, as to what has to be considered, for the determination of the design of digital applications (article 25(1)). Data controllers should first identify what it takes for the processing to comply with the Regulation. This is a process that requires a consideration of the nature, the scope and the wider context of the processing. Moreover, controllers should identify the purposes of the processing in advance, in accordance with the principle of purpose limitation. Subsequently, they should identify technical and organisational measures that fit the particular technological framework of the processing. This is not an once-for-all process, as data controllers should be updated with regards to new technical measures and administrative practices that ensure compliance with personal data protection. Eventually, the choice of technical measures available is a matter of balancing: the higher the risks for the data subject rights, the stricter safeguards that controllers should adopt under article 25(1) GDPR. After identifying the necessary technical and organisational measures, data controllers should consider in advance, how these measures will be implemented, from an economic perspective.

These principles can guide the interpreter of the Regulation, but even so there is a big degree of abstraction in the formulations of article 25(1) GDPR. As it was argued, if there is a high risk for the data subjects, the data controller should implement stricter measures. However, the concept of risk in the domain of data protection remains a vague concept, whereas it is not clear what constitutes a harmful impact that should be avoided. Moreover, as article 25 GDPR imposes an obligation of outcome, it is up to the controllers to demonstrate that they achieved the outcome. Compliance measures under article 25 should be demonstrated in a way that the data protection authorities can assess the attainment of the targets, set forth by this provision (EDPB, 2020, p. 7; Jasmontaite et al., 2018, pp. 77–78).

The questions regarding identification of threats for the data subjects and about the process of demonstrating compliance are very important when the interpreter pursues to apply the abstract formulations of article 25(1) GDPR in practice. Article 25(3) GDPR seems to be of extreme relevance with regard to these questions. This provision refers to GDPR's certification scheme as a means of demonstrating

compliance with article 25. There is ground for further research, as to how the certification scheme of article 25(3) relates to compliance with the prerequisites of article 25.

Sources

Legislation

Charter of the Fundamental Rights of the EU [2012] OJ C326/392 (CFREU)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31(Directive 95/46 on Data Protection)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 (GDPR)

Case law

Judgement of 24 November 2011, *ASNEF*, C-468/10, C-469/10, ECLI:EU:C:2011:777

Judgement of 19 October 2016, *Patrick Breyer*, C-582/14, ECLI:EU:C:2016:779

Judgement of 11 December 2019, C-708/18, *Asociația de Proprietari bloc M5A-ScaraA*, ECLI:EU:C:2019:1064

Opinion of AG Jääskinen of 25 June 2013, *Google Spain and Google*, C-131/12 , ECLI:EU:C:2013:424

Bibliography

Article 29 WP, 2014a. Opinion 8/2014on the Recent Developments on the Internet of Things. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (accessed 15 July 2021)

Article 29 WP, 2014b. Statement of the WP29 on the role of a risk-based approach in data protection legal frameworks. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf (accessed 15 July 2021)

Bygrave, L.A., 2020. Article 25. Data Protection by Design and by Default, in: Kuner, C., Bygrave, L.A., Docksey, C. (Eds.), The EU General Data Protection Regulation: A Commentary. OUP, Croydon, UK.

Bygrave, L.A., 2017. Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements. Oslo Law Review 4, 105–120.

Cavoukian, A., 2010. Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D. IDIS 3, 247–251. https://doi.org/10.1007/s12394-010-0062-y

CNIL, 2012. Methodology for Privacy Risk Management, How to Implement the Data Protection Act (English Translation).

De Vos, M., Kirrane, S., Padget, J., Satoh, K., 2019. ODRL policy modelling and compliance checking. Lecture Notes in Computer Science 11784, 36–51.

EDPB, 2020. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0. https://edpb.europa.eu/our-work-

tools/documents/public-consultations/2019/guidelines-42019-article-25-data-protection_en (accessed 15 July 2021)
EDPS, 2012. Opinion of the European Data Protection Supervisor on the data protection reform package. https://edpb.europa.eu/our-work-tools/documents/public-consultations/2019/guidelines-42019-article-25-data-protection_en (accessed 15 July 2021)
Jasmontaite, L., Kamara, I., Zanfir-Fortuna, G., Leucci, S., 2018. Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR. European Data Protection Law Review 4, 168–189. https://doi.org/10.21552/edpl/2018/2/7
Koops, B.-J., 2011. The (In)Flexibility of Techno-Regulation and the Case of Purpose-Binding. Legisprudence 5, 171–194.
Koops, B.-J., Leenes, R., 2014. Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law. International Review of Law, Computers & Technology 28, 159–171.
Kuner, C., Cate, F.H., Millard, C., Svantesson, D.J.B., Lynskey, O., 2015. Risk management in data protection. International Data Privacy Law 5, 95–98. https://doi.org/10.1093/idpl/ipv005
Lessig, L., 2006. Code Version 2.0. Basic Books, New York.
Solove, D.J., 2004. The Digital Person – Technology and Privacy in the Information Age. New York University Press, New York, London.
Westerman, P., 2018. Outsourcing the Law: A Philosophical Perspective on Regulation. Edward Elgar, Cheltenham, UK; Northampton, MA, USA.

Stitching lacunas in Open Source Intelligence – Using ethics to fill up legal gaps

Dr Jonida Milaj – Prof Dr Jeanne Pia Mifsud Bonnici[1]

1. Introduction

OSINT or open source intelligence is intelligence gathered from data that are publicly available in open sources, among which one can mention the internet, social media, newspapers, radio and television, government reports or even professional and academic literature. As technology develops, the volume of available data increases making organisations and individuals to rely for their intelligence purposes often solely on OSINT rather than on private and classified information. Economic evaluations as well as the easy accessibility and availability of OSINT tools and techniques has influenced the use of this method. Furthermore, there is a general believe that because the first material, the data, are publicly available, there should be no concerns about compliance with any data protection or privacy rules.

The Open Data Directive adopted in June 2019 addresses only data held by public sector bodies in the Member States, at national, regional and local levels, such as ministries, state agencies and municipalities, as well as organisations funded mostly by or under the control of public authorities. It focuses on the economic aspects of the re-use of information rather than on access to information by citizens and, encourages Member States to make as much information available for re-use as possible. The scope of this law is thus limited and it does not cover the use of OSINT for open data in social media platforms. Since there are no specific rules applying to OSINT at European level, for protecting the fundamental rights to privacy and data protection of individuals, the general legal framework becomes crucial.

This paper takes a legalistic and human rights approach and analyses in how far the use of open data from social media platforms for intelligence purposes is compatible with the fundamental rights of individuals and especially with data protection and privacy rules in the European Union.[2] As with many responsible data

[1] The authors are part of the Security, Technology and e-Privacy (STeP) research group, University of Groningen, Groningen, The Netherlands. This research was conducted in the framework of the MIRROR project that has received funding from the European Union's Horizon 2020 Research and Innovation Action Program under Grant Agreement No 832921.

[2] For the distinction between OSINT and SOCMINT please see: <https://privacyinternational.org/explainer/55/social-media-intelligence> accessed 5 May 2021.

concerns, legal compliance is just one part of a much bigger picture and it often forms the lowest rather than the highest bar one should strive for. In this light, the paper further elaborates on ethical concerns that are behind the legal rules and analyses how to use ethics for filling any gaps in the laws and ensure the protection of the fundamental rights of the individuals.

After this short introduction, in section 2 more information on the way OSINT operates is given. Section 3 analyses the compliance of OSINT with data protection and privacy rules. Section 4 goes one step further in identifying ethical concerns in the use of OSINT and elaborates upon the role of ethics in addressing these concerns. In section 5 a number of recommendations on how to use ethics for filling in legal gaps in OSINT are presented. The concluding remarks are presented in section 6.

2. Understanding OSINT and the information used

OSINT techniques allow for access to open-source data for anyone, anywhere and with any legal means. Those means can include tools and knowledge that are freely accessible and free in use. Thus, the OSINT 'miner' or user can range from an average enthusiast behind a computer to global intelligence agencies.

However, in literature OSINT is often referred to as a grey area. The reason for this is that while on one side OSINT can be a seemingly open, free and transparent system without legal restraints, on the other side it is also a system increasingly used by intelligence agencies with the aid of special techniques. The later questions the extent of the legal restraints on the techniques and on their use.[3]

In order to analyse the legality of OSINT uses, first the type of information used by an agency or individual must be identified. This is normally divided into four categories:

- White information;
- Grey information;
- Black information;
- Non-existing information.

White information is completely available to the public, is open and according to estimates, amounts to 90% of all data used in intelligence. Grey information is distinguished from white and black information because, even if not completely available all that is required to access it is to find the correct communication channel (e.g., universities, corporations or government institutions). You need to be a member of an organization in order to access this information but you do not need other special qualities (for example getting access to the archives of the city or becoming a member of a specific library in order to learn if a book is available). Black or classified information is not freely of semi-freely available and it is retrieved through covered activities. According to estimates, it constitutes only around 0,9% of all information used in intelligence activities.[4] The last category, non-existing information refers to information that cannot be found or accessed as such in open, semi-open or closed sources but it is deduced on the basis of other existing information.

[3] Gašper Hribar , Iztok Podbregar and Teodora Ivanuša, 'OSINT: A"Grey Zone"?' (2014) 27(3) International Journal of Intelligence and CounterIntelligence 529.
[4] Hribar, Podbregar and Ivanuša (n 3).

The legality of OSINT practices can thus be analysed based on the type of information used. This paper focuses only on the first category of information, white information, and only with regard to social media. White information on social media is freely accessible and available without the need of, for example, creating fake accounts or presenting fake credentials. In a more thorough legal research of privacy expectation in intelligence gathered by social media in the United Kingdom, Edwards and Urquhart argue that, currently, no privacy protection is given to white information.[5] Identifying the same problem and making a further step to offer some legal restraints to OSINT, Koops, Hoepman, and Leenes propose an integration of privacy by design in the systems of OSINT.[6] Both of these approaches indicate how current legal restraints to OSINT are lacking and require broader normative reasoning, especially given the very high percentage that the use of this technique based on white information occupies in intelligence activities. The following section will analyse how OSINT focusing on white information gathered from social media is considered in light of data protection and privacy rules in the EU.

3. Data protection and privacy concerns

As seen in the previous section, OSINT operates by harvesting open data that are freely available. These can be text, images, audio, etc. Being openly accessible though, does not change the qualification of some of these data as personal ones.[7] The public accessibility of the data makes many actors assume that using these data does not raise any responsibilities for addressing lawful data processing[8] or privacy criteria. For not falling into this fallacy, we will analyse below if the use of open data in a OSINT context complies with the legal rules. First data protection and then privacy concerns are addressed.

i) Data protection

There are two main data protection laws operating at EU level. The GDPR and the Police Directive.[9] Since this paper focuses on the use of open data in general and on OSINT practices available to individuals or organisations, without limiting our research to intelligence agencies or law enforcement activities, the GDPR is the relevant law. The Police Directive is not directly applicable to this general research given its limited material and personal scope of application.[10]

---

[5] Lilian Edwards and Lachlan Urquhart, 'Privacy in Public Spaces: What Expectations of Privacy Do We Have in Social Media Intelligence?' (2016) 24 International Journal of Law and Information Technology 279.

[6] Bert-Jaap Koops, Jaap-Henk Hoepman and Ronald Leenes, 'Open-Source Intelligence and Privacy by Design' (2013) 29 Computer Law & Security Review 676.

[7] Regulation (EU) 2016/679 0f the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (GDPR) [2016] OJ L119/1, art 4(1).

[8] Art 5 GDPR.

[9] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and the repealing of Council Framework Decision 2008/977/JHA (Police Directive) [2016] OJ L119/89.

[10] Art 1(1) Police Directive.

'Personal data' are defined in the GDPR as any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person, on the other side, is the one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Only a complete and irreversible anonymization of the data used would make the GDPR inapplicable. The GDPR does not regulate explicitly the use of open source data. However, as long as these data fall within the definition of personal data the general legal framework applies.[11]

For complying with the data protection framework, attention must be paid to the principles of lawful data processing established in article 5 GDPR, namely: (a) lawfulness, fairness and transparency; (b) purpose limitation; (c) data minimization; (d) accuracy; (e) storage limitation; (f) integrity and confidentiality; and (g) accountability. Furthermore, for personal data to be processed, compliance with the principle of lawfulness is very important. This principle requires compliance with one of the conditions established in article 6 GDPR.

For open source data collected from the social media, the condition of consent for processing the data cannot be established. Making personal data available does not automatically qualify as giving the consent to whomever has access to these data to process them as deemed necessary. Furthermore, we are all aware of the fact that often our personal data online are not made available from us, but from others. In this situation, processing of open data for research purposes in academia, for example, can be considered as lawful under the justification of performance of a task carried out in the public interest.[12] Open data processed for other OSINT purposes must comply as well with one of the conditions prescribed in art 6 GDPR.

In addition, some of the processed data might qualify as sensitive ones.[13] A personal image, for example, might reveal the religion of the data subject or his ethnic origin. Such sensitive information might also be part of posts data subjects have made in social media platforms.[14] According to the GDPR, processing of sensitive data should not take place unless falling under specific situations for which such processing can be justified. The justification of article 9(2)(e) GDPR on data that are made manifestly public needs to be considered in a restrictive way and always in combination with the fulfilment of the conditions for lawful data processing in art 6 GDPR. In the absence of a clear definition and understanding of the limits of use for data made manifestly public,[15] the protection of the rights of individuals should prevail. As a result, any processing of open data that qualify as personal data must comply with the data protection regime in the EU.

[11] C-73/07 *Satakunnan & Satamedia* EU:C:2008:727, paras 46-49.
[12] Art 6(e) GDPR.
[13] Under the category of sensitive data fall personal data that have the potential to reveal the racial or ethnic origin of the data subject, his political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
[14] Art 9(1) GDPR.
[15] Case T-320/02 *Esch Leonhardt v ECB* EU:T:2004:45; Edwards and Urquhart (n 5).

ii) The right to privacy

While the processing of open personal data needs to comply with the legal rules, OSINT is intelligence that derives from the analyses of such data. The information obtained may go far beyond what the individuals have made public and thus severely interfere with their private sphere.

The right to privacy as defined in article 8 ECHR and article 7 of the EU Charter of Fundamental Rights protects the private sphere of the individuals which seems from the wording of the articles as projected mainly in private spaces (private and family life, home and correspondence). When someone exposes himself in a space that is open to the public, including also the cyberspace, he creates the possibility to be visible to others whom have a right to observe what goes on around them. It is, however, one thing to be seen in public and another one to be tracked. The protection of the private sphere of the individuals would not be complete if data collected and recorded about their activities in public spaces are not covered.[16]

In Europe, the extension of the private sphere of individuals to the public space is to be found in the jurisprudence of the European Court of Human Rights. The capture of an event changes its nature from a simple observation to a record and, it is the systematic or permanent storage of data collected in open spaces as well as their compilation, processing, use or disclosure that makes these data fall under the protection of the right to privacy.[17] In *P.G. and J.H.* the European Court of Human Rights dealt with the scope of the right to privacy in public spaces establishing that: "*Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain*."[18] The same Court confirmed in *Perry* that the right to privacy exists also outside a person´s home or private premises.[19] While a simple viewing of activities, even if aided by technology, without any recording is considered as compatible with the right to privacy,[20] the situation changes as a result of new technologic developments which systematically or permanently record the data. Even though the above reasoning was designed for the physical world, the same logic can be easily extended to cyberspace and activities that individuals perform in social media.

Furthermore, individuals might still have a reasonable expectation of privacy for activities taking place in public. The reasonable expectation of privacy is to be seen mainly as a subjective element, linked with the feelings and expectations of an individual.[21] In *Rotaru* for example, the ECtHR recognized that an expectation of privacy followed by the right to protect it exists when a government agency systematically collects and stores personal information, even when this information is public.[22] Furthermore, in *Perry* the ECtHR reasoned that an individual has a reasonable expectation of privacy when could have not been reasonably expecting the

[16] Teresa Scassa, 'Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy' (2009) 7(2) Canadian Journal of Law and Technology 193.
[17] Sjaak Nouwt, 'Reasonable expectation of geo-privacy?' (2008) 5(2) SCRIPT-ed – A Journal of Law, Technology and Society 375.
[18] *PG and JH v The United Kingdom*, ECHR application no 44787/98, 25 September 2001, para 57.
[19] *Perry v The United Kingdom*, ECHR application no 63673/00, 17 July 2003, para 37.
[20] *Perry v The United Kingdom* (n 19), para 38.
[21] Tomas Gomez-Arostegui, 'Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations' (2005) 35(2) California Western International Law Journal 153.
[22] *Rotaru v Romania*, ECHR application no 28341/95, 4 May 2000, para 43.

use of technology for scopes beyond the normal foreseeability of their use.[23] The same reasoning would apply also with regards to OSINT since individuals using social media without the proper privacy filters are not expecting that the data will be harvested and processed for OSINT purposes. As a result, the right to privacy as established in article 8 ECHR and article 7 of the European Charter must be protected also in those cases in which data are made public from individuals themselves.

4. Ethics and Ethical concerns of OSINT practices

It is a well-known fact that technology is developing at a fast pace and answering the legal challenges proves difficult. Adopting proper legislation requires time and ethics are therefore of paramount importance as they can be considered as "soft law" even in absence of an ethical framework *stricto sensu* to respect. Even in a modern society governed by the rule of law unwritten laws keep existing and regulating behaviours.[24] Ethics goes far beyond the laws to consider ways of behaviour that would not cause harm to others.[25]

There are a number of legal instruments in the EU that have incorporated ethical provisions and that have contributed to raising some ethical concerns to the level of legally binding provisions. Some of these can be found also in the GDPR as well as in the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the European Union (CFR). The concept of human dignity, for example, present in the GDPR in article 88 and in Recital 4, is interpreted as containing "a very general ethical reference" when it says that "[t]he processing of personal data should be designed to serve mankind."[26] The concept is also found in art 1 CFR.[27] The ECHR and the CFR are a source of ethical norms when they empower individuals to control the way information about them is collected and used via the right to privacy[28] and the right to data protection.[29]

Moreover, according to the Ethics Guidelines for Trustworthy Artificial Intelligence from the European Commission, trustworthy AI should be respecting ethical principles and values.[30] They emphasise the need for transparency and accountability that is also present in the GDPR,[31] as well as the criteria for consent,

---

[23] *Perry v The United Kingdom* (n 19), para 41.

[24] This stems from Aristotle's Nicomachean Ethics in which he distinguishes between "the legal or conventional justice (that is achieved by applying legal rules) and natural justice (which remains valid everywhere, hence independent of particular laws)" - see Georgeta-Bianca Spîrchez, 'The relation between ethics and law', (2016) 1 Fiat Iustitia, 189.

[25] Ferdinand Curtney French 'The Concept of Law in Ethics' (1893) 2(1) The Philosophical Review 35.

[26] Hielke Hijmans and Charles Raab, 'Ethical Dimensions of the GDPR' (2018) in: Mark Cole and Franziska Boehm (eds) *Commentary on the General Data Protection Regulation* (Cheltenham: Edward Elgar, 2018) 2, available at <https://ssrn.com/abstract=3222677> accessed 30.3.2021.

[27] Art 1 CFR "Human dignity is inviolable. It must be respected and protected. "

[28] Art 8 ECHR and Art 7 CFR.

[29] The right to data protection is not explicitly mentioned in the text of the ECHR but the European Court of Human Rights has based it on the 'general' right to privacy in several decisions. See for example: *Leander v Sweden*, ECHR application no 9248/81, 26 March 1987, para 48; *Kopp v Switzerland*, ECHR application no 23224/94, 25 March 1998, para 53; *Amann v Switzerland*, ECHR application no 27798/95, 16 February 2000, para 69.

[30] AI HLEG, 'Ethics guidelines for trustworthy AI' [2019] available at <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai> accessed 13.3.2020.

[31] See for example art 57(1)(b) GDPR.

transparency, diversity, non-discrimination and privacy.[32] The principle of fairness is also considered a component of ethics. As such, article 5(1)(a)) GDPR "elaborates this and associates it with transparency" although this is not agreed by everyone.[33]

While there is no legal obligation to comply with ethics apart from those mentioned, this does not mean that engaging in OSINT, one should not respect them. The development of technology is faster than the adoption of legal responses and ethics are therefore of crucial help as they play the role of 'soft law' standards. In the same way OSINT has to comply with the rights to privacy and data protection from the beginning, it also must respect the ethical safeguards which have reached the level of legally binding provisions as well as other ethical concerns not legally binding. The rationale lies in the nature of the EU itself. It is governed by the rule of law enshrined in Article 2 of the Treaty on European Union, which is a prerequisite for the protection of all fundamental rights in the EU.[34] Especially, the rule of law in the EU aims at strengthening mutual trust between actors, in particular between citizens and governments. Even if ethics are not law, observing them contributes to pacifying relations in the EU. Moreover, ethics can often be found in the legislation since the role of law often consists in making ethical choices.

The main ethical concerns identified when engaging in OSINT practices are explained below.

i) Dignity and autonomy of individuals

OSINT practices mean that there is a risk that people are associated to a mere set of data and that entails a risk for their autonomy as human beings and for their dignity. Collecting data from individuals without informing them about this activity might emphasise the idea that data speak for the individual and that there is no need to get the information directly from them since data already does it for them. Thus, getting data about individuals without their involvement can be problematic regarding their autonomy and dignity as human beings.

ii) Trustworthy data, dignity and autonomy

Furthermore, it is problematic to collect data retroactively since past data potentially does not reflect what the person thinks and is now, and the same applies concerning the group they belong to. This concern would rise in case OSINT engages in individual profiling. This is linked to the question of how can we be sure that the data is trustworthy. Indeed, deeming a person to have kept the same ideas and opinions over the years can be harmful for her or his right to autonomy and therefore damage the human dignity. Thus, the period time should be considered when harvesting data and machine learning should be designed in a way that does not reach too far in the past and adopt a dynamic approach regarding people's development.

---

[32] AI HLEG, 'Ethics guidelines for trustworthy AI' [2019] available at <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai> accessed 13.3.2020.

[33] Hielke Hijmans and Charles Raab, 'Ethical Dimensions of the GDPR' in: Mark Cole and Franziska Boehm (eds.) *Commentary on the General Data Protection Regulation* (Cheltenham: Edward Elgar, 2018) 2.

[34] Dimitri Kochenov and Laurent Pech, 'Upholding the rule of law in the EU: on the Commission's 'pre-article 7 procedure' as a timid step in the right direction' (2015) Working Paper, EUI RSCAS, 2015/24, Global Governance Programme-164, Global Economics.

iii) Discrimination

This issue of discrimination can be found regarding the origin of the data that is analysed. Whose data are processed and how are specific categories of individuals targeted? It can be a problem to decide to focus on a specific national group or on a certain gender or age. Issues relating to autonomy can be seen with the risk that the data found on those grounds will help making shortcuts about people. In particular, there is a risk that it leads to individual or group profiling.

iv) Risks of biases, creation of stereotypes and discrimination

Furthermore, the data cannot speak for itself since it is something intangible and that does not have an existence on its own. It is a mere emanation of a human being. To understand what is really behind the data, it must necessarily be interpreted. As a result, risks of biases from actors appear. The ethical dilemma raises concerns on how far one can trust a computer program to grasp the opinion of someone based on available data or even of a whole population. Careful consideration must therefore be given to the way computers potentially reproduce the biases that already persist within society. That problem is linked to the extent to which computers can be trusted. Who will decide whose data is harvested is a key question. Moreover, data mining processes often rely on simplistic stereotyping of the target, the outcome of such searches may also be discriminatory consequently.

v) Chilling effects

The use of OSINT techniques can also produce chilling effects in the society. The consequence of using such technology can be a change in the behaviour of individuals: knowing that their feelings, opinions, ideas are analysed, they might decide to auto-censor themselves to avoid the screening of their social media. This can have chilling effect on certain human rights, notably freedom of expression. Risks of biases and shortcuts resulting from a look at the group and not at the individuals alone can be harmful to the perception other people have of that group. Discrepancies can arise from a simplistic analysis of individual's data while they do not necessarily reflect his opinions, and even less those of a whole group. Wrong ideas concerning a certain group of origin can be extremely harmful.

5. Introducing ethical safeguards

It is often said that laws are nothing more than codified ethics and that all laws are designed with ethical concerns in the background.[35] But a problem that we face nowadays is that the laws lack far behind any technological development. In the absence of specific legal regulation, the general legal framework applies but, as it was seen in the previous section, the later does not address all the potential ethical concerns that might arise by the use of specific technologies. As a result, the ethical concerns remain unaddressed with the risk of being projected into ineffective safeguards for the fundamental rights of the individuals.

[35] See Giovanni Buttarelli, 'An ethical approach to fundamental rights' (1 December 2016, EDPS Blog) <https://edps.europa.eu/press-publications/press-news/blog/ethical-approach-fundamental-rights_fr> accessed 1.12.2019, mentioning a quote often attributed to Mahatma Gandhi.

Since compliance with the legal rules often forms the lowest bar rather than the best practice one should strive for, it is important not to limit oneself to the legal aspects of the use of a new tool or of OSINT technology but to address also all potential ethical concerns at the upfront. Ethics goes far beyond the laws to consider ways of behavior that will not cause harm to others. In case of OSINT practices, the main harm to the individuals is the interference with their fundamental rights. Basing behavior on ethics would mean to safeguard the fundamental rights to privacy and data protection in the presence of legal lacunas.

The previous section identified a number of ethical concerns and highlighted their nature. Even though these concerns escape the current legal regulation and ethics are not *per se* legally binding, it is still possible to design a course of action, linked to their nature, in order to address them without falling in the fallacy of ethics washing.[36] Firstly an upfront, we can raise the awareness of designers and users of OSINT technologies about potential ethical concerns to help in addressing these issues at an early stage.

Secondly, we can add ethical concerns to a necessity and proportionality assessment before the introduction of any OSINT technologies. However, given the fact that these principles lack a normative value the risk remains that adding ethical concerns to the equation will not help. Ethics also lack in normative value and will only add some smoke to the already existing gray area of the application of the principles of necessity and proportionality without addressing the problem.

Thirdly, we can link any ethical concerns, depending from their nature, with pre-existing legal requirements. If ethical concerns are linked with the design of the tool, for example, we can address these concerns at an early stage and make them part of the data protection by design and default assessment. Since data protection by design is already a requirement of the data protection framework, we can add ethical concerns to such an assessment and address them to an early stage. We can extend any data protection impact assessment methodologies that will be undertaken to cover also ethical concerns. We would thus design not only a data protection impact assessment but also integrate it with an ethical impact assessment. In the same line, if the ethical concerns derive from the way of operating of the tool, we can identify the concerns and compile them in codes of ethics as well as in approved codes of conduct that will be obligatory to comply with and prescribe legal consequences for the users of the OSINT technology. In this way, we would be able to address legal concerns that do not yet find protection in the laws and at the same time fill in lacunas that we currently find in the legal framework regarding OSINT. Below follow a number of suggestions on how to extend existing legal requirements for addressing ethical concerns:

a) Ethics by design

While the concept of 'data protection by design' contained in the GDPR obliges controllers of personal data to implement technical and organisational measures, at the earliest stages of the design of the processing operations, to safeguard data

[36] Ben Wagner, 'Ethics as an Escape from Regulation: From ethics-washing to ethics-shopping?' in Mireille Hildebrandt (ed), Being Profiling. Cogitas ergo sum (2018, Amsterdam University Press) 84.

protection principles right from the start,[37] the concept of 'ethics by design' has emerged in parallel. In a similar fashion, it requires the introduction of an ethical analyses and safeguards from the start of a OSINT project. In this way, data protection concerns are extended with ethical ones.

b) Necessity and proportionality requirements

To ensure the respect of autonomy and human dignity, the principles of necessity and proportionality are of great relevance. Especially, they must give answers regarding the time span of data collection. How far back in time personal data is collected determines whether these principles are respected. Indeed, the older the data is collected and analysed, the lesser autonomy people are given. Moreover, ethical challenges can be identified regarding the volume of data that is processed. Depending how much is collected and processed, ethical concerns could grow higher or decrease.

c) Transparency

Other ethical safeguards pertain to transparency. As much as possible OSINT must seek to be transparent with whomever is involved in the research conducted. This finds echo with the right to information in the GDPR according to which there is "no privacy without transparency." Derogations to this right are included in article 89 GDPR which allows, for example, derogations from Article 15(3) in case the data are processed for scientific purposes.

d) Accountability

For scholars "[t]o ensure accountability, decisions must be derivable from, and explained by, the decision-making algorithms used."[38] Therefore, accountability is closely linked to transparency. However, since machines are assumed to be incapable of moral reasoning, "accountability must remain on the humans – those who designed or programmed the machine, or those who customised and deployed it, or those who use it." Predictive big data analytics should also not be used in a way that leads to predictions which replace in turn human expression. They should keep the human being at the centre at all times.

e) Acknowledging biases

In order to avoid the reproduction of stereotypes, the designed tools and agents dealing with personal data should develop a methodology that avoids making hasty conclusions when data is analysed. Stereotypes, whether they are on national, ethnical, gender, political or any other relevant ground must be considered; machines as well as humans should pay great attention to, first, identify potential stereotypes they may be dealing with, and secondly, to avoid reproducing them. This issue is

[37] Art 25 GDPR.

[38] Virginia Dignum, Louise Dennis, Marlies van Steenbergen, Christina Baroglio, Tristan de Wildt, Matthijs Smakman, Raja Chatila, Maurizio Caon, Juan Pavón, Matteo Baldoni, Roberto Micalizio, Malte S. Kließ, Leon van der Toree, Gonzalo Génova, Serena Villata, Galit Haim, Stefano Tedeschi, Maite Lopez-Sanchez, Marija Slavkovik, 'Ethics by Design: Necessity or Curse?' (2018) AIES 18 - Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society, 60.

linked to the problem of unfair inequalities between people and the discrimination resulting thereof.

6. Conclusions

As it was seen above, there are both legal and ethical concerns with which the users of OSINT need to comply. The fact that the data used for OSINT are in the open space does not change their qualification as personal data and the application of the legal rules. Furthermore, the use of these data might interfere with the private sphere of the individuals and thus the right to privacy of individuals needs to be safeguarded. As this paper argued, for the proper protection of the fundamental rights of the individuals one cannot limit himself to compliance with the legal aspects of the tool used and activity performed. Even the most perfect implementation of laws (that by nature are imperfect) would leave gaps that need to be filled, and ethics can be used for filling these gaps. Ethics go further than the legal rules in identifying potential concerns for the proper and effective protection of the rights of the individuals. Therefore, ethical concerns, even if not yet reflected in legal choices, need to be addressed at the upfront and a course of action linked with the type of ethical concerns identified needs to be designed.

In OSINT ethical concerns are linked especially to the dignity and autonomy of the individuals, to discrimination and prejudices as well as to chilling effects in the society. Addressing these concerns from the start of a OSINT project helps to safeguard the fundamental rights of the individuals in the presence of legal lacunas. Since ethics do not have a binding requirement in themselves, extending already existing legal requirements would contribute towards achieving the goal. In this way, ethics help to close the gaps between the standards set by the laws and the proper protection of the fundamental rights of the individuals. They contribute towards mitigating any disconnections between the laws and the technology.

Old Products, New Risks: The Findings of the New Technologies Formation and Automated Driving

Dr Nynke E Vellinga[1]

1. Introduction

Back in November 2019, the New Technologies Formation of the Expert Group on Liability and New Technologies published its report 'Liability for Artificial Intelligence and Other Emerging Digital Technologies'. This Expert Group was set up by the European Commission in 2018.[2] The New Technologies Formation of this Expert Group was asked to 'assess whether and to what extent existing liability schemes are adapted to the emerging market realities following the development of the new technologies such as Artifical Intelligence, advanced robotics, the IoT and cybersecurity issues. (…) In case the existing overall liability regime is deemed not to be adequate, the New Technologies Formation (the Formation) shall provide recommendations on how it should be designed.'[3] The report of the Formation contains a description of the liability for emerging digital technologies under existing laws in Europe, as well as the Formation's perspectives on liability for these technologies. These perspectives have resulted in the Formation's 34 key findings.[4]

As it goes beyond the scope of this article to discuss all findings in-depth, only those findings that are of particular relevance in the context of automated driving will be discussed (product liability, insurance, cybersecurity). Automated driving is one of the technologies the Formation lists as an emerging technology. With numerous sensors, camera's and great computational power, future vehicles can take over the entire driving task from the human driver. At the moment, automated vehicles are being tested on public roads across the globe. The aim of this technology is to reduce road fatalities significantly by placing the human driver out of the loop. After all,

[1]Postdoctoral Researcher, Department of Transboundary Legal Studies, Faculty of Law, University of Groningen, The Netherlands.

[2] https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592.

[3] Call for Applications for the Selection of Members of the Expert Group on Liability and New Technologies, http://ec.europa.eu/transparency/regexpert/index.cfm?do=news.open_doc&id=12065, 4. IoT stands for Internet of Things.

[4] European Commission Expert Group on Liability and New Technologies - New Technologies Formation, 'Liability for Artificial Intelligence and other emerging digital technologies' (21 November 2019), https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608 (hereinafter: NTF (2019)) 5-9.

human error contributes to over 90% of all road accidents.[5] The development of automated, or self-driving, vehicles is seen as disruptive, as it has the potential to revolutionise mobility. This new technology does not only have a great impact on mobility, it also challenges current legal frameworks. The New Technologies Formation acknowledges this.[6] Several of their key findings will therefore be discussed against the backdrop of the development and future deployment of automated vehicles, seeking an answer to the question: *What are the consequences of the Formation's recommendations in the context of automated driving and how can possible lacunas be addressed*?

In doing so, the emphasis will be on the liability of the producer of an automated vehicle for accidents caused by that vehicle. The EU product liability framework dates back to 1984, when the Product Liability Directive was introduced.[7] As a result, it is uncertain how this Directive deals with the risks and challenges posed by currently emerging technologies like automated vehicles. This is addressed by the New Technologies Formation in its report and will be discussed in this contribution. In doing so, relevant legal literature is outlined. Any issues arising from the report will be identified and solutions will be proposed.

2. Liability of the Producer

The New Technologies Formation comes to several conclusions regarding the liability of the producer of an emerging technologies product. The strict liability as laid down in the Product Liability Directive will also be of value in times when emerging technologies are in use: 'Fault liability (whether or not fault is presumed), as well as strict liability for risks and for defective products, should continue to coexist (…)'.[8] The Formation continues: 'Where more than one person is liable for the same damage, liability to the victim is usually solidary (joint). Redress claims between tortfeasors should only be for identified shares (several), unless some of them form a commercial and/ or technological unit (…), in which case the members of this unit should be jointly and severally liable for their cumulative share also to the tortfeasor seeking redress.'[9] Moreover, the Formation stresses that liability should rest with the party that was in control: 'Strict liability should lie with the person who is in control of the risk connected with the operation of emerging digital technologies and who benefits from their operation (..).'[10] In addition to the general findings of the New Technologies Formation, the Formation has also done a number of findings that see specifically to the Product Liability Directive. These findings are of great relevance to the field of automated driving as liability for road accidents is expected to shift from the driver to

[5] Santokh Singh, 'Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey' (National Highway Traffic Safety Administration February 2015) <https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812115>.

[6] NTF (2019) 16-17. See also European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, 19 February 2020, (COM(2020) 65) and Report from the Commission to the European Parliament, the Council and The European Economic and Social Committee, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics (COM/2020/64 final).

[7] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.

[8] NTF (2019) 6, finding 6.

[9] NTF (2019) 8, finding 31.

[10] NTF (2019) 6, finding 10.

the producer of the vehicle (or it's software) as vehicles become ever more connected. This contribution will therefor focus on the Formation's findings relating to product liability. One of these findings is finding 13, which relates to an ongoing discussion: can software qualify as a product within the meaning of art. 2 of the Product Liability Directive?[11]

Software

Article 2 of the Product Liability Directive defines product as 'all movables, with the exception of primary agricultural products and game, even though incorporated into another movable or into an immovable. (…) 'Product' includes electricity.' Before discussing the finding of the New Technologies Formation, it is important to first explore the ongoing discussion in legal literature on the status of software.[12] Roughly four different views can be distilled from literature.

- Software is a product[13]
- Software is not a product as it is not tangible[14]
- Software is only a product when it is stored on a tangible medium (e.g. USB-stick)[15]
- The combination of software and a tangible carrier is a product.[16]

Wagner supports the view that software is a product within the meaning of the Product Liability Directive. He points out that this functional way of applying art. 2 Product Liability Directive would only exclude real estate and services from being qualified as a product within the meaning of the Directive.[17] De Bruyne and Tanghe are also in favour of this view, as they see the inclusion of electricity as a product in art. 2 of the Directive as an indication that the Directive is aimed at a wider material scope than tangible products.[18] As Egger et al. rightly point out 'It is possible to interpret the existing legal framework in a way that allows adequate solutions for questions relating to smart products.'[19] Strikingly, in the Estonian Law of Obligations

[11] See for instance M. Lehmann, Produkt- und Produzentenhaftung für Software, Neue Juristische Wochenschrift 1992, 1721.

[12] This is also acknowledged inTatjana Evas, European Parliamentary Research Service: Civil liability regime for artificial intelligence (European added value assessment) (September 2020) 8, 37.

[13] See for instance Geraint Howells, Christian Twigg-Flesner, Chris Willett, Product Liability and Digital Products, in: Tatiana-Eleni Synodinou, Philippe Jougleux, Christiana Markou, Thalia Prastitou EU Internet Law. Regulation and Enforcement, 2017.

[14] Daily Wuyts, 'The product liability directive : more than two decades of defective products in Europe' (2014) 5(1) Journal of European Tort Law 1-34, 6; Eric Tjong Tjin Tai, 'Liability for (Semi)Autonomous Systems: Robots and Algorithms' in Vanessa Mak, Eric Tjong Tjin Tai, Anna Berlee (eds), *Research Handbook on Data Science and Law* (Edward Elgar 2018) 55-82.

[15] Martin Ebers, 'Autonomes Fahren: Produkt- und Produzenthaftung' in Bernd H Oppermann, Jutta Stender-Vorwachs (eds), *Autonomes Fahren. Rechtsfolgen, Rechtsprobleme, technische Grundlagen* (CH Beck 2017) 110.

[16] Gerhard Wagner, 'Produkthaftung für autonome Systeme' (2017) 217(6) Archiv für die civilistische Praxis 707, 717; Gerhard Wagner, 'Robot Liability' (19 June 2018) https://ssrn.com/abstract=3198764; MüKoBGB/Wagner, 7. Aufl. 2017, ProdHaftG § 2 Rn. 17-20; L Dommering-van Rongen, Produktenaansprakelijkheid. Een nieuwe Europese privaatrechtelijke regeling vergeleken met de produktenaansprakelijkheid in de Verenigde Staten (Dissertation, University of Utrecht 1991) 94-95.

[17] Gerhard Wagner, 'Robot Liability' (19 June 2018) <https://ssrn.com/abstract=3198764> accessed 1 May 2021. See also MüKoBGB/Wagner, 7. Aufl. 2017, ProdHaftG § 2 Rn. 17-20; Gerhard Wagner, 'Produkthaftung für autonome Systeme' (2017) 217(6) Archiv für die civilistische Praxis 707-765

[18] Jan De Bruyne, Jochen Tanghe, 'Liability for Damage Caused by Autonomous Vehicles: A Belgian Perspective' (2017) 8(3) Journal of European Tort Law 324.

[19] Egger et al, Challenges of a Digital Single Market from an Austrian perspective – towards Smart Regulations, ALJ 2019, 37–53 (http://alj.uni-graz.at/index.php/alj/article/view/132) 48.

it is explicitly stated that 'electricity and computer software are also deemed to be movables.'[20]

The New Technology Formation takes a clear stand in finding 13: 'Strict liability of the producer should play a key role in indemnifying damage caused by defective products and their components, irrespective of whether they take a tangible or a digital form.'[21] The Formation points out that, nowadays, digital content is fulfilling functions that tangible items fulfilled back when the Directive was drafted.[22] Thus, in line with the authors mentioned above and the Estonian legislator, the Formation finds that software should qualify as a product within the meaning of the Product Liability Directive. Consequently, if it is up to the Formation, an update to the software of an automated vehicle will be considered a product within the meaning of the Product Liability Directive. If the software has a bug, causing an accident, the injured person could claim damages from the software producer.

Defect

Concerning the question of whether a product is defective within the meaning of the Product Liability Directive, the New Technologies Formation raises the question whether unpredictable deviations in the AI's decision-making path constitute a defect.[23] The Formation continues: 'Even if they constitute a defect, the state-of-the-art defence may apply.'[24]This seems to be internally contradictory as a successful invocation of the state-of-the-art defence means that a product is *not* defective. As Taschner writes '"State-of-the-art" centers on the problem of whether a product which was manufactured according to technical standards prevailing at the time of its production is non-defective, even if it has caused damage.'[25] It is, however, very well possible that the New Technologies Formation meant the development risk defence, as the development risk defence can lead to a producer not being liable for a defective product.

Defences: art. 7 (b) Product Liability Directive

Two of the six defences at the producer's disposal are discussed be the New Technologies Formation. These concern the defences of art. 7 (b) on defects that have arisen after the product was put into circulation, and the development risk defence of art. 7 (e) of the Product Liability Directive.[26] Both defences are coming under pressure due to the development of new, digital, technologies as the producer can exercise influence on his product long after it has been put into circulation and as the risks of new technologies can be substantial but unforeseeable.

Concerning the defence of art. 7 (b) of the Product Liability Directive, the New Technologies Formation states in finding 14 : 'The producer should be strictly liable

---

[20] Section 1063 subsection 1 of the Estonian Law of Obligations Act (via www.riigiteataja.ee/en/eli/507022018004/consolide).
[21] NTF (2019) 42.
[22] NTF (2019) 43. See also finding 3[b] on functional equivalence (NTF (2019) 34-35).
[23] NTF (2019) 28.
[24] NTF (2019) 28.
[25] Hans Clausdius Taschner, Harmonization of Products Liability Law in the European Community, (1999) 34 Tex. Int'l L.J. 21, 31.
[26] More extensively: NE Vellinga, Legal Aspects of Automated Driving, (dissertation; Groningen 2020) Chapter 5.

for defects in emerging digital technologies even if said defects appear after the product was put into circulation, as long as the producer was still in control of updates to, or upgrades on, the technology.(…)'[27] The Formation does not provide reasons for this statement, but does make a valid point that should be explored further.

This point can be best illustrated by an example in which, contrary to finding 13 of the Formation, software is *not*[28] regarded as a product within the meaning of the Product Liability Directive: a car manufacturer sells one of his vehicle models with the option to buy a software-update to enable all autonomous functions of the car.[29] This software-update is still under development, but those who purchased this option will receive the update as soon as it is made available. Say two years after the purchase of the vehicle, the software-update becomes available and is installed on those vehicles. However, it turns out that there is a problem with the update, causing the vehicles to misinterpret a specific speed limit sign. This causes the vehicle to accelerate, leading to dangerous situations. If, due to this update, the vehicle causes damage, the injured party will probably want to claim damages from the producer of the software update (in this case the car manufacturer). In case software is not, contrary to the opinion of the New Technologies Formation, a product within the meaning of the Product Liability Directive, one would have to argue that the entire vehicle was defective. The car manufacturer can, however, invoke the defence of art. 7 (b) of the Directive: 'The producer shall not be liable as a result of this Directive if he proves: (…) (b) that, having regard to the circumstances, it is probable that the defect which caused the damage did not exist at the time when the product was put into circulation by him or that this defect came into being afterwards; (…).' This way, the car manufacturer avoids liability as the defect, the software-update, was only installed two years after the vehicle was put into circulation. A producer might even want to anticipate on this defence by always making complex software updates available some time after a vehicle has been put into circulation. This, however, would compromise the consumer protection pursued with the Product Liability Directive. It seems that the New Technologies Formation has wanted to avoid this situation with finding 14.

The New Technologies Formation argues that the moment the product is put into circulation should not set a strict limit to the liability of the producer if this producer, or a third party acting on behalf of the producer, is still in charge of providing digital services or updates to the product (finding 14), as is the case in the example.[30] The Formation gives two options as to when the moment the product was brought onto the market should not limit the producer's liability:

'The producer should (…) remain liable where the defect has its origin (i) in a defective digital component or digital ancillary part or in other digital content or services provided for the product with the producer's assent after the product has been put into circulation; or (ii) in the absence of an update of digital content, or of the provision of a digital service which would have been required to maintain the expected level of safety within the time period for which the producer is obliged to provide such updates.'[31]

---

[27] NTF (2019) 42.
[28] This starting point seems to also have been the starting point of the Formation: see NTF (2019) 43.
[29] See for example: www.tesla.com/de_de/models/design#autopilot.
[30] NTF (2019) 42, 28.
[31] NTF (2019) 43.

Going back to the example, the producer provided the software update well after the vehicle was put into circulation. This would fall within the option (i) mentioned by the New Technology Formation. Therefore, the producer of the vehicle should remain liable for the damage caused by the defect originating in the update. Thereby, the liability remains with the party that can exercise essential control over the product: the producer.[32] The producer from the example would no longer be able to avoid liability for the damage caused by the software update (if the update does not qualify as a product within the meaning of the Product Liability Directive) by simply issuing the update after the vehicle was put into circulation.

In point (ii), the New Technologies Formation speaks of '(…) an update of digital content, or of the provision of a digital service which would have been required to maintain the expected level of safety within the time period for which the producer is obliged to provide such updates.'[33] This ties in well with two quite recent EU Directive, namely Directive (EU) 2019/770[34] and Directive (EU) 2019/771.[35] The latter, Directive (EU) 2019/771, concerns certain aspects of the sale of goods. It contains a duty for the seller of a product to not only supply the updates it has agreed to by contract, but also to supply updates for the period of time 'that the consumer may reasonably expect given the type and purpose of the goods and the digital elements, and taking into account the circumstances and nature of the contract, (…)' (art. 7 sub 3 (b) Directive (EU) 2019/771). Directive (EU) 2019/770 contains a similar provision for the supply of digital content and digital services (see art. 8 Directive (EU) 2019/770). Together with these Directives, the by the New Technologies Formation proposed interpretation of the defence of art. 7 (b) Product Liability Directive contributes further to the protection of the consumer in these digital times. The Formation adds: 'The proposed features of a producer's strict liability are very much in the same vein and follow very much the same logic, though on different grounds.'[36]

Defences: art. 7 (e) Product Liability Directive

In addition to the defence of art. 7 (b) of the Product Liability Directive, the New Technologies Formation also goes into the development risk defence of art. 7 (e) Product Liability Directive. As the Formation recognises, this defence may gain in importance due to the development of emerging technologies.[37] According to this article, 'The producer shall not be liable as a result of this Directive if he proves: (…) (e) that the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered; (…).'

Member States have been given the opportunity to derogate from the development risk defence (art. 15 sub 1 (b) Product Liability Directive). Five Member States have made use of this option, some only with regard to a specific category of

[32] See also NTF (2019) 28.
[33] NTF (2019) 43.
[34] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.
[35] Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC. See also NTF (2019) 43.
[36] NTF (2019) 43.
[37] NTF (2019) 29.

products.[38] Luxembourg and Finland are the only Member States in which the development risk defence cannot be invoked in the context of liability of the producer for damage caused by an automated vehicle.[39] The New Technologies Formation would like to see this approach applied by all Member States when it comes to emerging digital technologies, as the Formation argues that a development risk defence should not apply.[40]

The Formation points out that emerging technologies are characterised by limited predictably, which will be intensified by machine learning.[41] Here, one could think of the self-learning capacities of automated vehicles: in some instances, the producer will equip the automated vehicle with self-learning capabilities, which means that the vehicle will learn from traffic situations every day of its lifetime. With this comes the risk that the vehicle learn something 'wrong'. For instance, it could start identifying all cats as dogs. Now, this might not have significant consequences, other 'learning errors' might well have detrimental effects. If, in such cases, the producer of the automated vehicle was allowed to invoke the development risk defence, the injured party would bare the risk of a design choice made by the producer. This is not a fair distribution of risks. Therefore, the New Technologies Formation states that 'In view of the need to share benefits and risks efficiently and fairly, the development risk defence, which allows the producer to avoid liability for unforeseeable defects, should not be available in cases where it was predictable that unforeseen developments might occur.'[42]

The final part of this sentence gives rise to some questions. First, is a development that is unforeseen predictable? Or in other words: do predictable and unforeseen contradict one another? And if not, when is it actually *predictable* that *unforeseable* developments *might* occur? Does this mean that even the slightest chance that an unforeseen development, like the 'learning error', might occur makes it impossible for the producer to invoke the development risk defence? Consequently, the development risk defence could only be invoked if it was *un*predictable that unforeseeable developments might occur. Although these questions are mainly semantic matters, they are important to be clarified so that the scope of the development risk defence becomes clear. In addition, to what technologies this limitation of the application of the development risk defence stretches is not elaborated upon by the New Technologies Formation. This leaves the question open of whether the limitation in application of art. 7(e) of the Product Lability Directive should also be applied to matters of product liability for damage caused by more traditional products, such as medication. Further clarification on this matter is desirable. That being said, a more limited scope of application of the development risk defence would provide a good measure against the unfair distribution of risks, such as in the example given above.

[38] See in more detail: Cees van Dam, European Tort Law (2nd edn, Oxford University Press, 2013) 436.
[39] Esther FD Engelhard, Roeland de Bruin, 'Legal analysis of the EU common approach on the liability rules and insurance related to connected and autonomous vehicles' in Tatjana Evas EU Common Approach on the liability rules and insurance related to Connected and Autonomous Vehicles (2017) (European Union 2017) 61; Cees van Dam, European Tort Law (2nd edn, Oxford University Press, 2013) 436.
[40] NTF (2019) 42.
[41] NTF (2019) 43.
[42] NTF (2019) 43.

3. Insurance

In line with matters of liability, the New Technologies Formation also pays attention to insurance. In finding 33, the Formation states that 'The more frequent or severe potential harm resulting from emerging digital technology, and the less likely the operator is able to indemnify victims individually, the more suitable mandatory liability insurance for such risks may be.'[43] A mandatory liability insurance does not, as the Formation points out, replace 'clear and fair liability rules.'[44] The Formation argues that to ensure the best possible level of safety of emerging digital technologies, it is important that a duty of care should be affected by insurance as little as possible.[45] A mandatory insurance, however, does have its benefits. The Formation states that a mandatory liability insurance would protect future injured parties against the risk of insolvency of the liable party and would ensure the internalisation of the costs of the activities pursued by the liable party.[46] The Formation points out that, because of the lack of experience with emerging technologies, it might proof impossible to find insurance to cover for these unknown risks.[47] As this could hinder the introduction of new technologies,[48] the Formation proposes to cap the liability for certain risks at a pre-determined amount.[49]

In the automotive field, a mandatory liability insurance is already in place. The EU Motor Insurance Directive requires all Member States to 'take all appropriate measures to ensure that civil liability in respect of the use of vehicles normally based in its territory is covered by insurance.'[50] An automated vehicle can be qualified as 'vehicle' within the meaning of the Directive.[51] Thus, an automated vehicle falls within the scope of the Motor Insurance Directive. An insurance for an automated vehicle is therefore compulsory.

In its report, the New Technologies Formation refers to first-party insurance.[52] The *Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility* shares this view as the Expert Group has stated that the creation of new insurance systems might be necessary to prevent undesirable outcomes.[53] A first-

[43] NTF (2019) 61.
[44] NTF (2019) 30. See also European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) recommendations 57-59. See more extensively on mandatory insurance for smart robots: Aysegul Bugra, Room for Compulsory Product Liability Insurance in the European Union for Smart Robots? Reflections on the Compelling Challenges, in: Pierpaolo Marano and Kyriaki Noussia, InsurTech: A Legal and Regulatory View (Springer 2020).
[45] NTF (2019) 30.
[46] NTF (2019) 61.
[47] NTF (2019) 61.
[48] Maurice HM Schellekens, Self-driving cars and the chilling effect of liability (2015) 31(4) Computer Law & security Review 506.
[49] New Technologies Formation (2019) 61. See for an example on a cap on liability: Convention on Limitation of Liability for Maritime Claims, London, 19 November 1976.
[50] Art. 3 Motor Insurance Directive.
[51] Art. 1 Motor Insurance Directive.
[52] NTF (2019) 30.
[53] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659). Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility. 2020. Publication Office of the European Union: Luxembourg 62.

party insurance is not unfamiliar to the automotive field: a form of first-party insurance is in place in, for instance, Sweden.[54]

4. Compensation Funds

In addition to compulsory insurance, the New Technologies Formation signals that compensation funds should be considered.[55] The Formation advises 'that in the areas where compulsory liability insurance is introduced, a compensation fund is also in place to redress damage caused by an unidentified or uninsured technology.'[56] Here, the New Technologies Formation seems to contradict itself. At the one hand, the Formation says these technologies should be insured (compulsory liability insurance), on the other hand the Formation refers to these technologies 'as unidentified or uninsured'. A technology cannot both be insured by compulsory liability insurance as well as be uninsured. And how can one take out insurance for something that is unidentified? It is more likely that the Formation means an unidentified or uninsured *tortfeasor*. This would be in line with the example, mentioned by the Formation, of the Motor Insurance Directive.

The Formation rightly mentions art. 10 of the Motor Insurance Directive as a model of a compensation fund. This article reads:

'1. Each Member State shall set up or authorise a body with the task of providing compensation, at least up to the limits of the insurance obligation for damage to property or personal injuries caused by an unidentified vehicle or a vehicle for which the insurance obligation provided for in Article 3 has not been satisfied (…).'

In addition, the New Technologies Formation argues that a no-fault compensation scheme could be advisable if the identity of the tortfeasor, for instance a hacker, cannot be determined. This compensation scheme could be 'equivalent to that applicable to victims of violent crimes, if and to the extent that a cybercrime constitutes an offence equivalent to the latter.'[57]

This shows that the New Technologies Formation is aware that with the emergence of new digital technologies cybersecurity risks, that may have detrimental effects if exploited, are on the rise.[58] Cybersecurity risks in the automotive sector have already been brought into focus by two ethical hackers who were able to wirelessly, via the vehicle's entertainment system, hack into a vehicle.[59] This not only gave the hackers control over the entertainment system, but also over essential functions of the vehicle (brake, steering, etc.). As vehicles become more connected, this enables automated driving but it also increases the risks of hacking. At the 2020 Automated

[54] Sandra Friberg and Bill W Dufwa, 'The development of traffic liability in Sweden' in Wolfgang Ernst (ed), *The development of traffic liability* (Volume 5, Cambridge University Press, 2010); Palmerini E and others, 'Regulating Emerging Robotic Technologies in Europe: Robotics facing Law and Ethics: Guidelines on Regulating Robotics' (Robolaw 2014) 64-65. See also Jonas Bjelfvenstam, Vägen till självkörande fordon – introduktion (SOU 2018:16), Elanders Sverige AB (Stockholm 2018) 592-594, 596-599. See on the interaction of liability, insurance and social security in Scandinavia: Koziol, Ausgleich von Personenschäden. Rechtsvergleichende Anregungen für das Zusammenspiel von Schadenersatz- und Versicherungsrecht, ALJ 2/2015, 186–195 (http://alj.uni-graz.at/index.php/alj/article/view/48), under III.

[55] NTF (2019) 62. See also European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) recommendations 58, 59.

[56] NTF (2019) 62.

[57] NTF (2019) 62-63.

[58] See below for more on the meaning of çybersecurity'.

[59] Andy Greenberg, Hackers Remotely Kill a Jeep on the Highway—With Me in It, Wired, 21 July 2015.

Vehicles Symposium, a scenario was investigated in which an entire fleet of automated trucks was hacked by a nation state actor.[60] If this were to happen in real life, the consequences could be very grave. The hacked fleet could be used to block important roads, to deprive a city of supplies by sending the goods elsewhere, or the hacked fleet could be used by terrorists as a weapon.

This raises the question of whether it can be expected that these risks are born by just one commercial party: the producer of the vehicle's in the fleet, the fleet operator or the insurance company. The liable party or parties might not be financially able to pay damages. Moreover, the damages from hacking a fleet of vehicles are so high, it might be economically unfeasible to insure these risks. If that is the case, this could lead to inhabitation of the development of automated vehicles. Given the likely safety benefits of automated vehicles and the benefits this brings to the society as a whole, this would be undesirable.

Take for instance an automated truck that carries chemicals. As discussed, automated vehicles such a this truck, are expected to bring considerable safety benefits. However, if such a truck were to be hacked, this can have detrimental consequences for the environment (through pollution of soil and water), as well as detrimental consequences for road safety (the truck could drive into a traffic jam, leading to mass casualties). The liable party or parties will then face high claims for damages which they might not be financially able to pay. It is therefore advisable to consider a compensation fund, contributed to by all the relevant parties in the automated vehicle industry that benefit from the use of automated vehicles (such as producers and fleet operators), out of which the parties injured from an extensive hack of automated vehicles can be compensated.

This compensation fund differs from the fund proposed by the New Technologies Formation. The fund proposed here is not used for compensation of damaged in case the tortfeasor has not taken out insurance or is not identifiable. It is aimed at making a substantial risk – the risk of cybersecurity breaches – of a development that serves the society as a whole more manageable by spreading that risk out over all parties that benefit from the development at hand. Through this fund, the risk and the costs of damages if the risk materializes becomes more manageable for the parties involved.

A good example of such a compensation fund is The International Oil Pollution Compensation Funds (IOPC Funds). The IOPC Funds are a response to, among others, the disaster with the Torrey Canyon back in 1967.[61] Torrey Canyon, an oil tanker, ran aground between the Scilly Isles and Land's End in Cornwall, UK, leading to the spillage of over 100,000 tonnes of crude oil.[62] The oil reached the coasts of Cornwall, Guernsey, and stretched out to Brittany in France, where it caused enormous

[60] Automated Vehicles Symposium, (online) July 27-30 2020: https://automatedvehiclessymposium.org/home, sessions: Mock Trial: AV Cyberattack: Who Pays for the Damages? Mock Trial: AV Cyberattack: Who Pays for the Damages? Part Two, organisers Karlyn Stanley, Ellen Partridge, Don Slavik et al.29 July 2020, https://s36.a2zinc.net/clients/auvsi/avs2020/Public/SessionDetails.aspx?FromPage=Sessions.aspx&SessionID=3630&SessionDateID=59 and https://s36.a2zinc.net/clients/auvsi/avs2020/Public/SessionDetails.aspx?FromPage=Sessions.aspx&SessionID=3632&SessionDateID=59.

[61] https://iopcfunds.org/about-us/.

[62] Adam Vaughan, Torrey Canyon disaster – the UK's worst-ever oil spill 50 years on, The Guardian 18 March 2017.

damage.[63] In response to this oil spill and the lack of an international agreement on liability and compensation for oil spills, a regime for the compensation of oil pollution victims was created.[64] This regime has further developed over time leading to the establishment of The International Fund for Compensation for Oil Pollution in 1971. Nowadays, this fund is governed by the International Convention on the Establishment of an International Fund for Compensation for Oil Pollution Damage of 1992 (1992 Fund Convention) and the 2003 Supplementary Fund Protocol.[65] The fund has to provide, briefly stated, 'compensation to any person suffering pollution damage if such person has been unable to obtain full and adequate compensation for the damage under the terms of the 1992 Liability Convention' (art. 4 1992 Fund Convention). This 1992 Liability Convention lays down uniform international rules and procedures for the determining of liability and compensation in cases of oil pollution.[66] Entities that receive more than a certain amount of oil via sea transport need to contribute annually to the IPOC Funds.[67] This way, the costs of the risks involved in the sea transport of oil are being placed with the parties that profit from this transport. This model could be used for a compensation fund for damage caused by the (large-scale) exploitation of cybersecurity vulnerabilities, such as the hack of a fleet of automated vehicles described above.

5. Cybersecurity in the Automotive Field

The emergence of cybersecurity vulnerabilities not only gives rise to the need to explore a compensation fund as described above, but also gives rise to questions on how the Product Liability Directive can deal with the exploitation of cybersecurity vulnerabilities. Cybersecurity issues could concern, for instance, the hack of the entertainment system of the vehicle to gain digital access to the controls of the vehicle, or a so-called zero day attack. A zero day attack refers to the situation where a vulnerability is exploited before the vulnerability has been fixed.[68] Cybersecurity seems to be a topic for the New Technologies Formation's colleagues of the Product Liability Formation[69] as the New Technologies Formation mentions cybersecurity just a small number of times in its report. The Formation does not explore the challenges posed to the Directive specifically by cybersecurity problems in-depth, nor does the Formation provide a definition of 'cybersecurity'.

In the automotive field, the UNECE World Forum for Harmonization of Vehicle Regulations (WP.29) has provided the following definition for cybersecurity: '"Cyber security" means the condition in which road vehicles and their functions are protected from cyber threats to electrical or electronic components.'[70] This differs from the

[63] Bethan Bell & Mario Cacciottolo, Torrey Canyon oil spill: The day the sea turned black, BBC News 17 March 2017, Adam Vaughan, Torrey Canyon disaster – the UK's worst-ever oil spill 50 years on, The Guardian 18 March 2017.
[64] See https://iopcfunds.org/about-us/.
[65] https://iopcfunds.org/about-us/, art. 2 1992 Fund Convention.
[66] Preamble International Convention on Civil Liability for Oil Pollution Damage, 1992.
[67] Art. 10 1992 Fund Convention.
[68] https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html.
[69] http://ec.europa.eu/transparency/regexpert/index.cfm?do=news.open_doc&id=12065.
[70] ECE/TRANS/WP.29/2020/79, art. 2.2. This document including amendments ECE/TRANS/WP.29/2020/97 and ECE/TRANS/WP.29/2020/94 will become UN regulation 155 (see ECE/TRANS/WP.29/1153).

definition given in the so-called EU Cybersecurity Act: ''cybersecurity' means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats (…).'[71] So, UNECE WP. 29 sees cybersecurity as a sort of state in which a vehicle is 'cyber secure', whereas the definition given by the EU Cybersecurity Act is the opposite as cybersecurity is regarded as being the activities that should lead to a 'cyber secure' (e.g.) vehicle. A search through the Oxford English Dictionary provides for the following definitions for cybersecurity and security:

Cybersecurity: 'security relating to computer systems or the internet, esp. that intended to protect against viruses or fraud.'[72]

Security: 'I. The state or condition of being or feeling secure. (…) 2. Freedom from danger or threat. a. The state or condition of being protected from or not exposed to danger; safety.'[73]

The UNECE WP.29 definition of cybersecurity is the most in line with the definitions from the Oxford English Dictionary. Therefore, this definition will be adhered to in this article. 'Cybersecurity threat' and 'cybersecurity vulnerability' will indicate the situation where the condition of cybersecurity is under pressure due to either external factors (a hacker) or internal factors (a gap in the system that should guarantee the vehicle's cybersecurity).

In addition to the question of how cybersecurity can be defined, two other questions will be identified here. First, a question regarding whether a product is defective within the meaning of the Product Liability Directive. A product, such as an automated vehicle, is defective within the meaning of the Directive if it does 'not provide the safety which a person is entitled to expect' (art. 6 Product Liability Directive). Is this the case when the automated vehicle ignores a traffic light, or when the automated vehicle ignores a traffic light due to a zero day attack? Can a consumer expect that the automated vehicle is so secure that a zero day attack will not take place? Or can a consumer expect that the automated vehicle is equipped with a failsafe[74] so that, when a cybersecurity vulnerability is exploited, the vehicle will bring itself to a safe stop or not drive off at all?[75] In this context, importance can be attributed to the technical requirements that need to be fulfilled for EU type-approval to be granted to a vehicle type, as well as to a European cybersecurity certification scheme cf. art. 49 of the EU Cybersecurity Act.[76]

---

[71] Article 2 (1) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[72] Oxford English Dictionary via www.oed.com/view/Entry/250879?redirectedFrom=cybersecurity#eid117229282.

[73] Oxford English Dictionary via www.oed.com/view/Entry/174661?redirectedFrom=security#eid.

[74] NE Vellinga, Legal Aspects of Automated Driving, (dissertation; Groningen 2020) Chapter 4.

[75] Automated Vehicles Symposium, (online) July 27-30 2020: https://automatedvehiclessymposium.org/home, sessions: Mock Trial: AV Cyberattack: Who Pays for the Damages? Mock Trial: AV Cyberattack: Who Pays for the Damages? Part Two, organisers Karlyn Stanley, Ellen Partridge, Don Slavik et al.29 July 2020, https://s36.a2zinc.net/clients/auvsi/avs2020/Public/SessionDetails.aspx?FromPage=Sessions.aspx&SessionID=3630&SessionDateID=59 and https://s36.a2zinc.net/clients/auvsi/avs2020/Public/SessionDetails.aspx?FromPage=Sessions.aspx&SessionID=3632&SessionDateID=59.

[76] Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units

Apart from identifying the justified expectations of consumers in general, cybersecurity will also play a role within the context of the development risk defence. Here, the question rises whether a cybersecurity breach or, more specifically, a zero day attack is a defect that could not have been discovered given the state of scientific and technical knowledge at the time when the product was put into circulation (art. 7(d) Product Liability Directive). By the time the vulnerability is exploited the knowledge specifically on how to exploit this vulnerability was obviously available, but this does not necessarily mean that this knowledge was available when the product was put into circulation. The New Technologies Formation has argued that the development risk defence 'should not be available in cases where it was predictable that unforeseen developments might occur.'[77] One could argue that whenever there is a cybersecurity aspect to a product, there is always also a risk of a cybersecurity breach. In that sense, it is predictable that a cybersecurity breach, such as a zero day attack, might occur. This could then lead to the unavailability of the development risk defence to the producer. Consequently, the producer would be liable for the damage caused by the cybersecurity breach. As described above, however, this could hinder development given the magnitude of cybersecurity risks and the subsequent damage. A compensation fund as mentioned in the previous section could provide a solution for this.

6. Conclusion

In its report 'Liability for Artificial Intelligence and other emerging digital technologies', The New Technologies Formation has given an overview of the challenges emerging technologies pose for existing liability regimes. New legal solutions are explored to ensure appropriate indemnifications of parties injured by new technologies, such as automated vehicles. In general, it can be noted that the Formation seems to be of the opinion that control should lead to liability (e.g. concerning the defence of art. 7 (b) of the Product Liability Directive).This will require further discussion on, inter alia, the definition of product within the Product Liability Directive and the development risk defence. Concerning automated vehicles, questions on the role of the user of the vehicle and possible fail-safe systems are left unanswered.

The New Technologies Formation also makes only limited comments on cybersecurity issues. Cybersecurity is nevertheless important as the more products become connected, the more vulnerable they will become to cybersecurity breaches. If these risks become too great for one party to bear, a compensation fund should be considered.

All in all, the findings of the New Technologies Formation, although they do require further clarification, should lead to a balanced legal approach to emerging digital technologies.

---

intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC and Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013) (Cybersecurity Act).

[77] NTF (2019) 43.

The safety and security of children on the Internet and cyberspace and the guarantees of their protection in the digital environment

Pjereta Agalliu[1] Ph.D. - M.Sc. Tevia Agalliu M.Sc. [2]

1. Introduction

1.1 The right of children to access the Internet and cyberspace[1]

In recent decades, the developments of the internet, as well as innovations in technology, have brought about radical changes and challenges in every society around the world. Our daily lives, human rights, economies and social interactions are profoundly influenced by information and communication technologies. This shared and free cyberspace promotes social and political inclusion, breaks down barriers to communication between countries, communities and citizens, allowing the interaction and exchange of information and ideas in real time across the globe.[2] The Internet is a global system of interconnected computer networks that make the electronic exchange of data (text, music video, photos, etc.), this information can be read, viewed or downloaded by other users. So the internet practically enables communication from one computer device to another.[3]

The right of children to internet access goes hand in hand with their right to information and the right to privacy protected by the Convention on Fundamental Human Rights (ECHR) in Articles 10 and 8, respectively.[4] The main framework of human rights for children is the United Nations Convention on the Rights of the Child (UNCRC).[5] According to scholars, this convention has been visionary, authoritarian, comprehensive and influential. However, it was written in 1989,[6] when the Internet had just begun, despite the fact that the Convention has been carefully formulated to be widely implemented in time and space. However there is uncertainty about how to interpret and implement it in relation to the digital environment.[7]

According to recommendations issued by the United Nations (UN) Committee on the Rights of the Child, all children should be able to have secure access to ICT and digital media, and be empowered to participate fully, to express themselves, seek information and enjoy all rights enshrined in the UNCRC and its Optional Protocols without any discrimination.[8] (You can find this text on pg. 2-3 of the original work)

[1] External lecturer, Criminal Department, Faculty of Law, University of Tirana, Albania.
[2] Criminal Msc Student, Faculty of Law, University of Tirana, Albania.

Despite the fact that cyberspace and the Internet are a virtual space and network, the interaction and relationships that are created with and in it are similar to what we create in real life, so all the guarantees and rights are relevant to this "online" space as well.

Children's access to the Internet is a guaranteed right as for any human being, the difference is that the child as a fragile being and in a developing physical, psychological-emotional and intellectual development is provided protection in this virtual relationship. The fact that the Internet or cyberspace are technological goods, taken in terms of the change they have brought to human life, carry with them unknowns or uncertainties which can bring harm. But at no point does the safety and protection of the child in the digital environment mean the denial of his or her right of access to it.[9]

In addition to the facilities and advantages that the Internet offers, it must be said that given that there are millions of people who use the Internet, in this context the number of abusers is large.

According to a study conducted by the organization World Vision in 2014, the main risks perceived by children are those related to content, followed by those related to behavior and then those related to contacts.[10] These risks have been reconfirmed in the study 2018-2019 on "Children's experiences in using the Internet in Albania".[11] This study highlighted a high rate of uncontrolled internet use by children. In general, the children surveyed use the Internet more and have more technological online skills than their parents. This poses a barrier for parents to effectively accompany their children's online experience, not only by controlling access, but by helping children develop critical judgment about online experiences and content.[12] Based on this arises the need to engage at an institutional level to guide children correctly during their access to the Internet, first through information; secondly, through the supervision of parents, educational staff and psychologists to the most specific structures composed of cyber specialists, strengthening the rule of law by adopting legal acts and mechanisms that provide real protection and security for children as well as mechanisms for punishing cybercrime in concrete cases committed against children.

2. Some of the negative effects of the Internet on children and the preventive mechanism

The situation of the COVID-19 pandemic, which forced most companies to go into partial or total closure, introduced to the online world and technology services even the smallest age groups which may not have had intensive internet access. Children may be exposed to a greater amount of targeted internet marketing that promotes unhealthy foods, gender stereotypes or age-inappropriate information. They may also be exposed to untrue information that can add to fear and anxiety. The limited protection of children online, at the time of the pandemic came as a result of the rush to establish distance learning, without having the opportunity to bring the best possible model of online school.[13]

Cyberbullying is another form of risk and violence in the online environment, although physical bullying is mostly reported in sonnets and there is underreporting of online bullying, this is also due to the lack of clear perception by children when

addressing the question in the survey, according to the 2020 report, was reported by less than 1 in 10 children, given the high levels of face-to-face bullying.[14] It needs to be done more, working with internet service operators to monitor and regulate children's involuntary exposure to sexual content online.

Many online games offer the opportunity for children to talk to each other while playing, exposing them to various dangers. The most common dangers posed by online games are cyberbullying, theft or misuse of personal information and seduction.[15]

A handful of young children also have social media profiles, which violate the age policies of many platforms (e.g. Facebook, Instagram, Snapchat, Tumblr and Twitter all have a 13+ age policy).[16] In the United States, although the Online Child Privacy Protection Act (COPPA) was enacted to protect children under the age of thirteen, the rules do not adequately protect children from online companies that collect and share their personal information. The concrete example is related to the social network TikTok, after thousands of complaints about the collection of personal data of children under 13 years old. The FTC stated in its complaint that TikTok violated COPPA rules by failing to provide direct notification to parents, by not obtaining parental consent before collecting personal information, and by not notifying parents of children of the collection of the application and the use of their personal information. In essence, any information the company collects from a child under the age of thirteen may be a violation of COPPA rules.[17]

WhatsApp in compliance with this law has announced a change in their terms and conditions for users located in Europe. Users will now need to be 16 years old to use WhatsApp. Almost all other social media services require users to be at least 13 years old to access and use their services.[18]

2.1 Forms of prevention of harm to the child and his protection in access to the Internet

The most classic form of protection against a risk is its prevention. Self-defense begins with being informed of what is at stake for 'you', and all the tools to guide you from being harmed. In this spirit is guided the whole mechanism for building a safe environment for children online, information, counseling, guidance towards the acquisition of good habits and habits when interacting in the digital environment of the child.

It is up to parents, carers, educators, educational institutions, child rights professionals and beyond, and governments to inform and raise children's awareness of Internet safety and the potential risks to which they may be exposed while using the Internet; instructing children on how to avoid the dangers of the virtual world and how they can react when faced with them.[19]

Like forms of physical, sexual, emotional violence, a child should also be aware of forms of cyberbullying as cyberspace has now become the ground for pedophiles, cyber predators and identity thieves not to mention the abundance of inappropriate content that is freely available.

As Rathnayake, the technical adviser on child protection and participation in World Vision Lanka puts it: *"It is not about denying your child access to the internet, knowing that these dangers exist in cyberspace."It's all about empowering your child by*

learning ways to identify online violence and the right set of actions to take when dealing with violence of this nature".[20]

Most online child protection and safety guides[21] strongly support recognizing the child and informing him or her about a new parallel environment in which his or her life will take place and that the 'Internet' is inevitable. An important role in this regard is played by all the actors mentioned above, but the parents or guardians of the children play a fundamental role.

In addition to information and guidance mechanisms, there are genuine programs for the safety and protection of children on the Internet. Recently in Albania, a multi-year program entitled #*I am safe on the Internet* has been launched, to make significant progress towards preventing and protecting children from sexual exploitation and abuse on the Internet. Working closely with children, government, parents and guardians of children, civil society, child protection professionals and the private sector, where it focuses on maximizing the benefits of children online and minimizing their exposure to potential risks and injuries . This program aims to:

- Investigate cases of sexual exploitation and sexual abuse on the Internet (CSEA) and prosecution of perpetrators;
- Report child sexual abuse materials and deleting them;
- Take protective measures, mitigating the risks and preventing the exploitation and sexual abuse of the child by the children themselves, families, teachers and guardians.[22]

3. The role of the Albanian state in guaranteeing cyber security and the challenges for punishing criminal offenses in the cyber environment committed against children

3.1 Albanian State Commitment to Internet Security and Cyber Security

The safety of children in cyberspace is one of the priorities of Albania and all institutions that have it in the focus of their activity.[23]

Regarding the level of commitment to cyber security, Albania is positioned in the countries with average level, in the regional level the 36th place while in the global level the 62nd place.[24] While the United Kingdom and the United States are positioned first in fulfilling their commitment to cyber security.[25]

This assessment is based on several elements the fulfillment of which makes a state seriously engaged in the challenge of cyber security. These aspects are addressed below by providing an overview of each aspect of the Albanian state's commitment to ensuring cyber security:

Legal aspect: *Consists of legal measures, a legislative framework*. In essence, the objective is to have sufficient legislation in place to harmonize practices at the regional / international level and to simplify the international fight against cybercrime.

Albania has ratified a number of conventions on the rights of children in terms of online and offline security, which have helped the country in aligning its legislation with international standards. The Convention on the Rights of the Child[26] began its effects in the beginnings of the democratic legislature in Albania. Perhaps this Convention at that time did not refer to the explicit protection of children from the online environment, much less to find application in this context in Albanian practice

still unfamiliar with emerging technology and not at all accessible to minors for the time we are referring to.

However, this instrument has laid the foundations for the completion of this legal framework that will be enriched in the years that followed until today. Thus, in line with the legal aspect of child safety, the Third Optional Protocol on the sale of children,[27] child prostitution and child pornography has been adopted. The legal framework is complemented by the Council of Europe Convention on Cybercrime (Budapest Convention),[28] the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention).[29]

This framework of legal measures is the basis of other legal acts that have emerged as a basis and in their implementation to make the protection of children against cybercrime effective and concrete. As is clearly sanctioned in the Constitution of the Republic of Albania, ratified international acts have force in the entire territory of the Republic of Albania,[30] in this context their legal force prevails over any other legal act that contradicts them. For this reason they constitute the pillar on which the internal laws and in this case the laws and normative acts for the safety of children in the cyberspace should be harmonized.

Technical Aspect: Technology is the main frontier of protection against cyber threats. Without adequate technical capabilities to detect and respond to cyber attacks, countries remain vulnerable.[31] The National Authority for Electronic Certification and Cyber Security (AKCESK) [32] has been established in Albania. Among other things, this Authority determines the minimum technical standards for data security and information networks / computer systems of the information society, in accordance with international standards in this field, in order to create a secure electronic environment.[33]

Organizational Aspect: In addition to developments in the field of information technology and the revolution on the digitalization of public services, the legal framework for cyber security has been completed and improved. Thanks to this progress, Albania has improved in the Global Cyber Security Index compared to 2017.[34] For this reason, in February 2021, the Government of Albania has approved the new five-year National Strategy for Cyber Security (2020 - 2025), which for the first time in the history of the country includes a special chapter on child protection online, by making it a priority and proving the State's commitment to the safety of children in every environment.[35]

Capacity building: Capacity building and accreditation of cyber security professionals, professional training courses in cyber security, educational programs or academic curricula, etc., is essential for the first three legal, technical and organizational pillars. In this respect, Albania is not at the desired level, seen this even in most of the reports (which we referred to during this paper) which emphasizes the need for professional training in cyber security starting from teachers and heads of educational structures, training of police officers who can deal in practice with situations of online violence reporting or any concern arising from the digital

environment and be able to respond. Building curricula updated on time, as technology moves at a rapid pace and you need to be in coherence with it.

Collaboration: Cybercrime is a global problem and is unlimited across national borders. As such, tackling cybercrime requires a multi-stakeholder approach with input from across sectors and disciplines. National and international cooperation is assessed based on the number of partnerships, collaborative frameworks and information sharing networks.[36] Albania is part of the Global Alliance against Sexual Abuse of Children on the Internet, created on December 5, 2012. In addition, Albania is part of the Global Alliance "We Protect" to end the sexual exploitation of children online.[37] It is established even the Online Child Protection Platform, to report concrete cases and to be informed about the ways they can protect themselves while using the internet; Also, the establishment of the National Advice Line for Children ALO 116 111,[38] guarantees children an effective tool to protect themselves in the digital environment.

3.2 Cybercrime, criminal offenses committed against children, such as sexual abuse and pornography

Children should be made aware of existing legislation on online child sexual abuse in order to inform the police if they are being blackmailed. It is also important that the police are properly trained and equipped to respond to such reports of children. In the 2020 study conducted by UNICEF Albania, one in ten children (9%) reported at least one of unwanted sexual experiences listed online, where teenagersn (12% of 15-17 year olds) have been more affected than young children. Researchers have pointed out that not all of these situations can result in harm, and that children may be able to say no to these demands. However, the figures show that the exposure of Albanian children to the risk of abuse and sexual exploitation is high enough to require the child protection system to increase its willingness to respond to these risks.[39]

Children can be easily exposed to illegal materials, often without realizing that they are illegal and harmful to their age. Children often open fake accounts for the purpose of opening these sites, they are intended for adults. Unfortunately, many parents are not aware of how to deal with internet security issues and the need for information. Lack of experience and pure sincerity of children can lead them to online risks. Children may accidentally come across pornographic content intentionally or out of curiosity.[40]

The fact is that in most cases, illegal internet networks where pedophiles exchange pictures can only be accessed if you provide pornographic material yourself. So not infrequently, the consumption of pornographic material is linked to the direct abuse of a minor, criminalists say. Therefore, child protection politicians and activists call on society to be more vigilant and, in case of doubt, to inform government agencies or child support organizations.[41]

The Budapest Convention is the only international treaty that makes sexual abuse a criminal offense related to child pornography. Article 9 sanctioned criminalization and punishment for those who recruit children into prostitution and those who address them, in connection with the production of child pornography, for

the purpose of distributing it through a computer system; providing or making available child pornography through a computer system; distributing or transmitting child pornography through a computer system; procurement of child pornography through one computer system or another; Possession of child pornography through a computer system or a computer data storage device. "Pornography with children" will include pornographic material that differs from the visual part:

a) A minor, who engages in clear sexual orientations;

b) A person who appears to be a minor, engaged in clear sexual orientations;

c) Realistic images that present a minor engaged in clear sexual directions.[42]

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007) contains provisions criminalizing the use of new technologies - in particular the Internet - to harm or sexually abuse children. The Convention represents great progress towards the prevention of sexual offenses against children, the prosecution of perpetrators and the protection of their victims. Available data suggest that about one in five children in Europe are victims of some form of sexual violence.[43]

The Criminal Code of the Republic of Albania, dictated by the ratification of the aforementioned Conventions, has undergone other changes and improvements in relation to cybercrime[44], which has a full connection with the criminal offense of pornography. Article 7 of the Criminal Code is added letter (j), regarding the applicability of criminal justice for crimes in the field of information technology, with the responsibility not only of Albanian citizens, but also of foreigners outside the territory of the Republic of Albania, if this criminal offense is committed against the interests of the Albanian state or Albanian citizens. Article 117 of the Criminal Code[45] provides for the elements of the criminal offense of pornography expressly as:

1. The production, distribution, advertising, import, sale and publication of pornographic materials in environments where there are children, by any means or form, constitute criminal offenses and are punishable by imprisonment of up to two years.

2. The production, import, offering, making available, distributing, transmitting, using or possessing child pornography, as well as creating conscious access to it, by any means or form, shall be punished by imprisonment of three to ten years.

3. Recruiting, using, coercing, or persuading a child to participate in pornographic shows, or participating in pornographic shows involving children, is punishable by imprisonment of five to ten years.

Currently, there is no specific data collected and published on child abuse online. To date, there have been no discussions or agreements between relevant actors on how to assess and report on Internet risks and responses to them. Neither the police nor the prosecution is fully equipped with the necessary infrastructure to effectively investigate child abuse cases online. The cybercrime unit reports a lack of opportunities to conduct active online surveillance, undermining their ability to initiate ex officio and proactive[46] investigations. For these reasons these cases are difficult in practice to identify and investigate as much as possible.[47] Despite the fact and the lack of Albanian case law regarding this offense, it cannot be concluded that there are no cases of pornography in Albania.

State institutions do not identify the situation of pornography in Albania, but refer only to general statistics of courts, prosecutors and police offices, which in each case do not identify pornography separately, but analyze it as part of statistics on

sexual abuse. Measures should be taken to train the police in recognizing this social and legal phenomenon of pornography, as it is more difficult for them to identify those cases that exist de facto but are not reported or are not identified.[48]

Although Albanian legislation as a whole complies with all relevant international standards on child sexual abuse, it is often fragmented and lacks very important definitions regarding child sexual abuse, engagement and coercion in sexual and other improper activities.

The Center for the Rights of the Child in Albania and ECPAT Albania, in May 2019, addressed the Parliament for amendments to the Criminal Code for the protection of children and young people from violence and exploitation. In an open hearing in the Parliament, CRCA / ECPAT Albania requested improvements and additions to the Criminal Code for harassment, pedophilia, pornography or even the use of children and young people online. The Director of CRCA / ECPAT Albania, stressed that the Report "Crimes with Impunity" published in February 2019, showed once again that monstrous crimes are being committed against children and young people online and due to the lack of legal provisions in the Code Criminal these crimes are going unpunished. He referred to a concrete event in which they were notified by the State Police of a case of online bullying that had triggered suicide attempts by a minor. Social networks were bombarded with the profile of a sexual predator spreading violent sexual intercourse between an adult and a minor. They considered the proposed additions and changes very important for the protection of children while browsing the Internet, emphasizing that their non-approval means that we accept that crimes against children will continue to go unpunished and that will continue to produce victims.[49]

But even today it seems that there have not been taken concrete steps in improving the operational structures, specialization of human resources and the realization of an effective protection of children as a subject of cybercrime. On October 2021, CRCA / ECPAT in Albania reported the study "Voices of Survivors in Albania", which puts the voices of children surviving sexual exploitation online at the forefront of responding to addressing vulnerabilities in the system protection and rehabilitation of children victims of sexual violence. The study brings up all the shortcomings that the child protection system encounters. The interviewed children stated that they did not have any information, at the time of the sexual abuse, on the existence and role of child protection workers in the Municipalities where they live. Even the employees of the front line of the service show to the extent of 56% that the public awareness for the exploitation and sexual abuse of children on the Internet is very weak or does not exist at all.[50]

Albania still has a long way to go without denying the important steps it has taken so far to establish the legal basis and mechanisms for ensuring child safety on the Internet and cyberspace. It should be understood that no law or structure set up will be sufficient if we do not first become aware as a society of cybercrime in particular and the responsible interaction of all instruments and their continuous improvement to realize a protection real children on the one hand and the punishment of cybercrime on the other.

4. Conclusions and Recommendations

Given the limited statistics and case studies on children's access to the Internet, which for Albania are very few and with a time gap, it is needed that the state and non-governmental organizations engage in more statistical studies to help having a better understanding and concrete data of the problems related with the use of internet from children.

Safe and responsible use of the internet needs to be encouraged together with the knowledge of potential risks. It is needed to educate children with the online world, to empower them to recognize the dangers and to be able to avoid them.

The role of parents, educational institution, professionals in the protection of children's rights is very important in promoting and preventing the dangers of the virtual world and the damage that can be caused to children.

More work should be done to strengthen the child's trust in state protection structures, in relation to the denunciation and reporting by the child of unpleasant situations, hurtful behaviors, and display of inappropriate images, cases of sexual abuse or pornography.

For Albania, cyber security and child protection in this digital space is a new challenge. However, the legal foundations have already been laid down and serve as an important guarantor that provides an institutional protection.

Although the Albanian legislation as a whole complies with all relevant international standards on child sexual abuse, it is often fragmented and lacks very important definitions regarding child sexual abuse, their engagement and coercion in sexual activities and other inappropriate activities. In this light, it is necessary to take concrete measures to amend the Criminal Code and introduce explicit sanctions with regards to cybercrimes committed against children.

Furthermore, there is a lack of training of police officers, prosecutors and insufficient equipment with the necessary infrastructure for effective investigation of cases of child abuse on the Internet. The cybercrime unit reports a lack of opportunities to conduct active online surveillance, undermining their ability to initiate ex officio and proactive[51] investigations. In this context, the Albanian legal framework as well as the responsible law enforcement institutions still have to improve in guaranteeing security from cyber threats, sexual abuse or pornography in cyberspace for children. It is seen as an immediate need to complete the legal framework with bylaws for the functioning of structures, institutions, bodies, professionals but also the guidance of parents, where cooperation will create the steps for a risk management platform to keep children safe in internet.

Sources

1. The Constitution of the Republic of Albania
2. National Strategy 2020-2025, Official Journal Year 2021 - Number 7.
3. European Convention for the Protection of Human Rights and Fundamental Freedoms.
4. Convention on the Rights of the Child Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989 entry into force 2 September 1990.

5. The United Nations Convention on the Rights of the Child (CRC) ratified by the Assembly of the Republic of Albania with law no. 7531 dated December 11, 1991.
6. Law No. 9834, dated 22.11.2007, "*On the Accession of the Republic of Albania to the Optional Protocol to the UN Convention on the Rights of the Child, on the Sale of Children, Prostitution and Child Pornography*".
7. Council of Europe Convention on Cybercrime (Budapest Convention), Albania ratified this Convention with Law no. 8888, April 25, 2002.
8. Additional Protocol with Law no. 9262, July 29, 2004, "*On the ratification of the Additional Protocol to the Convention on Cybercrime, on the criminalization of acts of a racist and xenophobic nature committed through computer systems*".
9. Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) The Convention was ratified by Albania with Law no. 10 071, on 9 February 2009 and entered into force on 1 July 2010.
10. Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.
11. The National Authority for Electronic Certification and Cyber Security (AKCESK) is responsible for overseeing the implementation of Law No. 9880/2008 "*On Electronic Signature*".
12. Law No. 107/2015 "*On Electronic Identification and Trusted Services*" and Law no. 2/2017 "*On Cyber Security*" and bylaws issued in their implementation.
13. Law no. 8888, dated 25.4.2002 "On the Ratification of the *Convention on Cybercrime*".
14. Law no. 10023, dated 27.11.2008, on Some Additions and Amendments to Law NO. 7895, dated 27.1.1995 Amended Criminal Code.
15. European Commission 2013, Global Alliance Report on Sexual Exploitation of Children Online, December 2013.
16. M. Menkshi, Doctorate "Criminal offenses of child abuse and exploitation. Juvenile criminal justice in the perspective of international acts and the European Court of Human Rights.
17. Child safety on the Internet Guide for children "*For a safe internet navigation*", http://femijet.gov.al/al/wp-content/uploads/2016/02/Broshura-F%C3%ABmij%C3%AB-t%C3%AB-sigurt-n%C3%AB-internet.pdf.
18. Child safety on the Internet Guide for children "*For safe internet navigation*".
19.https://www.wvi.org/newsroom/sri-lanka/10-things-remember-you-let-your-child-go-online
20. Guide for Parents and Guardians on Online Child Protection 2020
21. https://cesk.gov.al/legjislacioni/2021/Prinder.pdf22.
22. Guidelines for Online Child Protection 2020.
23. https://cesk.gov.al/legjislacioni/2021/Policy%20makers-converted.pdf
24.Guideline for the online child protection industry
https://cesk.gov.al/legjislacioni/2021/Industria.pdf
25. Child Safety on the Internet A guide for children "*For a safe internet navigation*".
26.
https://www.isigurt.al/sites/default/files/Siguria%20ne%20Internet%20femijet.pdf

27. Council of Europe Strategy for the Rights of the Children's human rights (2016-2021)
28. The Difference Between Cyberspace & The Internet Uploaded on 2017-05-22 in BUSINESS-Services-IT & Telecoms, FREE TO VIEW, NEWS-News Analysis. https://www.cybersecurityintelligence.com/blog/the-difference-between-cyberspace-and-the-internet-2412.html
29. Rethinking the rights of children for the internet age, Published on 19-03-2019 at 11:32 https://www.childinthecity.org/2019/03/19/rethinking-the-rights-of-children-for-the-internet-age/?gdpr=accept
30. COVID-19 and its implications for protecting children online April 2020. https://www.unicef.org/sites/default/files/2020-04/COVID-19-and-Its-Implications-for-Protecting-Children-Online.pdf
31. One click away. Experience in internet use by children in Albania https://www.unicef.org/albania/media/2581/file/NJe_klikim_larg_2020.pdf
32. Internet safety for children FIT Save the Children, Prishtina Dcember, 2016 https://www.oecd-ilibrary.org/sites/71b7058aen/index.html?itemId=/content/component/71b7058a-en
33. Kiara Ortiz, Underage Social Media Usage and COPPA, 1 April 2019, last visited on 31.03.2020. http://www.jgspl.org/underage-social-media-usage-and-coppa/
34. Age Restrictions on Social Media Service, Posted on 25 April 2018 https://www.childnet.com/blog/age-restrictions-on-social-media-services
35. Child pornography.State and policy failure? https://www.dw.com/sq/pornografia-e-f%C3%ABmij%C3%ABve-d%C3%ABshtim-i-shtetit-dhe-i-politikave/a-53772577 11.06.2020
36. Online sex crime are finally punished by Criminal Code https://www.isigurt.al/lajme/krimet-seksuale-online-me-se-fundi-ndeshkohen-nga-kodi-penal
37. UNICEF's first-ever national assessment on tackling child abuse online, 10 September 2019.https://www.unicef.org/albania/press-releases/unicefs-first-ever-national-assessment-tackling-child-abuse-online
38. Survivors "*Voices*", a joint study by ECPAT International and CRCA / ECPAT Albania Survivors' Voices Study.

***Web sources*:**

- https://www.oecd-ilibrary.org/sites/71b7058a-en/index.html?itemId=/content/component/71b7058a-en
- https://cesk.gov.al/rreth-nesh/index.html
- https://www.britannica.com/technology/Internet
- https://www.wvi.org/newsroom/sri-lanka/10-things-remember-you-let-your-child-go-online
- http://www.jgspl.org/underage-social-media-usage-and-coppa/

- https://www.unicef.org/albania/sq/deklarata-shtypi/mbrojtja-e-f%C3%ABmij%C3%ABve-n%C3%AB-internet-nj%C3%AB-nd%C3%ABr-objektivat-kryesore-t%C3%AB-strategjis%C3%AB-s%C3%AB-re
- https://www.unicef.org/albania/viral-summit-better-internet-children-and-adolescents-albania
- https://www.unicef.org/albania/sq/deklarata-shtypi/ti-japim-fund-dhun%C3%ABs-abuzimeve-ndaj-f%C3%ABmij%C3%ABve-n%C3%AB-internet
- https://raisingchildren.net.au/teens/entertainment-technology/digital-life/social-media#about-social-media-for-children-and-teenagers-nav-title
- https://www.crca.al/sq/barnhaus-free-legal-aid-vepro-per-femijet-news-press-release-child-protection-violence-media/studimi

The rapid emergence of Digital Markets: analysis of the antitrust legal frameworks in the EU and Albania

Kejsi ZIU LLM, MSc

1. Introduction

Digitalization is a phenomenon that has and will very likely continue to change our lives, whether we act as private citizens, consumers, employers or employees, economic actors, policy makers, law enforcers, etc. It has revolutionized all sectors of the worldwide economy and has facilitated the development of new types of products or services - and as a result, of new types of businesses and markets. The rapid and widespread development of digitalization has created many new ways to conduct online trade, including in Albania. It has definitely positively impacted the lives of respectively EU and Albanian citizens, as online intermediaries and platforms in particular have become vital players in the digital transformation of acquiring services, facilitating purchase for consumers as well as increasing innovation and cross-border trading on a larger scale between the countries of the Western Balkans region - including Albania - with the EU.

In addition, digitalization has driven existing operators with a physical market presence, to largely present their business to a wider, online audience. These developments relate greatly to the emergence of a new type of economy, the so-called 'digital economy', the pace of which has proven to surpass "traditional" business models. While there is a broad consensus on the benefits of the rapid digital transformation, the issues arising may have some repercussions for society and economy not only on a national level, but also on an international one, e.g. in the European Union. Specifically, how does EU competition law account for the digitalization phenomenon? Is the law digital era - proof, or are there adjustments that need to be performed on the current regulatory and enforcement frameworks?

This submission aims to showcase some of the trends and patterns in the EU competition law in order to address constantly evolving digital reality. Another specific focus of this submission is to provide a thorough analysis on the current antitrust legal framework in Albania, and whether Law No. 9121, dated 28.7.2003 "*On the Protection of*

Competition", amended, fully regulates potential gaps arising from the emergence of digital markets in the field of free online trade. It is important to address this issue, especially given that most of the Albanian legislation currently in force has been drafted before the digitalization phenomenon started materializing as widespread in the EU and the overall WB region. Therefore, it is not inconceivable that the emergence of the digital economy and digital markets challenges the longstanding, and at times inflexible, legal regimes that are currently in place.

2. The European Competition Law Context

Digital markets have been high on the existing EU competition policy's agenda ever since large digital multinational companies such as Amazon, Facebook, Google, Apple etc., have been providing their digital infrastructure for a variety of e-commerce services or purchases for consumers. So why is the application of antitrust legislation important for the digital economy? The simplest answer would be because the digital economy is ruled by data, including personal data. While the matter of privacy protection is not necessarily in and of itself important for competition regulators, consumer data is. Data can act as a barrier to market entry, but can also be used to foreclose competitors' access to market and leveraging market power from one market to abuse such market power in another market. Indeed, aside from providing many benefits to consumers, such companies often develop a "*winner takes all*" attitude with regard to gaining market power. Such practices in the cyber environment may result in arising barriers to market entry or expansion, or potentially suppress innovation. According to the European Commission, fully reaping the benefits of the digital revolution necessitates a consistent regulatory framework.[1] This has been the drive behind turning the digital single market as a priority by the European Commission since the start of its mandate. On 6 May 2015, the Commission launched a sector inquiry into the e-commerce of consumer goods and digital content in the EU.[2]

It is challenging for regulators to generalize what constitutes a digital market and market power, due to the unique functions and business models, as well as the nature of national markets and jurisdictions of the Member States where these companies operate. The European Commission has defined an online platform as an undertaking operating in two (or multi) sided markets, which uses the Internet to enable interactions between two or more distinct but interdependent groups of users so as to generate value for at least one of the groups.[3] Platforms involve services and activities such as marketplaces, social networking, search engines, payment systems and video sharing. Digital platforms have new business models and function with algorithms, which are designed to collect

[1] See Statement by Executive Vice-President Vestager on the Commission proposal on new rules for digital platforms, 15 December 2020. Accessible at https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_20_2450

[2] The sector inquiry was launched pursuant to Article 17 of Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, OJ L 1, 4.1.2003, p. 1.

[3] See also OECD, 2019, "Abuse of Dominance in Digital Markets", (2020), p. 6, para 3. Accessible at https://www.oecd.org/daf/competition/abuse-of-dominance-in-digital-markets-2020.pdf

and process data, with decisions made based on that data.[4] Data-driven network effects are one of the features that characterize digital platforms. A network effect "refers to the effect that one user of a good or service has on the value of that product to other existing or potential users".[5]

Digital platforms have challenged the neoclassical approach to doing business, which defined the goal of a private company as maximizing profits. The new business models prioritize growth over profits in the short to medium terms, that is, the maximization of the number of users rather than profits. To put it simply, big companies in some cases can harmfully gather and use consumer data to reinforce their dominant position in the market, which can be in violation to Article 102 TFEU. Economies of scale and scope, data-driven network effects and control of data sometimes can create high barriers to entry.

Whereas the concept of digital markets may include the following characteristics:[6]

- Market size – usually the largest digital companies are the ones also conducting online trade;
- Markets are often multi-sided, i.e., they bring together different groups of consumers via a platform;
- Products often provided to consumers are at low prices, using revenue from other sides of a market, or provided alongside paid premium offerings;
- Certain effects on consumer purchases – online consumers may enjoy paid premium offering on a product when more consumers use that same product.

Many EU and third countries are also following up on the negative effects of the market power of online platforms and seeking legal ways to deal with the related challenges. EU Governments and policy makers of the European Commission are now concerned about the market power of digital platforms and the associated potential risk of abuse and spill-overs into other markets as well.[7] Such concerns have become particularly evident since 2017, when three separate EU Commission investigations were launched to assess if certain online sales by practices prevent, in breach of EU antitrust rules, consumers from enjoying cross-border choice and being able to buy important products or book services, by restricting the ability of online retailers to set their own prices for these widely used items. The Commission also investigated concerns of

[4] See United Nations Conference on Trade and Development (UNCTAD), "Competition issues in the digital economy", 1 May 2019, pg.3. Accessible at https://unctad.org/system/files/official-document/ciclpd54_en.pdf

[5] Ibid. pg.4

[6] See also Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), {SEC(2020) 437 final} - {SWD(2020) 363 final} - {SWD(2020) 364 final}, Brussels, 15.12.2020 COM(2020) 842 final 2020/0374 (COD). Accessible at https://ec.europa.eu/info/sites/default/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf

[7] See United Nations Conference on Trade and Development (UNCTAD), "Competition issues in the digital economy", 1 May 2019. Accessible at https://unctad.org/system/files/official-document/ciclpd54_en.pdf

potential geo-blocking practices by some companies, in which prevent consumers from purchasing digital content because of the consumer's location or country of residence.[8]

3. Gaining market power through the use personal data: the position of digital "gate-keeper"

Traditionally speaking, a gatekeeper is a company that acts as an important link between two or more groups of platform users, e.g. buyers and sellers. When the company attracts a large share of users on one side of the platform (e.g., buyers), gatekeepers can become inescapable connectors for certain markets or customers. This means also that the users on the other side of the platform (i.e., the sellers) may have little choice but to use the gatekeepers' infrastructure. The EU Commission has thought in terms of identifying a 'digital gatekeeper' for as long as Google started selling products to EU consumers. The most famous EU competition law investigations that spurred the Commission's amended approach to digital market regulation are by far the Google ones.

The European Commission has conducted several inquiries against Google practices in the EU market, and one of them resulted in a fine against Google €4.34 billion for breaching EU antitrust rules in 2017.[9] The Commission stated that Google obtained the vast majority of its revenues via its flagship product, the Google search engine. With the emergence of Android smartphones and tablets, Google used its position on the market to ensure that Android users would continue to use Google Search also on their mobile devices.

Since 2011, Google had imposed illegal restrictions on Android device manufacturers and mobile network operators to cement its dominant position in general internet search. The Commission decision concerned three specific types of contractual restrictions that Google has imposed on device manufacturers and mobile network operators. These have enabled Google to use Android as a vehicle to cement the dominance of its search engine. Google has engaged in three separate types of practices, which all had the aim of increasing Google's dominant position in general internet search.

The Commission decision concluded that Google has engaged in two instances of illegal tying:

- First, the tying of the Google Search app. As a result, Google has ensured that its Google Search app is pre-installed on practically all Android devices sold in the EEA. Search apps represent an important entry point for search queries on mobile devices. The Commission has found this tying conduct to be

[8] Commission has investigated potential EU Competition Law breaches by Google on three separate accounts, accessible at respectively https://ec.europa.eu/commission/presscorner/detail/en/IP_15_4921 ; https://ec.europa.eu/commission/presscorner/detail/en/IP_16_922 ; and https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770 . See also https://ec.europa.eu/commission/presscorner/detail/en/ip_17_201

[9] For ref., see CASE AT.39740, Google Search (Shopping), ANTITRUST PROCEDURE Council Regulation (EC) 1/2003 Article 7 Regulation (EC) 1/2003, Date: 27/06/2017. Accessible at https://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf

illegal as of 2011, which is the date Google became dominant in the market for app stores for the Android mobile operating system.

- Second, the tying of the Google Chrome browser. As a result, Google has ensured that its mobile browser is pre-installed on practically all Android devices sold in the EEA. Browsers also represent an important entry point for search queries on mobile devices and Google Search is the default search engine on Google Chrome. The Commission found this tying conduct to be illegal as of 2012, which is the date from which Google has included the Chrome browser in its app bundle.[10]

The EU Commission concluded by stating that in accordance with Article 102 of the TFEU[11], Google has a dominant position in the national markets for general internet search throughout the European Economic Area (EEA), i.e. in all 30 EEA Member States. Google also has shares of more than 90% in most EEA Member States, by therefore reducing the incentives or the ability of rivals to compete effectively with Google.

3.1 Identified shortcomings to current EU competition regulation

- Identification of data-related anticompetitive behavior – it is challenging to identify anti-competitive behavior of market operators that use data, as they do not trade data as a stand-alone business and not relevant market for data can be found as a result under current competition rules. Potentially in some cases, several national challenges stemming from regulatory, enforcement, legislative and judicial entities, when designing, applying, and interpreting EU competition law, might bring as a result non –identification of some anticompetitive behaviors to refer to the Commission.
- *Ex post* intervention – "traditional" antitrust law usually operates on an ex-post manner, meaning that by nature this area of the law is designed to identify or penalize certain anti-competitive behaviors only after they have already occurred.
- Length of the investigative procedures (either by the European Commission or the NCAs) – as practice has proven before, investigations on potential anti-competitive behaviors into these types of multi-tier companies are lengthy in nature and can take up to several years. In the meantime, digital innovation moves at a very high speed. Therefore, the possible damage imposed on consumers before the abusive conduct is properly addressed may be of great proportions.

3.2 Proposed solutions by EU Competition Law

On 15 December 2020, the European Commission published the Proposals for the Digital Services Act package, "*an ambitious reform of the digital space*". The package is composed of the Digital Services Act (DSA) and the Digital Markets Act (hereafter, DMA,

[10] Ibid.

[11] Article 102 of the Treaty on the Functioning of the European Union (ex-Article 82 TEC) ; 2012/C 326/01. Accessed at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012E/TXT&from=EN

Proposal or DMA Proposal).[12] The proposals together aim "*to make sure that we, as users, have access to a wide choice of safe products and services online. And that businesses operating in Europe can freely and fairly compete online just as they do offline.*" [13]

First, the new Digital Services Act proposal makes a shift towards ex ante regulation. As mentioned throughout the course of this submission, the experience of the last years has shown important shortcomings related to the ability to apply (in this case) Article 102 TFEU to a wide array of behavior of large tech corporations which act as gatekeepers, and also, to the timing of intervention, so the EU Commission has proposed the adopotion of a new and flexible ex-ante regulatory framework for large online platforms acting as gatekeepers.

Secondly, the proposal provides criteria which clarify the threshold for competition intervention. The proposals stipulate transparent criteria of assessment on what gatekeepers are, the requirements necessary for designating market players as gatekeepers, the methods of designation and the possibility of companies facing such designation to present countervailing arguments.[14]

Thirdly, it provides predefined obligations and prohibitions which may be imposed once a market player is designated as a gatekeeper, stipulated as a "close-shop' list in order not to stifle innovation.[15]

3.3 Feedback on the Digital Markets proposal

There has been a lot of comments and feedback from EU stakeholders, businesses, National Competition Authorities regarding this Proposal. These stakeholders are saying that first of all, designing a test for an *ex ante* regulation for digital gatekeepers would require lawmakers to define precisely a range of new concepts (e.g. gatekeeper position, relevant areas of business, relevant ecosystem) departing to a certain extent from traditional competition law concepts.[16]

Also, with this new Commission proposal, it should be enshrined in EU law a set of clearly defined and predetermined obligations and prohibitions of certain unfair trading practices (e.g. 'blacklisted practices'), Under this 'do and do not' approach, both general prohibitions that apply regardless of the online platform's sector of activity (e.g. 'self-preferencing') and more specific rules (e.g. relating to operating systems, algorithmic transparency, or issues relating to online advertising services) could be considered.

---

[12] See Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), {SEC(2020) 437 final} - {SWD(2020) 363 final} - {SWD(2020) 364 final}, Brussels, 15.12.2020 COM(2020) 842 final 2020/0374 (COD) accessible at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=en . See also https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

[13] See also C.S. Rusu, J.van den Gronden, B.Beems: "*The Commission's Digital Markets Act Proposal: Boosting Competition on Digital Markets",* accessed on 10 February 2021, at https://www.ru.nl/law/research/radboud-economic-law-conference/radboud-economic-law-blog/2021/commission-digital-markets-act-proposal-boosting/

[14] Articles 2 and 3 of the Digital Markets Act, ibid.

[15] Ibid., pg.9

[16] Ibid., pg.10.

The second approach would be to enshrine in EU law a range of tailor-made remedies (e.g. transparency, data portability, interoperability) that regulators could impose on digital gatekeepers where considered necessary and justified following a prior case-by-case assessment.[17]

It was also proposed that in order for this new proposal on Digital Markers to work, an option would be Data portability mechanisms, which are already implemented in a range of EU legislative acts such as the General Data Protection Regulation (GDPR).[18] This would allow consumers to ask for the transfer of their personal data from one organization to another in order to switch service provider, the Digital Content Directive, which grants a form of portability right for the non-personal data provided or created by consumers, and the Free Flow of Data Regulation which applies to the porting of non-personal data between businesses. In addition, many firms offer portability services, i.e. data transfer between online services, on a commercial basis.[19]

While data portability is seen as an effective remedy in preventing ex ante anti-competitive outcomes, academics have raised a range of questions with respect to regulating ex ante portability of data. In this regard, although beyond the scope of this contribution, one should be wary of the interplay between some of the competition law obligations and other areas of EU law: for example, the obligation to ensure effective portability of data (Article 6(1)(h) Proposal), relates to requirements embedded in the General Data Protection Regulation 2016/679. [20]

Therefore, the EU legislation would need to clarify how the GDPR principles of purpose limitation and data minimization that limit data sharing of personal data would align with a new ex ante right to data portability.[21]

4. The Albanian context: the current antitrust legislation framework in force in Albania

How does the discussion on EU digital intermediaries impact the local markets or how does it relate to the competition law context in Albania? There is indeed no doubt that different jurisdictions, including both those EU or non-EU jurisdictions, make different assessments of where the balance of under and over-enforcement risks lies. These assessments cannot be separated from the underlying legislative, historical, and philosophical context of competition law in each jurisdiction. In this context, some queries to address throughout this section may be as follows:

- Are digital gate-keepers active in the current Albanian market setting? Are there any big-sized companies (measured for instance by the ability for business users and

[17] Ibid., pg.15

[18] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Accessible at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

[19] Ibid., pg. 5

[20] Ibid.

[21] Ibid., pg.27

consumers to switch between different platforms) that might not necessarily be operating in Tech, but that due to their dominant position on the market gained by (partly) using customer data, may obtain the tools to potentially engage in anti-competitive behavior in the future?

- Is there any immediate need for attention, i.e., is there risk that an identified anti-competitive behavior by a large company in an EU market setting potentially spill over into the Albanian market?
- What tools at the current disposal of the Albanian Competition Commission may be sufficient to identify potential anti-competitive behavior (e.g. abuse of a dominant position) in emerging digital markets in Albania?

For the purpose of conducting this analysis, we should take an initial look at the domestic legislation on the protection of competition. The scope of application of Law no 9121 date 28.7.2003 "On the Protection of Competition', amended [22] includes:

a) undertakings and groupings of undertakings, which, directly or indirectly, affect or may affect the market;

b) all entities defined in this point, which exercise their activity in the territory of the Republic of Albania, as well as for those that exercise their activity outside this territory, if the consequences of this activity are felt in the internal market.

- *Law no 9121 dated 28.7.2003 "On the Protection of Competition", amended: Article 3 -Definitions*

The law has defined the concepts of 'undertagin' and 'dominant position' on the market as:

1. "Undertaking" is any natural or legal person, private or public, that performs economic activity. Enterprises are also considered central and local administration bodies, as well as public entities or institutions, when performing economic activities.

[…]

5. "Dominant position" is that economic power held by one or more undertakings which gives them the opportunity to impede effective competition in the market by enabling them to act, in terms of supply or demand, in independently of other market participants, such as competitors, customers or consumers.

Analyzed from a general point of view, Article 2 of the Law no 9121 dated 28.7.2003 "On the protection of competition' last amended in 2010, has more or less a wide coverage of what constitutes an economic operator that may be subject to the law. Also, if we see the stipulation of the wide-coverage term 'undertaking', then we might say that digital sellers may also be included under this umbrella. The formulation of these two sub sections of Article 2 are similar to those stipulated by EU competition case law on what constitutes an undertaking.

In addition, sub section 5 of Article 3 of the Law is in accordance with the definition of dominant position detailed in Article 102 TFEU and Article 1 (3) of Council Regulation 1/2003[23] on the implementation of rules.

[22] Article 2/1 of the Law no 9121 date 28.7.2003 "On the Protection of Competition', amended in 2010. Accessible at https://www.vendime.al/wp-content/uploads/2015/07/LIGJI-PER-MBROJTJEN-E-KONKURRENCES-i-perditesuar.pdf

[23] Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty. Accessible at https://eur-lex.europa.eu/eli/reg/2003/1/oj

Also, Article 3/7 of the Albanian Law defines the relevant market as:

7. "Relevant market" are products that are considered as substitutable (interchangeable) by consumers or other customers, in terms of their characteristics, price and function, and that are offered or requested by companies in a geographical area with the same conditions of competition, an area which is separated from other restricted areas.

From way of interpretation, or at least in this author's optics, it seems that the Albanian Law on Competition in article 3/7 describes a market in its traditional "brick and mortar" sense, i.e that focuses mainly on retailers/economic operators that offer their products in a regula shop, at a certain (physical) geographical area, where same or similar conditions of competition apply.

Meanwhile, as specified previously numerous times, online trade in Albania has been rapidly developing these recent years, up to the point where it is a prominent way of purchasing, especially for the younger generation. In Albania as it stands, many consumers can buy all sorts of merchandise nowadays, electronic equipment, household appliances, travel bookings, clothes etc, most of which are advertised and sold by stores with an online presence through Facebook, Instagram or other similar social networks. Online shopping in Albania, but also in the rest of the world has become the norm, especially now during the global pandemic, where all business is conducted in an online settings.

Secondly, this Article of the Law mentions a certain geographical area as a condition to establish a certain market, but online trade from market places such as Google, Facebook Marketplace, or Instagram, blurres a bit the lines on the effectiveness of the tools currently set by the legislation to establish a specific market. These types of engines, as we have all have experiences first hand as consumers, 'keep learning' about its customers' characteristics and preferences through the use of personal data. This knowledge allows for more effective matching between users and therefore leads to more valuable interactions. In turn, the larger number of interactions results in more data, which again allows for improvements of the platforms. In other words, the platform 'learns' how to best facilitate interactions from the interactions.

There is perhaps another aspect to consider vis a vis markets' identification: in the framework of the Berlin Process initiated by EU leaders since 2014[24], some of the countries of the Western Balkans region, including Albania, have approved in 2020 the political commitment to create a Regional Common Market.[25] The aim of establishing this Common Regional Market would be igniting closer regional economic integration between the countries of the WB region, and bringing its companies closer to the EU Internal Market. Considering that at this stage, such an initiative still remains in the

[24] The Berlin Process is an intergovernmental cooperation initiative aimed at revitalizing the multilateral ties between Albania and other Western Balkans and selected EU member states, and at improving regional cooperation on the issues of infrastructure and economic development. This initiative includes six Western Balkan countries that are candidates for EU members, including Albania, potential EU member candidates, and some EU member states. For ref., please see also https://berlinprocess.info/

[25] "*Western Balkans Leaders Declaration on Common Regional Market: A catalyst for Deeper Regional Economic Integration and a Stepping Stone Towards EU Single Market*", 2020. Accessible at https://berlinprocess.info/documents/

political phase, there is no legal instrument in place to regulate any modalities. However, it might be interesting to think in advance on what may be the effects of creating this Regional Market for existing market entities in the region with a dominant position (or those potentially dominant after a complete integration of this Common Regional Market), or on the effects on how the digital markets of the region can be calculated in the future.

In third, while the concept of gate-keeper is of no current mention in the Albanian law on the protection of competition - of course due to being so recent - there are already in Albania few big companies with a dominant position on the telecommunication market, who hold strategic market status. These companies also sell many digital products and equipments through their respective websites, meaning that they at the least, store to a specific degree their consumer's data. Therefore, pertaining to market significance, if we were to take a look at these companies' size and scale, their potential ability to leverage their market powers into a variety of other markets, and their positions as an access point for businesses to customers, then maybe we could judge whether there might be potentially room or not to state their ability to be a gatekeeper. Of course it is not illegal for an undertaking or company to have a dominant position on the market for as long as it does not engage in abuse, but in any case we should keep in mind that in Albania in recent years that have been a lot of innovation products put forward by young start ups, which would naturally want to find a selling market. The rapid pace of change in the digital markets can make it difficult to understand how likely it is that a small start-up or firm might face competitive pressure in the long term by firms with a dominant position.

4.1 The role of the Albanian National Competition Authority in Emerging Digital Markets

If we take a detailed look into the decisions for these past three of four years by the Competition Commission of Albania (*Autoriteti i Konkurrencës*), it would be clear that it conducts and *ex post* intervention, in stipulation also with the Law on Protection of Competition.[26] Moreover, digital practices or online trade services are not really an immediate priority of the Commission, perhaps due to the fact that even at EU level as mentioned, there is still a lot of regulation guidance and fine-tuning needed to be used as example by the NCAs. Alternatively, the National Authority in Albania considers this issue to mainly be a criminal law domain (data privacy protection) and thus to be monitored by other relevant legislative bodies.

At any rate, I would suggest that the Albanian antitrust legislator and the Albanian competition regulatory bodies may wish to take a closer look to recent digital developments in the EU and legal initiatives in the EU, and see how this example can be implemented in Albania.

5. Conclusions and Recommendations

[26] See http://www.caa.gov.al/cases/list/category/2/page/1

The following are some brief reflections on the ongoing discussion of the impact of digitalization for legislators and competition law regulators. Some of the suggestions in the EU context are also reflected in the stakeholders' feedback following the Commission's Digital Markets proposal.

The EU context:

Ex-ante vs *ex-post* intervention – EU Competition experts have stressed that even with clearer *ex-ante* rules, *ex-post* antitrust enforcement will remain an important backstop. According to these opinions, the new EU proposal on Digital Markets must clarify how the proposed *ex-ante* regulatory framework would operate alongside the planned new competition tools and the current competition rules in order to avoid the risk of both under- and over-regulating digital gatekeepers. This would require the adoption of *ex-ante* rules flexible enough to be updated without heavy and lengthy legislative procedures and securing effective cooperation between the authorities in charge of monitoring the market, conducting market investigations and issuing compliance orders. In any case, an *ex-ante* framework should be based on case-by-case assessment and tailored remedies to avoid stifling investment and innovation.

Taking a cue from the EU NCAs (e.g. the Dutch model) – Reverting to the initial EU Commission's new proposal on Digital Markets and Digital Services, a very important feedback that scholars have suggested that the Commission needs to fine tune further is establishing clear cooperation mechanisms set up between the various authorities at EU level (i.e. Commission departments) and between the Member States (NCAs) in order to determine who is best equipped to intervene when coming across anti-competitive behavior.

In this regard, the Netherlands has proposed implementing the requirement of "interoperability" in the digital - and – platform economy. Broadly speaking, 'interoperability' refers to the ability of a system, product or service to communicate and function with other technically distinct systems, products or services. Horizontal interoperability refers to interoperability of competing products, services or platforms (e.g. interconnection between communication networks) while vertical interoperability refers to interoperability of a product, service or platform with complementary products and services (e.g. an e-book readable on different platforms). In the EU, interoperability requirements have already been used to promote competition in telecommunications (e.g. the Access Directive), Fintech (e.g. the Revised Payment Services Directive) and the software industry (e.g. the Microsoft case).[27]

The Dutch State Secretary described that the new EU regulatory telecom framework, which has yet to be implemented in The Netherlands, creates the possibility for the Dutch Authority for Consumers and Markets to also impose interoperability-requirements on non-traditional communication service providers, such as Skype and

[27] See "Dutch position on the Digital Markets Act" (2020), accessible at https://www.permanentrepresentations.nl/documents/publications/2021/02/17/dutch-position-on-the-proposal-for-the-digital-markets-act . See also Judgment of the Court of First Instance (Grand Chamber) of 17 September 2007, "Microsoft Corp. v Commission of the European Communities", ECLI:EU:T:2007:289.

WhatsApp (who offer number-independent communications services). According to the State Secretary, interoperability issues could also arise with other services. In that case, the proposed gatekeeper instrument could be used to prevent the potential impediment to competition. For example, the authority could prohibit (*ex-ante*) to offer less interoperability to third party services than the platform's own services.[28]

The Albanian context:

Developing a new National Cross-cutting Strategy for Information Society, which should incorporate a plan on emergening digital markets in Albania – as we speak, the current Cross-cutting Strategy for the Information Society, titled "Albanian Digital Agenda 2014-2020" [29]does not review digital developments from a competion law angle or concern.

Establishing a working group, or an expert group within the Albanian Commission on Competition to receive feedback from different market stakeholders, regulatory bodies and consumer associations - whether the introduction of a new Regulation of the Albanian Commission Authority is needed or not. I would personally not be of the opinion to change the law on competion for the time being, but a soft law type of apporach might work in orde to identify potential competition concerns in online trade in Albania. In addition, it would be quite useful to be able to identify which areas of the national competiton law might need improvement or amendments in the near future, considering also that this legislation would have to be harmonized soon with the EU acquis on competition policy, as part of Albania's ongoing path towards full EU membership.

Liasing the new digital market competition regulation by the CA with Law No.10 128, dated 11.5.2009 "On Electronic Commerce", amended by Law no. 135/2013 [30] – this is not a very used or recognized piece of legislation in Albania, but should be perhaps useful to integrate some definitions and principles on the information society service provider, the protection of consumers, etc., into a new regulation for digital markets.

Increased exchange levels of information and, if necessary, undertaking of coordinating measures of the CA with the relevant institutions stipulated in the law on consumer protection (Law no 9902 date 17.04.2008 amended) as well as the institution responsible for privacy data protection in Albania.

[28] Ibid.

[29] Accessible at https://akshi.gov.al/wp-content/uploads/2018/03/Digital_Agenda_Strategy_2015_-_2020.pdf

[30] Law No. 10 128, dated 11.5.2009 'On Electronic Commerce', amended by Law no. 135/2013 "On some additions and changes to law no. 10128, dated 11.5.2009 "On electronic commerce". Accessible at https://aida.gov.al/images/PDF/Ligji_10128_per_Tregtine_Elektronike_i_ndryshuar.pdf

Multi-sided platform abuses and optimal enforcement design – Law & Economics considerations

Prof Dr Stefan E. Weishaar MSc, LLM[1]

1. Introduction

In 1890, at a time when trust companies were swaying a dominant power over the American economy, the Sherman Antitrust Act was introduced. An important objective of it was to protect democracy as people feared that a rise of big business could affect democratic political participation.[2]

Competition laws were also introduced in other industrialized countries in the world, notably in Germany (in 1923). But it was not until the European Coal and Steel Community (1951) and the Treaty of Rome (1958) that Competition law obtained a stronger role in Europe, arguably to enable market access to coal and steel after the second world war[3]. In recent years, we have seen a stronger proliferation of competition laws around the world, several of them having marked features of extraterritorial application, especially the US, EU and China.

Since the early 2000s, the development of increasingly potent algorithms and business models challenges democracy and Competition law again. Through the use of the internet, or the application of apps companies that process personal data (data companies) are able to profile consumers, provide personalized advertisement and adopt search results. This leads to a situation where information found on the internet is tailored to a personalized profile. Based on what an algorithm determines to be of interest to an individual will be presented in the search results, reinforcing the believes and viewpoints of the person. In times where increasing amounts of information are not consumed via the traditional news channels (newspapers or TV news) this poses obvious problems to democracy.

The business models employed by these data companies rely on multisided markets and pose challenges to Competition law enforcement. The problems that two

[1] Professor of Law and Economics, Faculty of Law, University of Groningen, The Netherlands.

[2] See Laura Phillips Sawyer (2019) US Antitrust Law and Policy in Historical Perspective, Harvard Business School Working Paper Working Paper 19-110, https://www.hbs.edu/ris/Publication%20Files/19-110_e21447ad-d98a-451f-8ef0-ba42209018e6.pdf, p. 4

[3] Richard T.Griffiths, (2004) Griffith lectures History of the European Union, An audio course on the Origins and Development of the E.U., available at: https://www.home-academy.nl/products/history-of-the-european-union

sided (or multisided) markets pose for Competition law enforcement have been identified in the 2000s by Rochet and Tirol.[4] Such multisided business models are characterized by significant network effects between the markets, where the profit maximization decision is based on the interdependent demand of all serviced markets, often with substantial amounts of cross subsidization where one side essentially cross-subsidies the other. Advertising companies for example pay so that Facebook can offer its services without remuneration to consumers. Also the service to consumers is not for free, as they spend time to watch advertisements and surrender their private data (interests, pictures, etc.) to Facebook, often without reading the privacy policies and without understanding what can be done on the basis of their personal data.

This paper does not have the ambition to present a summary of the multi-sided platform (MSP) literature, but to offer Law and Economics considerations on how abuses of data companies extorting personal data to sell to advertising companies could be addressed.

In order to delineate the object of analysis the paper, first concisely introduces multi-sided platforms (section 2) before continuing to highlight the resulting challenges they pose to current Competition laws (section 3). Section 4 will then present the Law and Economics works on public and private enforcement and analyze if the current enforcement regime works effectively to deter extortionary behavior of data companies against private parties. In section 5, alternative deterrence via data protection rules is discussed. A conclusion will highlight the main points.

2. Multisided platforms

This section of the paper offers a concise introduction to MSPs in order to delineate the object of research. This section is based on Evans (2008).[5] MSPs provide goods or services to two or more distinct groups of customers who need each other. They thereby facilitate exchanges between them that otherwise would not have been occurring due to too high information and transaction costs between the parties involved.

MSPs have various functions. Evans (2008) presents a typology of various forms of Multisided markets and distinguishes according to their function. MSPs can facilitate matchmaking, enabling one side to find the other (e.g. eBay). They can also build an audience so as to facilitate match making (e.g. Google). Or MSPs can efficiently provide shared resources at lower costs to all members (e.g. Linux).

A key feature of the MSPs is thus that they are serving two separate markets at the same time. The profit maximization decision in such situations will depend on the value an additional customer on one market is capable to generate on the other market. Such effects are conventionally described as 'indirect network effects'.[6]

[4] Jean-Charles Rochet and Jean Tirole (2003) Platform Competition in Two-Sided Markets, 1 J. Eur. Econ. Ass'N 990 ;Jean-Charles Rochet and Jean Tirole (2006), Two-Sided Markets: A Progress Report. Rand Journal of Economics 37(3): 645-67.

[5] Evans, David (2008) Competition and Regulatory Policy For Multi-Sided Platforms with Applications to the Web Economy, available at: http://ssrn.com/abstract=1090368

[6] Evans, David (2008) Competition and Regulatory Policy For Multi-Sided Platforms with Applications to the Web Economy, available at: http://ssrn.com/abstract=1090368 p. 7

Another characteristic of MSPs which seems to be related to indirect network effects is that there is often an asymmetry in the pricing schedules for the parties involved. The side that is 'more important' or 'harder to get' tends to pay less for the service. There is thus an amount of cross-subsidization between the separate markets. There are also markets where there is no monetary payment at all requested from one side, or where the payment takes a different form. The use of Facebook for example is for free for individuals but 'payment' is taken in the form of obliging them to divulge private information and/or by requiring individuals to spend time to watch advertisements when watching for example videos on YouTube.

Markets with such characteristics are inherently difficult to set up because the viability of the business model depends on having a big enough customer base to motivate the customers on the other market to pay a premium for the services offered. But once established successfully, there is the possibility to offer attractive services to both markets and to grow. This is due to the substantial degree of economies of scale on the cost side but also on the demand side. Such markets can then develop into the winner takes most if not all markets, where there will be one or only a few large firms operating in the market. MSP markets can thus develop into concentrated industries.

3. Competition law challenges

The previous section has explained that MSP markets can give rise to concentrated markets and are often characterized by one market cross-subsidizing the other market.

From a Competition law perspective, this could give rise to markets where undertakings hold a position of dominance on a relevant market that can be abused. Standard approaches to Competition law and industrial economic techniques are, however, not easily applied to MSP markets. MSP markets must be assessed jointly to determine competitive constrains but can be challenged by other MSPs, single sided competitors, or vertically integrated competitors that attack their profit centers.

The standard market definition for example requires the determination of a relevant market. The SSNIP-test (Small but significant and non-transitory increases in price) is used to help to determine the relevant market by analyzing if consumers regard a product as a substitute. Yet MSP business models are not characterized by substitutes on one market but are only understood when connecting separate markets.

Also analyzing the conduct of undertakings on a single market could be problematic as the setting of low or no prices for one customer group could constitute predatory pricing. The Court of Justice of the European Union (CJEU) established first, that undertakings holding a dominant position and charging prices below average variable costs must be considered *prima facie* abusive inasmuch as in applying such prices they pursue no other economic objective than to eliminate its competitors. Second, the CJEU held that prices between average total costs and average variable

costs are abusive if they form part of a plan to eliminate competitors.[7] Such a presumption can be rebutted, but it is very difficult.[8]

In order to distinguish between lawful and unlawful intends to exclude competitors the CJEU relies on sound and consistent evidence that can be direct or indirect.[9] There is a wide discretion in the type of evidence used to prove an exclusionary intent.[10] But unless there are 'paper trails' that management forgot to clean up, or where management was bragging imprudently, indirect evidence may be relevant. In any event, the recouping of losses is not something that must be established to prove predatory pricing.[11] Yet cross-subsidization is a marked feature of MSPs, and below cost pricing may indeed be a valid path to profit maximization for companies.

Another abusive conduct, the charging of excessively high prices, may also be relevant in the context of MSPs. Exploitative abuses such as the charging of high prices are prohibited under Article 102(a) TFEU as an abuse that directly or indirectly imposes unfair purchase or selling prices or other unfair trading conditions. There are, however, only few cases where undertakings' exploitation of their dominant position has been prohibited so that the thrust of enforcement of Article 102 TFEU is mainly directed against exploitative abuses.[12]

Employing competition law to control exploitative pricing is also not straight forward because excessive profits will attract new competitors to the market that will end the dominance and drive down prices, provided of course that there are no inhibiting barriers to entry.[13] The US Sherman Act for example does not address excessive pricing.[14] There is also no uniformly accepted economic method to identify excessive prices which renders identifying them both difficult and controversial.[15] In essence an objective and reasonable price needs to be determined and compared to the price that is actually charged, then it needs to be determined if it is excessive or not. Moreover, monopoly profits even if working to the detriment of consumers constitute economic transfers between parties and are as such not objectionable; the reduction of social welfare stemming from too low production levels and distortions of overall production is of course problematic. Another challenge regarding excessive pricing abuse is that any legal rule designed to condemn exploitative pricing must be robust and predictable for the regulatee so as to avoid undue legal uncertainty. Moreover imposing pro-competitive legal remedies beyond fines is complex, probably requiring continuous monitoring, and adding to the challenge of addressing and containing excessive prices. Another obstacle to addressing excessive pricing is that it requires the competent competition authority to have considerable information

[7] **C-62/86** ***AKZO Chemie BV v Commission****, (1991) ECR I-03359, para.* 71 and 72, and **Case C-333/94** ***P Tetra Pak International SA v Commission,*** *(1996) ECR- I-05951, para 41, and C-202/07 France Telecom v. Commission* (2009) ECR I-2369, para 109.

[8] Roger van den Bergh (2017) Comparative Competition Law and Economics, Edward Elgar, p. 345

[9] Case T-82/91 Tetra Pak International v. Commission (1994) ECR II-755, para 151.

[10] Roger van den Bergh (2017) Comparative Competition Law and Economics, Edward Elgar, p. 346

[11] 202/07 France Telecom v. Commission (2009) ECR I-2369, para 110.

[12] Sufrin and Jones (2011) EU Competition Law, 4th edition, p. 363

[13] This section is based on Richard Wish and David Bailey (2012) p. 718 ff.

[14] See Richard Wish and David Bailey (2012) p. 718, footnote 8.

[15] See Richard Wish and David Bailey (2012) p. 721 ff.

regarding prices, costs and the market at its deposition – something that in reality it may not have.

An important problem with regard to MSPs and the case of consumer exploitation by data companies is of course that Article 102(a) TFEU addresses the charging of high prices. Yet, collateral for the services rendered are non-monetary in nature, thus in terms of time consumers spend to watch advertisements or personal data that they surrender. Monetizing these forms of payment is possible of course via employing shadow pricing methodologies but it is not entirely clear if the scope of Article 102(a) TFEU could be expanded to include such collateral. In any event, Article 102(a) TFEU has been used to sanction unfair trading practices imposed by dominant firms on its customers.[16] Though in its Facebook case the Bundeskartellamt refrained from relying on European Competition law and relied upon Article 19(1) GWB instead. This provision is modeled upon Article 102 TFEU and sanctions any abuse of a dominant position.[17]

4. Law and Economics insights on public and private enforcement

The previous section has shown that the application of Competition law to MSPs is not easy. A dimension added by Law and Economics to the discussion of legality of particular conduct under Competition law is if the enforcement is efficient or not. Nobel Prize Laureate Gary Becker made the point that not every trespass must be punished and deterred because enforcement is costly. To maximize social welfare it is important to compare the social marginal costs of enforcement to the social marginal benefits of enforcement.

One important complexity closely related to the efficiency of enforcement is if it should best be public or private. Analysing the case at hand, it is apparent that private enforcement runs into several issues.

Private parties may for example not even realize that they are harmed. Be it that they underestimate the overall amount of time they spend by watching advertisements or by being unaware of the privacy implications and associated economic consequences.

For private parties, the costs of proving damage and the causal relationships often are prohibitively high. Many violations against private parties will therefore not result in litigation. This is particularly the case when the damage costs for individuals are relatively small, then public enforcement or class action must be relied upon.

In order to determine if it is beneficial for private parties to seek enforcement of their rights, they will compare their costs and benefits. Their decision will be guided by their private costs and benefits with little if any consideration for the societal benefits stemming from enforcements. Yet the rectification and deterrence of violations has societal benefits not only from an abstract ethical viewpoint but also because it might lead to the cessation of undue business practices all together, thereby

[16] Botta, M., and Wiedemann, K., (2019) The Interactino of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyseey, The Antitrust Bulletin, Vol. 64(3) pp. 428-446, p. 441

[17] Botta, M., and Wiedemann, K., (2019) p. 441 are critical of the legal choice made by the Bundeskartellamt and point out that it offers the advantage that German law and cases are applied rather than EU law.

creating positive externalities for other actual and potential victims. Law and Economics describes these benefits as positive externalities that are insufficiently taken into account by private enforcement.

Bearing tribute to the positive externalities just presented, there are also perverse incentives that render private enforcement less effective. Individuals have an incentive to wait for other victims to start procedures. Such behaviour is commonly referred to as free-riding.

Reliance on private enforcement can also give rise to wrong judgements if adjudication is done by judges that do not have the necessary economic or technical training. Having specialized courts or public enforcement in such situations could help to minimize such costs of convicting the innocent (a false positive, type I error) or letting the culprit go free (a false negative, type II error).

Private enforcement has several advantages over private enforcement. Public authorities are endowed with qualified staff and funds and can actively monitor markets. They may also have an information advantage in detecting and proving infringements and also in terms of higher likelihood of legal enforcement and conviction of trespassers.

There are, however, also situations where public enforcement encounters difficulties. For example in situations where private parties have better information at their disposition. Another example are situations where the public fines are too low to offer effective deterrence or where staff and funds are inadequate in monitoring violations and enforcing the law. In such situations private enforcement is a crucial complement to public enforcement. Public enforcement may also be suboptimal if there are biases in the enforcement. These can for example stem from self-interested civil servants and public choice type of problems.

Discussion of private and public enforcement in the case at hand

In light of the foregoing presentation of Law & Economics insights, it is apparent that private enforcement would have to overcome non-trivial challenges when addressing the case at hand. Private parties can be expected to suffer severely from information asymmetry. Individuals are largely ignorant about the capabilities of big data, face recognition or search algorithms. Private parties will therefore not easily bring law suits, especially also because the damage costs for an individual are very difficult to detect, to prove and causality is not easily established. There is thus a mismatch between the benefits and costs of litigation for individuals that is not easily overcome. In the absence of class action cases they can easily join, private parties might prefer to free-ride rather than to engage in litigation themselves.

In 2001 the CJEU held in *Courage* that the full effectiveness of Article 85 TEC (now 101 TFEU) would be endangered if it were not open to any individual to claim damages suffered from a contract or by conduct liable to restrict or distort competition.[18] This principle has also been extended to infringements under Article 102 TFEU.[19]

[18] C-453/99 – Courage and Crehan, ECLI:EU:C:2001:465, paragraph 26. But also C-295/04 – Manfredi, ECLI:EU:C:2006:461, paragraph 60; Case C 360/09 – Pfleiderer, ECLI:EU:C:2011:389, paragraph 28; C-199/11 – Otis and Others, ECLI:EU:C:2012:684, paragraph 41; C-536/11 – Donau Chemie and Others, paragraph 21; C-557/12 – Kone and Others, ECLI:EU:C:2014:1317, paragraph 21.

[19] C-637/17 – Cogeco Communications, ECLI:EU:C:2019:263, paragraphs 39 and 40.

The core Competition law Articles 101 and 102 TFEU are directly applicable and alongside Regulation 1/2003[20] on the implementation of the rules on competition constitute the foundation of private Competition law enforcement. The 2014 Damages Directive[21] prescribes a series of minimum requirements for harmonizing private competition enforcement but Member States retain discretion in the implementation so that private enforcement regimes across the Member States differ. The Commission report on the implementation of the Damages Directive points out that – albeit still too early to draw firm conclusions - the number of damage actions before national courts has significantly increased and damage actions have become much more widespread in the EU and concludes that the rights of victims of antitrust infringements have been substantially strengthened in all Member States.[22]

For long the European Commission has recognised the importance of further strengthening private enforcement in EU law and EU Competition law and issued several notes[23] and recommendations to introduce collective redress mechanisms in damage claims, as exemplified in its 2013 recommendation,[24] though this recommendation merely mentions competition in its recitals. The recent Directive on representative actions for the protection of collective interests of consumers does not extend to Competition law.[25]

There are several Member States where collective redress mechanisms allow Competition law claims including the Netherlands, Italy, Belgium and France, while Germany for example does not allow for collective redress in Competition law but other alternative models for bundling cases are available and, legal cases will still have to be decided.[26] The effectiveness of private Competition law enforcement will thus depend on the stringency of the particular national provisions.

In situations where private enforcement falls short, public enforcement should be considered to address MSP abuses. As presented in the preceding section, however, there are several methodological challenges that need to be overcome. These challenges are of course also encountered in private Competition law enforcement cases. Besides establishing an abuse on the relevant market these include the estimation of the prices for the time customers spend watching ads and the value of the private data and the determination and objective benchmark prices for services

[20] Council Regulation (EC) 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty [2003] OJ L1/1.

[21] Directive 2014/104/EU of the European Parliament and of the Council of 26 November 2014 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union Text with EEA relevance, OJ L 349, 5.12.2014, p. 1–19

[22] See COMMISSION STAFF WORKING DOCUMENT on the implementation of Directive2014/104/EU of the European Parliament and of the Council of 26 November 2014 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union, Brussels, 14.12.2020 SWD(2020) 338 final

[23] See Towards a Coherent European Approach to Collective Redress: Next Steps, SEC(2010) 1192, 5 October 2010 OJ 1932.

[24] Commission Recommendation of 11 June 2013 on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union Law, *OJ L 201, 26.7.2013, p. 60–65, recital 7.*

[25] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (Text with EEA relevance) OJ L 409, 4.12.2020, p. 1–27. See Annex I.

[26] Johannes Hertfelder and Ines Bodenstein, (2021), Collective or Class Actions and Claims Aggregation in the EU: the Defendant's Perspective, Global Competition Review

rendered. It also includes the question if non-monetary costs would at all fall within the ambit of Article 102(a) TFEU.

Both public and private enforcement may therefore give rise to under deterrence and it may therefore seem that Competition law, neither in terms of private or public enforcement, seems to be particularly well placed to address the problem at hand. Alternatives should therefore be considered.

5. Alternative deterrence via data protection rules

In light of the challenges for Competition law enforcement and the resulting under deterrence of violations relating to MSPs and private parties, it might be expedient to take a look at alternative instruments for deterrence.

For violations of data protection principles, including the principle of transparency, the GDPR provides the possibility to impose administrative fines of up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.[27] Also private damage cases can be brought before competent national courts by any person who has suffered material or non-material damage as a result of an infringement and receive compensation from the controller or processor for the damage suffered.[28] Proving violations will be relatively easier since damages can be both material and immaterial and thus go beyond economic proof of damage. So the GDPR may constitute a more convenient way for individuals to claim for compensation than Competition law.

It of course needs to be pointed out that the by applying data protection rules, even if applied successfully, the actual Competition law violation of abuse is not punished, but it may still be deterred as a fine may very well reduce the profitability of the MSP business scheme. It also needs to be pointed out that there is also a significant difference in the prima facie level of public fines. Under the GDPR it is only up to 4% of the annual turnover while under Competition law it is 10%. Yet in practice it may not make a significant difference in terms of deterrence as the maximum fine is rarely applied in Competition law cases.

Article 80 GDPR allows for representation of data subjects. The GDPR falls within the scope of Directive (EU) 2020/1828 on representative actions for the protection of the collective interests of consumers, as it is listed in Annex I of the directive, so the application of class action may be easier than under competition law as such. The ease of enforcement under the GDPR may therefore give rise to a higher level of deterrence than competition law.

In case where both public and private enforcement are falling short of providing adequate deterrence, regulatory intervention should be considered to prevent abusive conduct. In the area of Telecommunication for example the concern for excessive pricing led to (price) regulation and the decline of prices.[29] Sector specific regulation is, however, not trivial to design, enforce and to keep up-to-date. Especially

[27] GDPR Article 83(5).
[28] GDPR Article 82(1) and 82(6).
[29] DIRECTIVE (EU) 2018/1972 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 December 2018 establishing the European Electronic Communications Code L 321/36, 17.12.2018 and European Commission, MEMO/08/438, Brussels, 26 June 2008, Termination rates: Questions and Answers

in sectors that are characterized by rapid technology advances, business model innovation and that swiftly penetrate extend to other markets or that strongly vertically integrate.

With the 10th amendment of the GWB[30] that entered into force on the 19th of January 2021, Germany has introduced Article 19a GWB that enables the Bundeskartellamt to take preventive measures against companies that hold a position of paramount significance across markets (Ueberragende Marktuebergreifende bedeutung). In order to determine if a company holds such a position factors including access to data relevant for competition and vertical integration are considered, thereby highlighting the challenges of big data companies.

Also the European Commission has undertaken action and on 15th December 2020 proposed the Digital Markets Act[31]. This regulation would enable the European Commission to oblige large digital companies (so called 'gate keepers') to grant access to platforms, consumer data or other relevant information and forbid abusive practices including tying, bundling or self-preferencing.

6. Conclusion

Since the early 2000s competition regulation tries to address multisided platform markets. An increasing number of competition law cases brought against big data companies bears testimony to the struggle of competent enforcement authorities to prevent abusive behaviour. Despite ever higher record fines, the business models continue to strive and data companies seem to grow ever more potent. Since traditional competition law approaches are not easily applied to multisided markets, it is unsurprising that also consumers are left in a precarious position. This paper has examined in how far consumers can rely on competition law to prevent abuses. It was found that private enforcement is unlikely to lead to adequate deterrence because consumers may not know the extend of the damage because they are inadequately informed about the potency of data that is being collected (information asymmetry) and damage calculation is difficult. Moreover, the overall costs for an individual is low, certainly in comparison to the costs of launching and conducting a legal proceeding. To mitigate collective action would be important. Yet also collective action claims, just as public enforcement, encounters the problem that the current industrial economic and competition law approaches to abuse of dominance are mainly geared to abuses on relevant markets and hence not adequately reflecting the strong network effects of multisided markets.

It has therefore been proposed to examine an alternative route for effective deterrence: this has been found on the basis of the GDPR where both material and immaterial damages can be compensated without having to proof economic facts required in the context of a competition law proceeding. Obviously this alternative approach does legally not cure the abuse, i.e. the infringement of competition law, but

[30] Bundesgesetzblatt Jahrgang 2021 Teil I Nr. 1, ausgegeben zu Bonn am 18. Januar 2021
Gesetz zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 und anderer Bestimmungen (GWB-Digitalisierungsgesetz)1 Vom 18. Januar 2021

[31] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act), COM/2020/842 final

damage payments rendered under the GDPR would help to recoup undue profits resulting from abusive practices and hence serve as an effective deterrent against abusive practices. Perhaps the best is the enemy of the good, and it is better to act to prevent markets from developing into certain directions by whatever effective means possible.

It has also been pointed out that recently jurisdictions have started to propose or even enact the Digital Markets Act and the 10th amendment to the GWB. These constitute ex-post measures to regulate digital companies and practices that are also associated with multisided markets. Such regulation does not work to solve legal cases ex-post but is much more focussing on the ex-ante regulation so as to avoid challenges to competition law and to ensure a more level playing field. Consumers that have already been harmed have little to gain from such measures, but they may still take comfort in the hope that for their future much detriment could be avoided through such market interventions.

The European Union's evolution of Market Manipulation offence

Marina Poggi d'Angelo Ph.D. [1]

1. Introduction

The purpose of this paper is to outline the importance, nowadays, to regulate the European financial market in an effective way, not only providing administrative sanctions but especially implementing criminal sanctions. The reasons for this are twofold: firstly, to allow economic resources to circulate efficiently and safely; secondly, to protect investors' savings.

The most important function of financial markets is the efficient allocation of resources to produce goods and services in the future. There is a strong link between the development of the financial system and economic growth and indeed when savings, as an unspent income, are made available to investors, they fuel the growth process of an economic system.

When adopting this point of view, it may happen that providing only administrative sanctions in serious cases of market abuse is not effective to achieve the integrity of the financial markets as a whole. As stated in Recital 6 of the Market Abuse Directive (MAD II): «*it is essential that compliance with the rules on market abuse be strengthened by the availability of criminal sanctions which demonstrate a stronger form of social disapproval compared to administrative penalties. Establishing criminal offences for at least serious forms of market abuse sets clear boundaries for types of behaviour that are considered to be particularly unacceptable and sends a message to the public and to potential offenders that competent authorities take such behaviour very seriously*».

On 6th of August 2021, the European Securities and Markets Authority (ESMA), the securities and markets regulator of the European Union (EU), published a Report of the Market Abuse Regulation (MAR), which is the first in-depth review of the functioning of MAR since its implementation in 2016[2]. Accordingly, ESMA carried out the mapping exercise of the application of the administrative and criminal sanctions, collating the data provided by National Competent Authorities in relation to a given period (2017-2019).

The responses regarding the criminal sanctions imposed over the reporting period show a certain dispersion: whereas three authorities (Finland, Ireland and Poland's authorities) do not report any criminal sanction over the reporting period, Norway and

[1] PhD in Criminal Law - Law Faculty - La Sapienza University (Italy).
E-mail: marina.poggidangelo@uniroma1.it.
[2] The report is available at: https://www.esma.europa.eu/press-news/esma-news/esma-publishes-outcomes-mar-review.

Germany's authorities report the existence of a significant number of MAR criminal sanctions.

The responses provided by National Competent Authorities in relation to the administrative sanctions imposed on insider dealing and market manipulation over the reporting period are similarly disperse. Overall, it can be concluded that a relatively low number of administrative sanctions were imposed in the timespan under examination.

The ineffectiveness of administrative sanctions is the reason why providing a specific offence for market manipulations in serious cases is considered as an effective way to regulate financial markets and protect investors.

The punishment of market manipulation has become one of the main objectives of the European Union as the public opinion equate excessive speculation with outright fraud, due to its destabilising effects on stock markets and the triggering role it plays in major financial shocks, such as the LIBOR scandal (*London Interbank Offered Rate*).[3]

With the aim to delve deeper into this subject and analyse the structure and the evolution of the Market manipulation offence in the European Union, as a first step we will retrace the origin and the definition of one of the two market abuse crimes: market manipulation. Then, we will investigate specifically the general history of Market Abuse in the European Union. And finally, we will see the latest transformation of the Market manipulation offence and the issues related to the recent digitalisation of manipulative behaviour.

2. The Market Manipulation's Origin and Definition.

One of the two market abuse crimes is Market Manipulation offence, with Market Manipulation being the oldest form of "market abuse". While Insider Trading, the other Market Abuse crime, is considered a recent phenomenon, having developed only in the twentieth century, Market Manipulation has been present for a long time in every market where prices are determined by supply and demand. Traditionally, there have been many famous cases in history, such as the collapse of the "*South Sea Company*"[4] (which is likely the first "stock market" boom), the illegitimate manipulation of the stock price in the "*Guinness affair*" in 1980, until *Citigroup Global Markets* manipulated the price of individual shares in 2005[5].

It has been observed that there is a long-established tradition of market control and the adoption of specific rules to prevent market abuse, which can perhaps be traced even from the Roman Empire and the institute of "*fair price*".[6]

Market manipulation amounts to an "unwarranted" interference in the operation of ordinary market forces of supply and demand which undermines the "integrity" and efficiency of the market.[7] In general terms, to manipulate the market refers to disseminating information that is false and negative about an issuer in an effort to drive down the price of

[3] About Libor Scandal cf. L. VAUGHAN – G. FINCH, *The long read Libor scandal: the bankers who fixed the world's most important number*, in *www.theguardian.com*, 18 January 2017.
[4] See N. FERGUSON, *The Ascent of Money: A Financial History of the World*, Allen Lane, 2008, ch. 3.
[5] Financial Services Authority Final Notice, *CitiGroup Global Markets Ltd*, 28 June 2008.
[6] Cf. B. M. MITNICK, *The Political Economy of Regulation*, Columbia University Press, 1980, 243.
[7] IOSCO, *Investigating and Prosecuting Market Manipulation*, 2000, 8.

its securities or, alternatively, disseminating false information in order to drive a company's share price higher.[8]

The Market Manipulation offence's *ratio* is to make stock market more efficient thanks to quick and free transmission of information. Indeed, since the birth of stock markets, the need to avoid information asymmetries or behaviours, which cause information distortions and "speculative bubbles", has become particularly important. Already in the 17th century, in the Netherlands, the price of tulip bulbs, after an exponential growth, collapsed so quickly that it led to an actual financial crash.[9]

Market Manipulation, as an offence, presents a preliminary problem of definition. Some of the most important jurisdictions do not define the term "*manipulation*" altogether. The classic definition of market manipulation was given in famous US cases in "*General Foods Corporation v Brannon*" 1948[10], where "manipulation" was defined as "*the creation of an artificial price by planned action*", and in "*Cargil Inc. v. Hardin*" 1971[11], where it was marked as "*an activity, scheme, or artifice that deliberately influences the price of a financial asset, resulting in a price other than the one that would have resulted in the absence of such intervention*".

Subsequently, the United Kingdom defined market manipulation firstly in the Financial Services Authorities (FSA 1986) and later in the Financial Services and Markets Act (FSMA 2000).

In the EU, a general definition of market manipulation was envisaged in 2003 in the Market Abuse Directive (MAD I), following the traditional distinction between "*transaction-based*" and "*information-based*" market manipulation.

It is important to highlight that all attempts to define market manipulation in legislative provisions follow three different approaches, which are reflected in three distinct jurisdictions: the "*effects-based approach*", the "*intent-based approach*" and a combination of these two:

1. The artificial price, or "*effects- based approach*"[12], requires a proof of the creation of artificial prices or of false or misleading impressions. A modified version of this approach is adopted by the EU Market Abuse Directive.

2. The "*intent based approach*" requires the alleged manipulator's intent to induce other market participants to trade. It is an approach adopted by UK Regulation[13].

3. A combination of two, which also requires proof of inducement. This is the approach adopted by US Courts[14].

However, most definitions of price manipulation have as a common, inextricable component the element of "*price artificiality*", which can be defined as the divergence of price from the legitimate forces of supply and demand. The determination of the right price in relation to the artificial price can be very difficult and sometimes even impossible to

---

[8] See B. RIDER – K. ALEXANDER – S. BAZLEY – J. BRYANT, *Market Abuse and Insider Dealing*, Bloomsbury Professional, 2016, 120-121; S. HORAN, *Corporate Crime*, Bloomsbury Professional, 2011, 1099.

[9] C.P. KINDLEBERGER – R.Z. ALIBER, *Manias, Panics and Crashes. A History of Financial Crises*, Palgrave, 2005, 99.

[10] United States Court of Appeal, *General Foods Corporation v Brannon*, 170 F.2d 220 (19 October 1948).

[11] United States Court of Appeal, *Cargil Inc. v. Hardin*, 452 F.2d 1154 (7 December 1971).

[12] Cf. J.D. COX – R.W. HILLMAN- D.C. LANGEVOORT, *Securities Regulation: Cases and Materials*, Wolters Kluwer, 2017, 771.

[13] S. BAZLEY, *Market Abuse Enforcement: Practice and Procedure*, Bloomsbury Professional, 2013, 247-248; K. ANDERSON -A, PROCTER – J. GOODLIFFE, *A practitioner's guide to the law and regulation of market abuse*, Thomson Reuters, 2017.

[14] See E. AVGOULEAS, *The Mechanics and Regulation of Market Abuse*, Oxford University Press, 2005, 107.

establish. But ultimately, it is irrelevant whether the artificial price was created through the dissemination of false information, the conduct of artificial transactions, or through trades structures to achieve this result. What matters is the effect of those devices on market prices and the harm they inflict on the market's information efficiency.

3. The History of Market Abuse Regulation in Europe.

The regulation of Market Abuse has a long history in the European Union[15]. Abuse in the financial markets has been historically regulated through a combination of criminal law, applied to all users of the financial markets, and the regulation of market professionals.

The first Market Abuse regulation in the European Union was implemented in 1979 with the "*Stock Exchange Listing Directive*" (79/279/EEC), which introduced the obligation to disclose in relation to specific and important events. The next step was the "*Insider Dealing Directive*" (1989/592/EEC) of 1989, which however was focused only on the definition and prohibition of Insider Dealing.

The European Union adopted its first Market Abuse Directive in 2003, which built a broad and comprehensive framework for the regulation of market abuse - both Insider Trading and Market Manipulation - modelled partly on the UK Market Abuse regime. However, during the financial crisis of 2008, it was realised that the practical impact of the Directive was rather limited. For this reason, in 2014 the first Directive was replaced by a Regulation (MAR) and a new Directive (MAD II).

The aim of the new Regulation is to establish a more uniform interpretation of the Union framework for market abuse by defining more clearly the rules applicable in each Member State.

More specifically, the Regulation covers the different forms of market manipulation developed by the "*capital market*" discipline: the "*information-based manipulation*", the "*transaction-based manipulation*" and the "*short selling*"[16].

Although the European legislator has regulated the market abuse through a Regulation, many crucial aspects of the new regime are governed by the "*Market Abuse Directive on Criminal Sanctions*" or MAD II (2014/57/EU).

Even if this approach is often considered insufficient because the European Union has only an indirect authority in criminal law[17], the Directive obliges each Member State to align their legislation with European Law and if they do not comply with it, they will be subject to the Infringement Procedure (articles 258 and 259 of TFEU).

Hence, this directive is in addition to the numerous acts of EU law affecting the substantive criminal law of the Member States, by requiring Member States to criminalise certain conduct and to penalise it by effective, proportionate and dissuasive criminal sanctions.

---

[15] For an in-depth historical reconstruction, cf. S. MOCK, *History, Application, Interpretation, and Legal Sources*, in M. VENTORUZZO – S. MOCK, *Market Abuse Regulation. Commentary and Annoteted Guide*, Oxford University Press, 2017, 9.

[16] Cf. N. MOLONEY, *EU Securities and Financial Markets Regulation*, Oxford University Press, 2014, 740; S. MOCK, *The Concept of Market Manipulation*, in M. VENTORUZZO – S. MOCK, *Market Abuse Regulation. Commentary and Annoteted Guide*, Oxford University Press, 2017, 37-38.

[17] A. KLIP, *European Criminal Law. An Integrative Approach*, Intersentia, 2016, 182.

4. The European Market Manipulation Offence's Latest Modification.

In 2014, EU redefined the Market Manipulation offence to limit further criminal liability. The Directive MAD II, under art. 5, par. 1, recommends Member States to take the necessary measures to ensure that market manipulation is referred to as a criminal offence at least in serious cases, and when committed intentionally[18].

According to the MAD II, market manipulation shall comprise the following activities:

(a) Entering into a transaction, placing an order to trade or any other behaviour which:

(i) gives false or misleading signals; or

(ii) secures the price of one or several financial instruments an abnormal or artificial level;

(b) Entering into a transaction, placing an order to trade or any other activity or behaviour which affects the price of one or several financial instruments which employs a form of deception;

(c) Disseminating information through the media which gives false or misleading signals, where the persons who made the dissemination derive for themselves or for another person an advantage or profit from the dissemination of the information in question; or

(d) Transmitting false or misleading information or providing false or misleading inputs or any other behaviour which manipulates the calculation of a benchmark.

Although market manipulation is defined by art. 12 of the Regulation and prohibited by art. 5, par. 1 of the 2014 Directive, a different definition of manipulation as an element of the offence was provided. This difference lies in the fact that, for the objectives of criminal law, a more stringent approach is necessary to respect the general principle of culpability. The seriousness of market manipulation is defined by Recital 12 of the Directive whereby: "*in cases such as those where the impact on the integrity of the market, the actual or potential profit derived or loss avoided, the level of damage caused to the market, the level of alteration of the value of the financial instrument or spot commodity contract, or the amount of funds originally used is high or where the manipulation is committed by a person employed or working in the financial sector or in a supervisory or regulatory authority*".

5. The Recent Digitalisation of the Manipulative Behaviours.

The redefinition of the Market Manipulation offence may, however, also be ineffective in providing a real investor protection due to the recent digitalisation of transmission of false or misleading information.

The digitalisation of the manipulative behaviours takes two different shapes: on the one hand, stock exchange transactions now use automated systems; on the other hand, some investment decisions are made on the internet under the influence of social media.

In the first case, MAR regulated the use of automated trading techniques (Algorithmic Trading and High frequency trading), deeming them not abusive (under

[18] However, Italy has just adopted the EU Regulation. The deadline for transposition of the Directive expired on 3 July 2016 in the belief that Italy's market abuse discipline was already in compliance with the European provisions. Cf. M. GAMBARDELLA, *Condotte economiche e responsabilità penale*, Giappichelli, 2020, 364.

penalty of contravention of Directive 2014/65/EU, the so-called MiFID II)[19] but explicitly including them among the possible ways of market manipulation. These automated trading techniques pose some problems regarding market transparency and efficiency as a 'human' trader is not able to operate investment strategies at the same speed as machines[20].

In relation to the second form of manipulative conduct, today, market manipulation occurs across national borders through a variety of ways, including the use of the internet. Indeed, while the digital revolution has enabled the development of a globalised and interconnected world, it has also led to the emergence of new forms of crime committed by means of digital systems. The recent market operations that have taken place as a result of decisions taken on internet made it indeed very problematic to understand whether they are "normal" market fluctuation or real manipulations.

A number of key issues regarding the stability and security of financial markets have arisen, as the simplification with which it is possible to sell or buy shares and bonds through online portals or apps, and the extraordinary resonance offered by social networking platforms (e.g., Twitter, YouTube, Reddit, etc.) to share one's investment ideas.

An example of that are the GameStop and Elon Musk's tweet cases: in January 2021, the GameStop case broke out, as the video game shop chain recorded strong rises thanks to the coordinated action of small and micro shareholders organised on a digital forum[21]; in November 2021, Tesla shares closed down nearly 5% Monday after CEO Elon Musk asked his Twitter followers if he should sell 10% of his stock in the electric vehicle company[22].

6. Conclusion

In conclusion, Market manipulation is considered as old as capitalism. As mentioned earlier, the most important function of financial markets is efficient allocation of resources. Since this is a fragile mechanism and may easily be disturbed by exogenous and endogenous shocks or distortions, the need for extensive regulations has arisen.

One of the main justifications of financial regulation is that the multitude of externalities and failures have such a large impact on the real economy, that financial sector institutions should be tightly regulated to make them more resilient.

In addition, alongside administrative sanctions - which have shown little dissuasive force - provision of criminal penalty for serious and harmful cases of intentional market manipulation is deemed to be useful to regulate the market and to protect people's savings in an integrated market such the European financial market.

Today, especially when it is possible to manipulate the price of shares digitally at the click of a button and to influence millions of people on social media to buy or to sell a share, it has become more urgent to define a specific crime that can effectively protect investors.

---

[19] Cf. D. BUSCH – G. FERRARINI, *Regulation of the EU financial markets: MiFID II and MiFIR*, Oxford University Press, 2017.

[20] Cf. M. PALMISANO, *L'abuso di mercato nell'era delle nuove tecnologie.* Trading *algoritmico e principio di personalità dell'illecito penale*, in *Dir. pen. cont.*, 2019, 129.

[21] On the subject, L. GOODMAN et al., *Robinhood and GameStop: Essential issues and next steps for regulators and investors*, in *www.centreforfinancialstability.org*, 4 February 2021; B. BRUMBERG, *Investigations Into GameStop Trading and Reddit: Former SEC Enforcement Chief Provides Insights*, in *www.forbes.com*, 9 February 2021. In Italy, see the comment of F. D'ALESSANDRO, *Il caso GameStop: una tempesta perfetta mette in crisi lo statuto della manipolazione del mercato*, in *Dir. pen. e proc.*, 2021, 1234.

[22] M. DELLATTO, *Elon Musk's Twitter Followers Vote for Him To Sell 10% Of Tesla Stock*, in *www.forbes.com*, 7 November 2021.

The relevance of intermediate steps of protracted process as inside information in the light of the new European Regulation of Market Abuse

Dalila Federici Ph.D. [1]

1. Introduction

This paper will describe the definition of inside information as a key concept of the Market Abuse regime. Under European law, it is prohibited dealing (or make selective disclosure) on the basis of non-public, precise information concerning one or more financial instruments which, if made public, would be likely to affect the price of those instruments or the price of related derivative financial instruments. An example of inside information is a merger between two listed companies. It is therefore prohibited for the insiders to buy the shares of the companies taking advantage of the knowledge of the future merger before it is announced to the market.

In the last ten years one of the most relevant issue has been the relevance of intermediate steps of protracted process as inside information. The problem concerns the possibility of dealing on the basis of information concerning a future and uncertain event included in a decision-making process with progressive formation (e.g. the negotiation of a merger). The conclusion of the process (in the merger example) undoubtedly constitutes inside information. On the other hand, it cannot be said that it has always been clear whether the individual intermediate stages (the various stages of negotiation), which are imperative and functional to the achievement of the final event, should also be considered as inside information. The issue is relevant because if the intermediate steps of protracted processes are insider information, its use and selective disclosure is prohibited.

After the 2014 reform, the article 7 of Market Abuse Regulation (MAR - Regulation No. 596 of 2014), differently to the Directive of 2003 (Market Abuse Directive - MAD I), explicitly includes the relevance of intermediate steps of protracted process as inside information.

The question has been raised as to whether the explicit relevance of the intermediate steps of the protracted process leads to a widening of the definition. Or, on the contrary, did the definition of inside information in Directives 2003/6/EC and 2003/124/EC already tacitly include the intermediate step of protracted processes?

[1] Ph.D. in Criminal Law, Law Faculty, La Sapienza University (Rome, Italy) – dalila.federici@uniroma1.it

To answer this question it is necessary analyse the definition of insider information under the MAD I with a specific focus on the concept of "precise nature" and its potential impact on the price (known as price sensitivity).

The methodology used for the analysis of the definition is as follows:

- literal interpretation
- doctrinal analysis
- EU jurisprudence analysis and comparative insights from the US jurisprudence.

Specifically for case law, the decision of the Court of Justice in the case *Markus Gelti* v. *Daimler AG*[2] will be taken into account. As far as the comparison with the United States of America is concerned, attention will be drawn to the development of case law on the concept of materiality.

2. The definition of Inside Information in the MAD I Directive and the Directive No. 124 of 2003 and in the Art. 7 MAR

The Directive 2003/6/EC (MAD I) of the European Parliament and the Council completed and updated the Union's legal framework to protect market integrity. It's known that an integrated, efficient and transparent financial market requires market integrity. The Commission Communication of May of 1999 identified a series of action that was needed to complete the single market for financial services. The Lisbon European Council of April 2000 called for the implementation of the action plan by 2005. The Council seat up a Committee of Wise Men on the Regulation of European Securities Market and the Committee proposed the introduction of new legislative techniques based on four-level approach: framework principles, implementing measurers, cooperation and enforcement.

At the first level, we found the MAD I that required to all states to create an offence for Market Abuse. Specifically, the Directive required to prohibited trading on the basis of inside information[3] and also, at the art. 6, provides that all Member States shall ensure that issuers of financial instrument inform the public as soon as possible of inside information which directly concerns the said issuers.

We found the definition of inside information at paragraph 16 and art. 1 of the MAD I in the Directive No. 124 of 2003, that implemented the first one as regards the definition and public disclosure of insider information.

Inside information, according to MAD I, is any information:

1) of a precise nature;
2) which has not been made public;
3) relating, directly or indirectly, to one or more issuers if financial instruments or to one or more financial instruments;
4) could have a significant effect on the evolution and forming of the prices of a regulated market.

The implementing Directive at the art. 1 specified that an information:

[2] Court of Justice, 28 June 2012, C-19/11, *Markus Gelti c. Daimler AG*; See for a paper on the sentence LOMBARDO, *Acquisto di partecipazione di controllo, fattispecie a formazione progressiva, informazione privilegiata e* insider *secondario*, in *Le Società*, 2016, p. 706 and following.

[3] See RIDER – ALEXANDER - BAZLEY - BRYANT, *Market Abuse and Insider Dealing*, Bloomsbury, Third Edition, 2016, 87

1) has precise nature if it indicates a set of circumstances which exists or may be reasonably expected to come into existence or an event which has occurred or may reasonably expected to do;

2) is sufficient specific to enable a conclusion to be drawn as to the possible effect if that set of circumstances or event on the prices of financial instruments or related derivatives.

An information can have effect on the prices, on the basis on the art. 1, paragraph 2 of the Directive No. 124 del 2003, if a reasonable investor would be likely to use as part of basis of his investment decisions. In particular, reasonable investors base their investment decision on *ex ante* available information. Therefore, we need to take into consideration the impact of the information in the light of the totality of the related issuer's activity, the reliability of the source and the any other market variability.

This was the legal framework on the definition of inside information until the 2014. As can we see in the text of the both Directives, there is no mention to the relevance of the intermediate steps of protracted process as inside information.

Six years after the entry into force of the legislation in the EU, a group of experts in charge of financial supervision in Europe (the "Lerosièr" group, named after its Chairman), in 2009, noted the need for a new system of enforcement aimed at creating uniform rules and establishing certainty in all member countries. However, market and technological developments since the entry into force of the Directive of 2003 have resulted in considerable changes to the financial landscape. So, in the 2014 the market abuse regime has been reformed in order to make the repression of illegal phenomena more effective and homogeneous throughout the Union.

The European Union adopted Regulation No. 596 of 2014 (MAR), concerning the amendment of the administrative discipline of market abuse and Directive 2014/57/EU (Market Abuse Directive - MAD II) concerning the reform of criminal offences. These repealed the previous directives (No. 6 and No. 124 of 2003).

The new definition of inside information is contained in Article 7 of MAR, which distinguishes four distinct sub-sets of inside information: the first one (Article 7(1)(a) of MAR) concerns financial instruments, the second one (Article 7(1)(b) of MAR) commodity derivatives, and the third one (Article 7(1)(c) of MAR) emission allowances or auctioned products based on them; finally, Article 7(1)(d) of MAR clarifies the scope of inside information for persons charged with the execution of orders concerning financial instruments.

All inside information has to have the same characteristics as those of the previous provision of the MAD I: precise nature, non-public, likely, if it were made public, to have a significant effect on the relevant prices of financial instruments, derivative financial instruments, related spot commodity contracts, or auctioned products based on emission allowances. As regards the likelihood to have a significant effect on the above prices, it concerns information a reasonable investor would be likely to use as part of the basis of his or her investment decisions.

Art. 7, paragraph 2, MAR specifies that also the intermediate steps (e.g. negotiation on a merger) of a process which are connected with bringing about or resulting in future circumstances or future event (e.g. the merger) may be deemed to be precise information.

The aim of the new definition was to cover all possible information that could influence investors' decisions because it's known that in the markets the value of the goods is determined by the meeting between supply and demand and these are influenced by the knowledge operators. It follows that it is necessary that the relevant notice are accessible to

all in the same time and in the same way, and also it is necessary the existence of a prohibition to trade on the basis of it, before it become public. At the same time, in order to protect market integrity, and to prevent any information asymmetry there should be no false news.[4]

For that reason the question of the relevance of steps of protracted process as insider information before the 2014, and if a person can legally trade on its basis, was in the last ten years a very important topic. We can find the resolution first of all in the law case of EU Court of Justice *Markus Gelti v. Daimler*.

3. The difference between the new definition of Inside Information and the old one in the light of the Jurisprudence of the EU Court of Justice

The market and technological developments since the entry into force of the MAD I have changed and the Directive was replaced by the Directive 2014/57/EU (MAD II) and the Regulation 596/2014 (MAR). It's known that the new financial and technical developments enhance the incentives, means and opportunities for market abuse: through new products, new technologies, internet.

As we have seen, now at the Article 7, paragraph 2, of MAR the definition of inside information explicitly mentions the relevance of the intermediate steps of protracted process but, since the 2012, after a sentence of the EU Court of Justice, we know that is prohibited to dealing - also there is a duty to disclosure - on the basis of information that is a steps if it is precise.

It is well known that European law must be interpreted in the light of the rulings of the Court of Justice, therefore this ruling supplements the content of the directive.[5] For this reason it is necessary not only to analyse the text of the legislation but also the relevant case law.

The leading case is *Markus Gelti v. Daimler* , of 2012, concerning a reference for a preliminary ruling from Germany, on the interpretation of MAD I and Directive No. 124 of 2003. As regards the *Daimler* judgment, although this relates to duty to disclose, it is also of particular interest for the definition of inside information constituting the offence of insider dealing. The definition of inside information is not only relevant to the offence but also to duty to disclose price-sensitive information to the public. Although the definitions do not exactly coincide, there is a close link between them, and this is evident. There can be no doubt as to the lawfulness of the use of the information once it has been made public in accordance with the rules and forms of MAD I (and now art. 17 of MAR) and of the Consolidated Law on Finance. In order to ensure greater protection for the markets and to eliminate the risk of information asymmetry, however, the use of a wider range of information than that on which there is an obligation to disclose is prohibited. The reason for this is easy to understand: firstly, the issuer cannot be obliged to disclose information which does not fall within its sphere of control (e.g. knowledge of market information); secondly, the disclosure obligation must be balanced against the need for confidentiality. On closer inspection, the notion of inside information relevant to the prohibition of trading and the duty of disclosure cannot coincide, because to do so would oblige the issuer to make a premature disclosure which could even create inefficiencies in the market.

[4] Cf. SEMINARA, *Diritto penale commerciale*, *Volume III*, *Il diritto penale del mercato mobiliare*, Giappichelli, 2018, 53
[5] *Ex multis*, Court of Justice, C- 215/19, *Pacific World e FFD International*

The information which may not be abused consists, therefore, of all the information which the issuer is obliged to disclose, plus another series of data. This refers, for example, to so-called market information, i.e. information that indirectly concerns the entity, such as knowledge in advance of the market of the approval of favourable tax legislation.

Therefore, the case law on the subject of the obligation to disclose is in any case suitable to serve as an interpretative parameter for the concept of privileged information relevant to the offence of insider trading. In fact, since the information which is subject to the duty of disclosure is narrower than that which cannot be used, it follows that everything subject to the duty of disclosure is necessarily subject to the prohibition of abuse.

The EU Court had to assess whether an intermediate step in a protracted process possesses all the constituent elements of inside information, and in particular the requirement of accuracy (since it can undoubtedly meet all the other requirements, i.e. non-disclosure, reference to financial instruments and price sensitivity). According to the Court of Justice, information can be said to be precise when it meets two cumulative requirements: a) the information must refer to a set of circumstances - or an event - which exists or may reasonably be expected to occur; b) the information must be sufficiently specific to allow conclusions to be drawn on the possible effect of that set of circumstances or event on the price of financial instruments or related derivatives.

The Court ruled that there is a duty to disclose - and consequently a prohibition of dealing – of the information which is precise and is ability significantly to affect market prices and no relief has its chronological location in a process rise to an event. In the Court's view, the fact that the concept of circumstances or events may also include an intermediate stage is supported by Article 3(1) of Directive 2003/124, which mentions, among the examples of inside information whose disclosure may be delayed (in the cases provided for in Article 6(2) of MAD I), certain cases which are clearly attributable to an intermediate stage, such as ongoing negotiations.

Moreover, the Committee of European Securities Regulators, stated in 2007 in its Guidelines that "if the information concerns a process which occurs in stages, each stages of the process as well as the overall process could be information of a precise nature" and "it not necessary for a piece of information to be comprehensive to be considerate precise".

We have established that an inside information, can be also a step of protracted process, if it is an information that is precise.[6] So, for example, the director of a listed company is prohibited from dealing on the basis of knowledge of agreements on a future merger of his company with another one

The other question to be resolved is if the expression "reasonably expected" requires that the probability be assessed as preponderant or significant. And if it depends on the extent of the consequences for the issuer and, where their effects are significant, if it is sufficient that the occurrence of the future event, although uncertain, be not improbable.

Firstly, we must note that there is a divergence between the Member States in the translation of Directive No. 124 of 2003. In particular, each State uses the adverb "reasonably"[7] instead the German version uses the expression "with sufficient probability".[8] However, such linguistic divergence cannot be taken into account for the purposes of interpreting Union rules. They must be interpreted uniformly and in the light

[6] Cf. CONSULICH – MUCCIARELLI, *Informazione e tutela penale dei mercati finanziari nello specchio della normativa eurounitaria sugli abusi di mercato*, in *Le Società*, 2016, 187.

[7] The Italian transaltion uses "ragionevolmente", the French "raissonablement", the Spanish "razonablemente"

[8] mit hinreichender Wahrscheinlichkeit.

of the general economy and the purpose of the legislation of which they form part.[9] As exception of the German version, the legislators of the Member States of the Union have mainly used the term "reasonably" which would indicate a criterion formed on rules derived from common experience. However, it should not be interpreted as requiring evidence of a high probability of circumstances or events.[10] The Court ruled that the expression "reasonable expected" not require that the probability of the event occurring be assessed as preponderant or significant.

The expression "reasonably expected", according to the Court, is a separated condition from the price sensitivity of the article 1 of the Directive No. 124 of 2003. That is the possibility, by dint of the fact that information is specific, to draw conclusion as to the effect of circumstance on the price of the financial instrument.

In fact, there is no reason to believe that a greater magnitude leads to a greater probability of the event occurring. The two criteria (precise nature and price sensitivity) are two minimum requirements, both of which must be met in order for the information to qualify as privileged. The balance between the likelihood of occurrence and the possible impact on prices is, in the view of the Luxembourg Courts, intended to determine whether the information is likely to have a significant impact on prices and, therefore, whether a model investor would take it into account. This statement seems to be in line with US case law, where the probability magnitude test is used in the case of highly speculative events to assess whether the information is material, i.e. whether it is information that a reasonable investor would use as one of the data on which to base his investment decisions.

This test was ruled by the Second Circuit of US Court in *Sec. v. Sulphur*[11] and then in *Basic Inc. v. Levinson.*[12] The second one was a case of a person omitted to disclose an information about preliminary merger discussions. In this occasion, the Court provided that to know if this information is material, a balance must be struck between two factors:

- the probability of the event occurring;
- the impact it would have in the light of the company's total activities.[13]

4. Materiality

The concept of materiality has its matrix in US law. It was used as an element of the Securities Fraud – that can be assimilated to the market abuse offence - in the Securities Act 1933 and the Securities Exchange Act 1934, legislation initiated after the collapse of the Wall Street Stock Exchange. It is an element that the Prosecutor must prove in the judgment.

We have not found any definition of materiality in the text. To outline the definition we need to analyse the decisions of the US Court. The leading cases are *TSC Industries v Northway Inc*[14] e *Basic Inc v. Levinson*[15]. The first one has as object a case rule by the proxy

[9] *Ex multis*, Court of Justice, C- 215/19, *Pacific World e FFD International*
[10] Court of Justice, 28 June 2012, C-19/11, *Markus Gelti c. Daimler AG*, § 46.
[11] 410 F.2d 833 (2d Circ. 1968)
[12] 485 U.S. 224 (1998)
[13] STRADER – JORDAN, *White collar crime, case, materials and problems*, Lexis Nexis, III ed. 2015, 248
[14] 426 U.S. 438 (1976)
[15] 485 U.S. 224 (1988)

rule, in particular, rules on the acquisition of powers in general meetings. In this case the company failed to disseminate certain information.[16]

In accordance with the US Court, the concept of *materiality* is objective and its definition depends on the related subject: the reasonable investor. Indeed, the information will be relevant according to its ability to influence the judgment and choices of reasonable investors. In this case the concealed information is material because the reasonable investor would be likely to use the moment of the vote in the assembly; it is no necessary if the investor really would have voted differently.[17]

As mentioned in the previous paragraph, the US Court in *TSC Industries v. Northway Inc* created the *TSC test:* an information is material if its relevance would be able to influence total mix information available to the investor.[18]

Basic Inc v. Levinson has as object a case of false information to the market about a possible merger: an uncertain event. In this case the Court, first of all rejected the fraud-on-the market theory, according to which the information is relevant because it is false. This theory does not have the advantage of keeping all the facts adequately separate. The misleading or false is a separated element which cannot be indicative of relevance.

For the US Court, it is correct to use the test utilized by the Second Circuit in *Sec v. Sulphur co.*[19]*:* the probability-magnitude test. As seen, in the paragraph 3, the Court provides that to know if this information is material, a balance must be struck between two factors:

- the probability of the event occurring;
- the impact it would have in the light of the company's total activities.[20]

5. Conclusion.

It can be concluded that, according to the EU Court of Justice, a step of protracted process can be an inside information since the first Market Abuse Directive in 2003 if they have all the condition of an inside information: the precision and if it is price sensitive. It has precise nature also if not is preponderant or significant if it may come in existence and it is price sensitive if, according to probably magnitude test, it is enable to drawn as to the possible effect on the prices of the financial instrument. In other word, since from the MAD I is not allowed to deal or recommending to deal on the step of protracted process if it is material for a reasonable investor. For example is prohibited from dealing on the basis of knowledge of on-going arrangements of a possible merger.

In conclusion, the new definition looks almost identical to the previous one. Indeed, the explicit addition of the relevance of intermediate steps as privileged information does not broaden the definition because it has included in the definition the case law of the European Court of Justice *Markus Gelti v. Daimler.*

The differences are as follows: a) with reference to the inside information in relation to commodity derivatives, MAR refers to information concerning directly or indirectly one or more commodity derivatives or the related spot commodity contract. In addition, with the previous text under MAD, MAR provides that the inside information has to be

[16] STRADER- JORDAN, *White collar crime, cases, materials, and problems*, LexisNexis, III ed 2015, p. 243 and following; WANG-STEINBERG, *Insider Trading*, Oxford, Third ed., 2010, p. 107 ss.
[17] STRADER - JORDAN, *White collar crime, cases, materials, and problems*, cit., p. 244.
[18] STRADER, *Understanding White Collar Crime*, cit., §5.09.
[19] 401 F.2d 833 (2d Circ. 1968).
[20] STRADER – JORDAN, *White collar crime, case, materials and problems*, cit., 248

reasonably expected to be disclosed or required to be disclosed in accordance with legal or regulatory provisions at the Union or national level, market rules, contract, practice or custom, on the relevant commodity derivatives markets or spot markets; b) Article 7(1)(c) of MAR extended the definition of inside information contained in MAD to include information concerning emission allowances and auctioned products based on them, provided that such information abides by the abovementioned confidentiality and preciseness requirements, together with the likelihood to have a significant effect on the prices of the instruments or of related derivative financial instruments; c) finally, Article 7(1)(d) provides that "for persons charged with the execution of orders concerning financial instruments", inside information "also means information conveyed by a client and relating to the client's pending orders in financial instruments, which is of a precise nature, relating, directly or indirectly, to one or more issuers or to one or more financial instruments, and which, if it were made public, would be likely to have a significant effect on the prices of those financial instruments, the price of related spot commodity contracts, or on the price of related derivative financial instruments."[21]

According to the MAR Review Report of September 2020 of ESMA (European Securities and Market Authority) the new definition of inside information is working properly and is therefore sufficient to combat market abuse, since it is sufficiently broad to allow for flexibility in capturing market abuse behaviours. Thus, the current definition of Article 7 is adequate to combat market abuse.

Despite ESMA's positive feedback, the "Digital era" brings new problems to the surface. For example, as far as the reasonable investor is concerned, the development of financial markets and businesses has also led to the need to use computer systems. It should not be overlooked that investment decisions are now based on algorithms so as to undermine even the model of the reasonable investor as a flesh-and-blood person so much so that even the supervisory authorities are calling for the use of artificial intelligence.[22] After 2014, the European legislator has indeed taken care to regulate the use of algorithmic trading in the MAR, considering it not abusive (under penalty of contrast with Directive 2014/65/EU, the so-called Markets in Financial Instruments Directive - MiFID II) but explicitly including it among the possible methods of market manipulation. These techniques of automated trading (which are algorithmic trading and high frequency trading) pose certain problems with regard to the transparency and efficiency of the market because a 'human' operator is not able to operate investment strategies at the same speed as machines. Indeed, through such systems, orders are placed (or withdrawn from the market) in a matter of seconds, opening up the market to new risks, not only in the event of abuse, but precisely because of the use of technology. This mode of investment has posed the crucial problem of access to price-sensitive information. Indeed, those who use automated procedures undeniably enjoy an advantageous position over those who do not. For this reason, the doctrine has wondered whether there should be a limitation on the use of high frequency trading or a restriction on access to certain information. It has been pointed out

[21] The latter case identifies the relevant meaning of financial information for the market abuse practice known as "front running", consisting of one party, mainly a broker or a person charged of executing orders, that, being aware of a forthcoming order or transaction on a financial instrument, uses such information by acquiring or disposing of relevant financial instruments ahead of the relevant order or transaction

[22] ABRIANI – SCHNEIDER, *Il diritto societario incontra il diritto dell'informazione. IT,* Corporate governance e Corporate Social Responsability, *Riv. delle Società*, 2020, p. 1326 e following.

that such a limitation would not be in line with the principles of fair access to information and market transparency.[23]

In conclusion, we will have to wait a few years to assess whether the new definition of inside information and the test used to ascertain if it is price sensitive are appropriate with respect to new technologies.

[23] For a deepening on the subject, see ANNUNZIATA, I processi di mercato automatizzati e il trading algoritmico, in Cian - Sandei (edited by), Diritto del Fintech, Wolters Kluwer Cedam, 2020, p. 406 and following.

Legal & regulatory effects of FinTech's in digitalizing financial markets – A European and US perspective

Klaus Xhaxhiu Ll.M.[1] – Zaim Lakti Ll.M.[2]

1. Introduction

The term 'FinTech' originates since the early 1990s, where it would refer to a project called 'Financial Services Technology Consortium'. However, since 2014, regulators, consumers and market participants have increased their focus of attention for this sector. The rapid growth of FinTech's caused a much higher regulatory scrutiny, which could be justified by the significant role they play in the financial sector. Saying that, FinTech's are startup companies in a highly regulated financial sector relying on their early-stage financing to the venture capitals or institutional investors.

On this research paper we analyze the regulatory effects of FinTech's in digitalizing the European Union (EU) and the United States (US) financial markets. We compare their legal approaches and present our conclusions while presenting the future challenges in the last section.

First, taking into consideration the idea of creating a European Banking Union, Article 127(6) TFEU, allows the European Central Bank (ECB) to be entrusted with specific tasks concerning policies relating to the prudential supervision of credit institutions and other financial institutions especially FinTech's. The latter has gained in importance, although it requires unanimity in the Council. Moreover, the European strategy for FinTech's is part of the "Digital Agenda for Europe," which the European Commission has outlined as one of the seven flagship initiatives. In March 2017, the Commission presented its action plan on consumer financial services. These addresses, inter alia, the opportunities offered by FinTech's, but focuses on the specific issues of electronic identification and distance selling. All great initiatives but compared to other non-EU markets, still not in the edge of being entrepreneurial friendly.

[1] Senior Associate – Compliance / AML, Vistra (Germany) GmbH, Frankfurt DE, klaus_xhaxhiu@hotmail.com
[2] Acquisition & Procurement Associate, QFS Corporation, New York USA, zlakti@fordham.edu

Second, under existing US law, the traditional Bank Charter permits firms to take depositors and make loans and depository institutions have exclusively right to take insured deposits. FinTech firm started to get into the bank charter territory and disrupted traditional financial industry same way as Uber did to taxis, or Airbnb to hotels. New payment firm such as PayPal led the way to sell loans to individual retail investors via old payments systems. However, new payments methods like cryptocurrency provided alternative payment channels. This led to new legal challenges because it fully excluded banks as intermediaries and the government had no control over the transaction. The US approach has been slightly different from the one in the EU. Office of the Controller of the Currency (OCC) has proposed new special purpose national bank charter for FinTech firms. This charter will bring FinTech marketplace lender and online payment providers within the regulatory perimeter and granting them federal preemption. There are still many legal and financial challenges to be addressed in the digital markets for the EU and the US, especially taking into consideration also the huge challenge of Cryptocurrencies.

2. The European perspective

a. FinTech in Europe

The term 'FinTech' originates from the early 1990s, where it would refer to a project called 'Financial Services Technology Consortium', started by Citigroup to boost technological cooperation effort[3]. However, since 2014 many regulators and consumers including market participants have increased their focus of attention for this part of the financial industry[4]. In general, this term describes companies that offer innovative, technology-based application systems related to the topic of "finance". Although these are often so-called "start-ups", this is not a mandatory requirement; already established companies which also use innovative technologies can fall under the term "FinTech" as well[5].

The growth of FinTech brough greater regulatory difficulties, which could be justified by the important role in the financial industry. As FinTech's are generally startup companies in the financial sector, which by the way is a highly regulated sector worldwide, they rely on their early-stage financing to the venture capitals or institutional investors.

More than 340 active financial technology companies had established themselves in Germany by 2016 and within Europe, the German FinTech market ranks second after the UK. In a global comparison, Germany has also increasingly caught up in the past years[6].

[3] Arner, Barberis, & Buckley, The Evolution of Fintech: A new Post-Crisis Paradigm? 2015
[4] Ibid.
[5] Germam central bank: https://www.bundesbank.de/de/aufgaben/bankenaufsicht/einzelaspekte/fintechs/fintech-598228.
[6] Gregor Dorfleitner, Lars Hornuf: FinTechMarkt in Deutschland. (PDF) Bundesministerium der Finanzen (BMF), 17. Oktober 2016, abgerufen am 26. Juni 2017.

When bringing innovation to the market, profit falls on a second line and by that the initial public offering (IPO) phase plays a significant role to the lifecycle forecast of them. The latter, starting in the context of the creation of the European Banking Union[7], while mentioning Article 127(6) TFEU, which allows the ECB to be entrusted with specific tasks concerning policies relating to the prudential supervision of credit institutions and other financial institutions especially FinTech[8]. This has gained in importance, although it requires unanimity in the Council.

b. The European FinTech approach

The European strategy for FinTechs is part of the "Digital Agenda for Europe", which the European Commission has outlined as one of the seven flagship initiatives[9]. In March 2017, the Commission also presented its action plan on consumer financial services. This address, inter alia, the opportunities offered by FinTechs, but focuses on the specific issues of electronic identification and distance selling[10]. In the course of the adoption of the EU 2020 strategy and with the decision on the Digital Agenda, the Commission wants to use the economic potential of the EU member states for the creation of a common digital market and common infrastructure and establish it step by step. The unification of European standards is intended to enable a strengthening of the EU's digital economy[11]. This should support European domestic foreign trade by standardizing the digital exchange of goods. A common European foundation is to form the basis for further EU legislation and legal frameworks. Creating such systems and frameworks brings strengthening of the European economy against the influence of large international Internet corporations and keeping control of them. Transparency and net neutrality must ensure that strong market positions are not abused.

According to the European Commission, the Digital Agenda includes the following measures:

1. Implementation of the Digital Single Market.
2. Opening access to legal online content (eGovernment Action Plan).
3. Simplify electronic payments and invoicing (complete the single euro payments area (SEPA) and review eSignature Directive).
4. Ensure user confidence in payment security.
5. Standardize telecommunications services.
6. Improve interoperability and standardization.
7. Strengthen trust and online security: fight cybercrime and online child pornography, protect privacy and personal data.
8. Promote high-speed and ultra-high-speed Internet access.

[7] SSM Regulation (EU) 1024/2013

[8] Dieter Krimphove, Thomas Müller; FinTechs – Rechtliche Grundlagen moderner Technologien, Europarechtliche Aspekte von FinTechs, 86.

[9] Digital-Agenda – So will Europa digital den Anschluss behalten. Süddeutsche Zeitung. 5. Mai 2015. Überblick von Varinia Bernau. Abgerufen am 3. Dezember 2015.

[10] European Commission – Digital Agenda for Europe, official Website.

[11] Digital-Agenda – So will Europa digital den Anschluss behalten. Süddeutsche Zeitung. 5. Mai 2015. Überblick von Varinia Bernau. Abgerufen am 3. Dezember 2015.

9. Investing in research and innovation
10. Improving digital skills, qualifications and inclusion.[12]

c. FinTechs is a highly regulated sector in Europe

FinTechs as part of a highly regulated sector (banking & payments – where regulators and legal frameworks are putting pressure) have not reached to a structuring & trust level of the established companies with many years of expertise in their field. Prior to IPO, a company typically builds up 'trust' from the investment community over time by meeting its prospectus forecast. The latter is not the case for the new FinTechs, which can also be without any positive balance sheets but still go for an IPO, trusting only to their innovation and new business model[13]. At the end of the day, the future requires innovation.

In the US from the other side, the OCC has brought up a FinTech charter proposal which would allow FinTechs to preempt money transmitter regulations[14]. This would grant a crucial bypass and remove many time-consuming state licensing requirements. By doing that, FinTechs would focus on what they do best, bring innovation, and even though the normal anti money laundering and consumer protection laws would apply, the ecosystem is still more favorable then in Europe[15]. So maybe the EU has a few things to learn from the US ecosystem.

3. The US perspective

a) The United States transition from traditional banking to digitalized banking

The United States has been a country with tremendous number of banks mostly because of its economic expansion and limits on intra-state branching within the country. In 1920, there were 30,000 banks, many of them small banks. During the Great Depression until 1970 this number decreased to 13,000, and only to go down to 5,900 by 2017[16]. This does not mean the number of financial transactions declined. How this transition happened then?

First, national banks have many legal advantages over state banks which led to a shift of banking business toward national banks. One important advantage is the Controller, the Federal Reserve Board, and the Federal Deposit Insurance Corporation (FDIC), because of the dual banking system and the federal preemption, can convince Congress to enact a law that is binding for state banks too[17]. This played out in court. In *Marquette National Bank of Minneapolis v. First of Omaha Service Corp.* 439 U.S 299, 313-19

[12] Digital Agenda for Europe. Mitteilung der Kommission vom 19. Mai 2010 an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Eine Digitale Agenda für Europa". KOM(2010) 245 endgültig; nicht im Amtsblatt veröffentlicht (deutsche Fassung, auf EUR-Lex).
[13] Möslein/Omlor, FinTech-Handbuch, 2019, 601-643
[14] Barr/Jackson/Tahyar, Financial Regulation: Law and policy, second edition, 186.
[15] Ibid.
[16] Tim Sablik, *Fed. Reserve Bank of Richmond, Who Wants to start a Bank?* (2016).
[17] Michael S. Barr, Howell E. Jackson, Margaret E. Tahyar, *Financial Regulation: Law and Policy, pg. 160* (2018).

(1978) the court permitted national banks to export the interest rate from one state to another. This court decision helped national banks to gain advantages against state banks.

Second, new social and technological needs arised in the 21st century. Under existing US law, the traditional Bank Charter permits firms to take depositors and make loans and depository institutions have exclusively right to take insured deposits. However, many goods like marijuana are legal in many states while remain illegal on federal level, therefore they remain out of the financial system[18]. This brought legal challenges because of the Supremacy Clauses[19]. Despite legalization in these states, state banks still cannot use their financial system to transfer funds, take insured deposits of this kind. Some states, such as Colorado, reacted to this by creating a new type of bank charter, a state level cooperative, which does not require federal deposit insurance but would require access to the Federal Reserve System's payment systems.[20] This was still not enough. The market demand and the need of federal institutions to oversee financial activities led that the Office of the Comptroller of the Currency (OCC) to consider whether it is in the public interest to entertain applications for a special purpose national bank charter from financial technology (Fintech) companies that engage in banking activities and meet the standards applicable to national banks[21].

b) How FinTech further digitalized the United States financial markets

FinTech firm started to get into the bank charter territory long before the OCC proposed a new special bank charter. It disrupted traditional financial industry same way as Uber did to taxis, or Airbnb to hotels. FinTech start-ups have taken a variety of forms, from firms seeking to reach scale, to those seeking to provide services to incumbents, or to be bought by them and incorporated into larger firms. Some of these can be seen as dis-intermediating the financial sector- seeking to break it part into tis components parts and peeling some of these components away from banks, insurance companies, or broker dealers[22].

New digital approaches include new online marketplace or peer-to-peer lenders[23], payment transmitters[24], and data aggregators. Online lenders use computer algorithms to analyze the creditworthiness of borrowers, often issuing loan decision within a few

[18] 21 U.S.C. §§ 841(a)(1), 802(6), 812(c); 18 U.S.C §2.
[19] Article VI, Paragraph 2 of the U.S. Constitution is commonly referred to as the Supremacy Clause. It establishes that the federal constitution, and federal law generally, take precedence over state laws, and even state constitutions.
[20] Col. Rev. Stat. Ann. § 11-33.
[21] The Office of the Comptroller of the Currency (OCC), *OCC Summary of Comments and Explanatory Statement: Special Purpose National Bank Charters for Financial Technology Companies.* 2017.
[22] Michael S. Barr, Howell E. Jackson, Margaret E. Tahyar, *Financial Regulation: Law and Policy*, *pg. 185* (2018).
[23] It is a practice of lending money to individuals or businesses through online services that match lenders with borrowers. This enables an individual to obtain a loan directly from another individual, cutting out the traditional bank as the middleman. A solid example of this is SoFI, www.sofi.com.
[24] The definition of money transmitter is at 31 CFR 103.11 (uu) (5) and it includes any person, whether or not licensed or required to be licensed, engaged as a business in the transfer of funds.

hours. For instance, investment brokerages use this technology when they give margins[25] to their customers. Then, these loans are funded by selling interest in the loan to investors, including both individual retail investors and institution ones. There are two main innovation that helped FinTech digitalize old financial markets.

First, new payment firm such as PayPal or Venmo using computer algorithms led the way to sell loans to individual retail investors via old payments systems set up by the credit card networks and the banks. However, the absence of a bank charter means that online lender and payments providers cannot take deposits from the public and they cannot avail themselves of the preemption powers. In *Madden v. Midland Funding, LLC,* 783 F.3d 246 (2nd 2015) court held that federal preemption did not apply after the national bank sold or otherwise assigned the loan to another party. This means, the state laws apply, and they would need to partner with a local state bank to grant and fund the actual loan. How this process usually works is that the bank holds the loan for few days, usually three days, then sells it to the online lender or a third party. The bank retains a portion of the loan. This new business model was called into question from many federal courts' decisions because it is perceived from the state supreme courts that this is in violation of state licensing and usuary laws[26]. The Supreme Court has declined to hear any of the cases and let to significant to uncertainty in the online lending industry.

However, OCC and FDIC recently issued rules codifying the above long-held interpretation of federal law that non-usurious loans originated by a bank and then transferred to a non-bank entity are not subsequently usurious under state law. Also, they backed the possibility of a new payments charter to preempt all state money transmission licensing requirements, and let firms obtain one charter, rather than many licenses for each state.[27]

Furthermore, the raise of new innovative payments methods like cryptocurrency (Bitcoin, Ripple, etc) which provide independently alternative payment channels. This led to new legal problems because it fully excluded banks as intermediaries and government had no control over the transactions. How far blockchain and cryptocurrency will go to disrupt the whole financial systems is still unclear even though some banks have adapted this technology. The critical issue here is whether these digital currencies will be seen as a new asset class or a new form of money. The Uniform Commercial Code (UCC) board has created a commission to draft the regulations on cryptocurrencies transactions because under the current rules it is categorized as a "general intangible"[28]. Alto, it remains to watch how OCC and FDIC will regulate it.

c) The United States proposed regulation

[25] Margin investing is a form of loaning. The broker lends you money against your investment you held in the broker's account.

[26] *CashCall, Inc. v. Comm'r of Fin. Regulations*, 139 A.3d 990 (Md. 2016); *Commonwealth of Pennsylvania v. Think Fin., Inc.* E.D. Pa. Jan. 14 2016).

[27] Pratin Vallabhaneni, Glen Cuccinello, Max Bonici, *INSIGHT: Regulators' Preemption Scuffle Offers Opportunities for Financial Services*, *Aug 4 2020 at https://news.bloomberglaw.com/us-law-week/insight-regulators-preemption-scuffle-offers-opportunities-for-financial-services.*

[28] The Uniform Commercial Code (UCC), § 9-102 (42).

The US approach has been slightly different from European Union (EU). Office of the Comptroller of the Currency (OCC) has proposed new special purpose national bank charter for FinTech firms which will bring FinTech marketplace lender and online payment providers within the regulatory perimeter and granting them federal preemption[29] in exchange for accepting the regulation and supervision that inheres in the national bank charter.

The proposal would allow firms to apply for one of the three coring banking activities: receiving deposits, paying checks, or lending money.[30] It also would provide federal preemption to the same extend as a national bank. This will allow FinTech firms to preempt state money transmitter regulations. Federal preemption would grant a crucial bypass of expensive and time-consuming state by state licensing requirement for online payment transfer firm like Venmo, PayPal and cryptocurrencies providers. Community Reinvestment Act, anti-money laundering, and state consumer protection laws would continue to apply. These proposed regulations led to a lawsuit spearheaded by the Conference of State Bank Supervisors (CSBS) and the New York State Department of Financial Services.

On May 14, 2021 Federal Deposit Insurance Corporation (FDIC) issued a request for information on Digital Assets[31]. It is gathering information and soliciting comments from interested parties about insured depository institution' current and potential digital asset activities. FDIC-Regulated Firms. After years of uncertainty, the FDIC recently approved deposit insurance applications for two new industrial loan companies (ILCs): *Nelnet Bank* will originate and service private student loans and other consumer loans, as an internet-only bank. *Square Financial Services* will originate commercial loans to merchants that process card transactions through Square's payments system[32]. The parents of these companies will not become bank holding companies subject to Federal Reserve regulation and supervision[33]. Similar FDIC restrictions, however, will apply by written agreement.

4. Conclusions

There are still many legal and financial challenges to be addressed in EU and US digital financial markets especially on regards to cryptocurrencies and whether FinTech should be under central banking authorities. We anticipate that the global market demand will help European and US regulatory agencies to better understand the challenges and the opportunities that lay ahead. Until now, US approach seems to be

[29] Office of the Comptroller of the Currency (OCC), *Exploring Special Purpose National Bank Charters for Fintech Companies.* 2016

[30] See, C.F.R § 5.20(e) (2017).

[31] See https://www.fdic.gov/news/press-releases/2021/pr21046a.pdf. Last checked on May 29, 2021.

[32] See https://news.bloomberglaw.com/us-law-week/insight-regulators-preemption-scuffle-offers-opportunities-for-financial-services. Last check on May 29, 2021.

[33] The parents of the traditional banks are required by federal law to be organized as holdings entity and subject of Federal Reserve Control.

more pragmatic for two reasons. First, FinTech is an industry that is rapidly expending, and it is more convenient for consumers which adds value to financial systems. Second, digital assets, a trillion dollars market cap, would enter the financial systems and increase its efficiency and its transparency. Also, we anticipate that US with an already established legal infrastructure will capitalize the FinTech revolution by creating its own official digital asset before EU does.

Financial markets based on the technology of distributed registers in Albania

Katrin Treska Ll.M.[1] – Prof. Assoc. Dr. Engjell Likmeta[2]

1. Introduction

The use of virtual currencies has already become not only a well-known practice, but also a world-wide investment tool. Albania in this regard, until 2020, did not have a regulatory framework for virtual currencies, or as they are known in everyday language "Bitcoin". However, the data have shown that the lack of a regulatory framework has not prevented the spread of the use of virtual currency in Albania, or by Albanian citizens. Only in May 2020, the Albanian Parliament was invested in the approval of the regulatory framework - law no. 66/2020 "On financial markets based on distributed ledger technology". The authors in this paper will stop to analyze the regulations made by this new law, its positive expected effects, but especially those provisions that may have left room for interpretation in the implementation of the law in everyday life, and especially in the Albanian context. By analyzing these elements, the authors will stop at a preliminary assessment of the risks of misuse of virtual currencies in money laundering, due to the lack of experience of Albanian institutions in managing and controlling this new tool of transactions.

Distributed ledgers constitute databases spread across multiple sites, countries or institutions, which are typically accessible by anyone. Records of transactions are stored one after the other in a continuous ledger, rather than sorted into event-specific or thematic blocks, but they can only be added once the participants reach a quorum. A ledger is 'un- permissioned', if it has no single owner and the process is open to everyone (as in the case of Bitcoin). The integrity of the ledger is maintained through consensus from the participants about its state[3].

[1] General Director of Legal Services at the Institution of the President of the Republic and part time lecturer at Faculty of Law, University of Tirana.
[2] Full-time lecturer in the Faculty of Law, University of Tirana.
[3] Angelos Delivorias, European Parliamentary Research Service, PE 593.565, November 2016 https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/593565/EPRS_BRI(2016)593565_EN.pdf. Last accessed 4.5.2022

The blockchain is a type of database that takes a number of records and assembles them in a block, which is then 'chained' to the next block using a cryptographic signature. This allows them to be used like a traditional ledger, which can be shared and corroborated by anyone with the appropriate permissions. Until recently, the most widely known application of this technology was in the public ledgers of transactions underpinning virtual currencies, such as Bitcoin. Recently, however, the idea that the use of this and similar methodologies belonging to the wider group of 'distributed ledger technologies' could be extended to traditional financial services, has been gaining ground[4].

DLT is an entirely new way to construct highly secure, highly capable and widely distributed databases. DLT can deliver many potentially transformative applications in the capital markets[5].

The capital markets exist to provide connections between the providers and users of finance. At a minimum, DLT has the potential to make those connections faster, cheaper and more reliable – improvements that will benefit every firm, not to mention investors and issuers[6].

2. Albanian legal framework

In Albania, taking into account the wide spread of DLT and virtual currency, this field was totally not only unexplored, but even unregulated. This doesn`t mean that Albanian citizens were not involved in this kind of transactions. In unregulated markets, there were more and more talks about virtual currencies and investments in them. This meant that any kind of activity in this direction was not only unregulated by law, but also uncontrolled by state institutions.

On 21 may 2020, the Albanian Assembly adopted Law no. 66/2020 "On financial markets based on distributed ledger technology". The object of this law, as the first law trying to regulate DLT, is to regulate the issuance of digital tokens/virtual currencies, licensing, monitoring and supervision of entities carrying out distribution, trading and custody of digital tokens/virtual currencies activities, as well as digital token agents, innovative service providers and automated collective investment undertakings[7].

This law aims to apply to all activities regulated hereby and entities who exercise such activities in the territory of the Republic of Albania or from the Republic of Albania, issues those which till May 2020, remained unregulated by any legal act in Albania.

---

[4] Angelos Delivorias, European Parliamentary Research Service, PE 593.565, November 2016 https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/593565/EPRS_BRI(2016)593565_EN.pdf Last accessed 4.5.2022

[5] Stephen Bayly, Chief Technology Officer, HSBC Securities Services, "Distributed Ledger Technology in the Capital Markets", 12.03.2019, https://www.gbm.hsbc.com/insights/securities-services/distributed-ledger-technology, Last accessed 4.5.2022

[6] Stephen Bayly, Chief Technology Officer, HSBC Securities Services, "Distributed Ledger Technology in the Capital Markets", 12.03.2019, https://www.gbm.hsbc.com/insights/securities-services/distributed-ledger-technology, Last accessed 4.5.2022

[7] Article 1, of Law no. 66/2020 "On financial markets based on distributed ledger technology".

According to the responsible institutions that initiated this law, the use of virtual assets and related financial services are rapidly transforming the picture of financial markets for both market investors and market infrastructure providers (payment systems, stock exchanges, trading venues, securities custodians, issuing companies). This has also caused our country to face specific challenges for both regulators and market participants, and because there is uncertainty about how the existing regulatory framework can be applied to virtual assets. Currently, there are several laws that regulate the financial system in Albania, such as the Law on Securities, the Law on Banks, Payment Systems, etc. All of these laws do not regulate the activity of virtual assets and as a result this activity was currently unregulated[8].

Therefore, in Albania, the law was seen as a need to make the most of the benefits offered by this technology, but also to address a number of potential risks such as the creation of fraudulent schemes or unauthorized schemes to provide virtual assets, the risk of using virtual assets for money laundering, as well as market manipulation, in order to have a complete legal regulation so that this activity is clearly regulated[9].

Therefore, the legislator was convinced of the adoption of this law, aiming at several main objectives such as[10]:

- Make the best use of all the potential of fintech and DLT technology;
- Potential reduction of payment system costs;
- Encouraging financing for the local economy through alternative sources of financing;
- Attracting foreign investors;
- Creating economic benefits for the country.
- Prohibition of the operation of a DLT Exchange, in an unauthorized manner in the territory of the Republic of Albania;
- Prohibition of providing virtual assets with initial offer in an unauthorized manner.

3. What does the new law provide?

Distributed ledger technology has enabled for the first time in history conducting secure economic transactions between two parties at a distance, without the involvement of intermediaries or third parties (banking institutions, VISA, Paypal etc.) as guarantors of reliability. Thanks to the combination of powers of large computer processors with elements of cryptography, these registers contain at all times complete and immutable

[8] Ministry of Finance and Economy, Risk Impact Assessment on the draft law "On financial markets based on distributed ledger technology", 2019-MFE-18, page 1. For more: https://www.parlament.al/ProjektLigje/ProjektLigjeDetails/51359, Last accessed 4.5.2022

[9] Ministry of Finance and Economy, Risk Impact Assessment on the draft law "On financial markets based on distributed ledger technology", 2019-MFE-18, page 2. For more: https://www.parlament.al/ProjektLigje/ProjektLigjeDetails/51359, Last accessed 4.5.2022

[10] Ministry of Finance and Economy, Risk Impact Assessment on the draft law "On financial markets based on distributed ledger technology", 2019-MFE-18, page 2. For more: https://www.parlament.al/ProjektLigje/ProjektLigjeDetails/51359, Last accessed 4.5.2022

information on it data and transaction history of each value integrated in these systems, which is agreed and periodically updated by all of its users. Basically, this technology is a distributed registry, which can be inspected by everyone, but cannot be controlled by anyone, thus enabling reliable economic transactions that are authenticated by mass cooperation of users and generated by self-interest of each of the users and not by any public authority[11].

Taking this in consideration, the government of Albania assessed the need to complete its legal framework in this direction, by approving a new law that regulates financial markets based on distributed ledger technology, by specifying not only the legal requirements to be able to exercise this type of activity, but also establishing the responsible institutions that must strictly monitor and control this activity in Albania.

The new law, in its first Chapter treats General Provisions, mainly introducing the definitions of the terms the law provides, as defining explicitly what "Virtual Currency" means, as one of the virtual assets which is a digital representation of value used as a medium of exchange, means of payment, unit of account, or store of value, which:

(i) is not a Digital Token;
(ii) is not issued or guaranteed by a central bank or a government authority;
(iii) is not necessarily attached to a legally established currency;
(iv) is not FIAT Money and therefore does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange;
(v) has been issued on its own DLT; and
(vi) can be transferred, stored and traded electronically[12].

The **second chapter** of the law, regulates the licenses and competent authorities to give these licenses, in order to be able to carry out the activities as provided under the present law. There are 5 types of licenses:

1. DT Agent License, which shall be granted by the AFSA (*Financial Supervisory Authority*) to a Legal Entity fulfilling the general requirements and specific criteria provided in the law;
2. DLT Exchange License, which shall be granted by both the AFSA and the NAIS (*National Authority on Information Society*) to a Legal Entity fulfilling the general requirements and specific criteria provided in the law;
3. Innovative Service Provider License, which shall be granted by the NAIS to a Legal Entity fulfilling the general requirements and specific criteria provided in the law;
4. Third Party Custody Wallet Provider License, which shall be granted by both the AFSA and the NAIS to a Legal Entity fulfilling the general requirements and specific criteria provided in the law;
5. Automated DT Collective Investment Undertaking License, which shall be granted by the NAIS to legal entities fulfilling the general requirements and specific criteria provided in the law.

The law of course provides articles about the necessary requirements a person should fulfill in order to be licensed, validity and duration of a license, and the

[11] Council of Ministers of the Republic of Albania, Report of the draft law "On financial markets based on distributed ledger technology", page 1. For more: https://www.parlament.al/ProjektLigje/ProjektLigjeDetails/51359. Last accessed 4.5.2022

[12] Article 3, point 80, of Law no. 66/2020 "On financial markets based on distributed ledger technology".

competences of the Authorities to assess all technological requirements and criteria, and all financial and regulatory aspects in accordance with the provisions of the Law. The validity of the License shall last for an indefinite time[13].

What is important to mention, between other criteria the law provides, is the one that requires to a legal entity to demonstrate, by documentary evidence, to have appointed a Board of Directors/Supervisory Board and guarantee by sworn statement that their relevant members:

> i. have a good professional and personal reputation, have sufficient knowledge, skills and experience, and commit sufficient time to carry out their duties and are able to clearly understand the type of activities and risks associated with them; and
>
> ii. that the Applicant will allocate sufficient human and financial resources to the training of the members of the Board of Directors or as the case may be, the Supervisory Board[14].

To carry out such activities, it requires persons with high integrity. But at this first stages, the law has provided only a sworn statement by the applicant, without providing the way this criterion is going to be evaluated.

The law in this same chapter, provides the licensing procedure and its timing. However, the margin of evaluation of the criteria, from the way it is defined in the law, is not exhaustive and leaves a lot of room for the authority that will implement the law, to evaluate on a subjective basis. Such a shortcoming is because the law itself should have exhaustively defined the elements and the evaluation procedure.

This is especially necessary considering that we are dealing with a completely new law, and the state institutions in Albania have not yet managed to create the necessary experience to control and supervise the implementation of this law, much less in such a new field not only for Albania. Taking into consideration that the entry in force of the law was not postponed, it did not leave the necessary time for the institutions to be prepared for its implementation and monitoring.

In the same chapter of the law, are described the powers of authorities towards the license holder, including information and investigation powers, such as[15]:

- the right to issue freezing orders: If AFSA deems that in order to protect the interests of current or potential clients, it is necessary the investigation of the License Holder, may initiate in collaboration with NAIS an investigation of the latter's activity; or
- the AFSA may issue an executive order freezing any person's bank accounts in cases where it deems that there is a risk that the person under investigation may harm investors;
- the AFSA may require adequate safeguards to protect the interests of investors, before unfreezing the bank accounts of the person under investigation.

Meanwhile, on-site inspections are also allowed, ant any officer of the Competent Authorities, on showing adequate proof of its authority, may enter the premises owned by a License Holder, for the purpose of obtaining the information or documents or any other evidence necessary for the purpose of the investigation.

[13] Article 6, paragraph 1, of Law no. 66/2020 "On financial markets based on distributed ledger technology".
[14] Article 9, point 1, letter "c)", of Law no. 66/2020 "On financial markets based on distributed ledger technology".
[15] Article 18, of Law no. 66/2020 "On financial markets based on distributed ledger technology".

State institutions, may in any case of breaching the law, suspend or revoke the License, in cases provided by the law, such as[16]:

- when the license holder fails to meet the general requirements and/or specific criteria provided by the Law;
- when the license holder provides false or inaccurate information to the Competent Authorities;
- contravened or does not comply with one or more of the general requirements and/or specific criteria provided by the Law;
- when competent authorities find that the subject is in breach of the provisions of the applicable legal framework.

In any case, a License Holder cannot assign or transfer the License to a third party without the prior written consent of the Competent Authority, which has to check beforehand if the legal person requested to be delegated or transferred the license meets the conditions set out in the law[17]. In any case, the Albanian authorities must be notified in advance for any intention related to any form of direct or indirect Change of Control of the License Holder, through any form of commercial transaction[18]. Such a requirement of the law is understandable, as long as the entities operating in this field, should enjoy credibility and public authorities must have control of these activities at any time.

The law dedicates a special chapter (Chapter III) to the Digital Token Agent, regulating the specific criteria any applicant should fulfill before being licensed, cases of conflict of interests, duties of the Digital Token Agents, and his liability for all the damages suffered by any Applicant or License Holder, as a direct consequence of a breach of any of the duties or obligations of the DT Agent provided for in the law.

Digital tokens and/or virtual currencies offerings, are regulated in the fourth chapter of the law, which applies to[19]:

- A Security Token Offering (STO), whereby the offer to the public has a total consideration equivalent to, or higher than, Euro 1.000.000,00 (one million) or its equivalent in ALL, calculated over a period of 12 (twelve) months;
- A Security Token Offering (STO), whereby the offer to the public has a total consideration of less than Euro 1.000.000,00 (one million), or its equivalent in ALL, calculated over a period of 12 (twelve) months;
- An Initial Coin Offering (ICO), whereby the offer to the public has a total consideration equivalent to, or higher than, Euro 8.000.000,00 (eight million), or its equivalent in ALL, calculated over a period of 12 (twelve) months;
- Initial Coin Offering (ICO) whereby the offer has a total consideration of less than Euro 8.000.000,00 (eight million), or its equivalent in ALL, calculated over a period of 12 (twelve) months.

From the entry into force of this law, Security Token Offerings can be launched by an Issuer in or from Albania, if the Issuer is a Person Resident in Albania. Meanwhile, The Digital Security Tokens issued through a Security Token Offerings which is not launched in or from Albania, can be offered in Albania only if the respective applicable

[16] Article 19, of Law no. 66/2020 "On financial markets based on distributed ledger technology".
[17] Article 20, of Law no. 66/2020 "On financial markets based on distributed ledger technology".
[18] Article 21, of Law no. 66/2020 "On financial markets based on distributed ledger technology".
[19] Article 33, of Law no. 66/2020 "On financial markets based on distributed ledger technology".

legislation is not less protective of the investors' interests than the Albanian law. All the process of launching a Security Token Offering, must be followed under the authorization and monitoring of the AFSA, which reviews the application for Authorization together with the relevant documentation.

Even the DLT Exchange is regulated in a separate chapter, (Chapter V), providing specific criteria a DLT Exchange License Applicant must fulfill, during the whole activity, duties, and his liability for all the damages suffered by any of its clients, caused as a direct consequence of a breach of any of the duties or obligations of the DLT Exchange provided in the law.

In any case, the law specifically requires that the Applicant for DLT Exchange License, which shall be a Centralized DLT Exchange, must demonstrate, by providing evidence in this respect, to have adopted and to maintain the following minimum security measures to set up a resilient internal system, capable to prevent and manage cyber-attacks and to offer to their clients a mean of recourse in case of fund loss[20]:

a) two-factor authentication of users;

b) "whitelisting" of users IP addresses;

c) use of off-line storages;

d) use of multi-signature digital Wallets;

e) periodical performance of tests to verify the resilience of the system;

f) periodical execution of penetration tests to verify the cyber security of the system;

g) performance of at least one yearly audit inspection to assess the maintenance and efficiency of the minimum security measures as indicated by the law;

h) measures to properly ensure and guarantee the segregation of the users' funds from the DLT Exchange's funds through the setup of separate Wallet addresses.

The law also provides clear regulations abut Innovative Service Providers and Innovative Technology Agreements (chapter VI). Innovative Technology Agreements, according to Albanian law, refers to Smart Contracts and any software used in projecting, programming and implementing DLT-based services[21]. Any Legal Person wishing to operate as an Innovative Service Provider must possess the relevant License granted by NAIS, because these activities may only be performed by those who hold the relevant License and only during the validity period of the License[22].

The Albanian law also acknowledges "Third Party Custody Wallet Providers", as legal entities that must first hold the relevant license to provide services to safeguard and custody private cryptographic keys on behalf of their clients, to hold, store and transfer digital tokens and/or virtual currencies[23]. To grant this type of license, in addition to the general requirements provided in the law, there are also some specific criteria that must be fulfilled, such as[24]:

[20] Article 55, of Law no. 66/2020 "On financial markets based on distributed ledger technology".
[21] Article 3, paragraph 42, of Law no. 66/2020 "On financial markets based on distributed ledger technology".
[22] Article 62, of Law no. 66/2020 "On financial markets based on distributed ledger technology".
[23] Article 3, paragraph 73, of Law no. 66/2020 "On financial markets based on distributed ledger technology".
[24] Article 77, of Law no. 66/2020 "On financial markets based on distributed ledger technology".

- implement all the necessary security measures to set up a sound internal system, capable to prevent or manage any form of cyber-attacks and to offer to clients a mean of recourse in case of fund loss as a consequence thereof; and
- have a minimum corporate capital of ALL 18,000,000 (eighteen million).

In any case, the law lets some flexibility that does not fully guarantee the principle of legal certainty and legitimate expectations, because it provides that additional obligations may arise as a result of the by-laws granted pursuant to the law[25], without setting a limit on the legal criteria that must be met by an entity. Such a provision may bring into practice uncertainty for entities operating in such a specific field, as the conditions and criteria for licensing and consequently the exercise of the activity, can be easily changed by a sub-legal act, putting these entities before the obligation to meet the new conditions and criteria.

The law lists in an exhaustive manner duties of the Third Party Custody Wallet Providers, as well as their liability for all the damages that have been caused by its clients as a direct consequence of a breach of any of the duties provided in the law[26].

There is a specific chapter in the law (Chapter IX) which regulates the "Prohibition of Market Abuse", which considers as market abuse:

- Market manipulation; and
- Trading based on privileged information.

This Chapter applies, in relation to all transactions with Digital Tokens/Virtual Currencies, to[27]:

a) acts or omissions committed in the Republic of Albania in relation with transactions with Digital Tokens/Virtual Currency of any Legal Entity Resident in Albania;

b) acts or omissions committed outside the Republic of Albania in relation to transactions with Digital Tokens/Virtual Currency by any Legal Entity Resident in Albania;

c) acts occurring in the territory of the Republic of Albania in relation to any Digital Tokens /Visual Currency, whether traded in or from the territory of the Republic of Albania; and

d) actions occurring outside the territory of the Republic of Albania in relation to any transactions with Digital Token / Virtual Currency traded in the territory of the Republic of Albania.

The law provides for the actions that constitute market manipulation, including every action that compromises[28]:

- transactions or trading orders that give, or are likely to give false or misleading signals in relation to the offer, demand, or price of Digital Tokens/ Virtual Currencies, or which provide the retention through a Person or several Persons acting in cooperation, related to the price of one or more of the Digital Tokens/Virtual Currency at an artificial level, unless the person who has effected the transaction or has given the

[25] Article 77, paragraph 3, of Law no. 66/2020 "On financial markets based on distributed ledger technology".
[26] Article 79, of Law no. 66/2020 "On financial markets based on distributed ledger technology".
[27] Article 87, of Law no. 66/2020 "On financial markets based on distributed ledger technology".
[28] Article 89, of Law no. 66/2020 "On financial markets based on distributed ledger technology".

trading order demonstrates that his reasons for doing so are legitimate and that these transactions or trading orders are consistent with accepted market practice;

- transactions or trading orders carried out through fictitious equipment or any other form of fraud;
- the dissemination of information through the media, including the Internet, or by any other means that provides or is likely to provide false or misleading signals in relation to the Digital Token/Virtual Currency, including the dissemination of rumors and fake news or misinformation, in the event the person who performed the dissemination was aware, or should have been aware, that the information was false or misleading.

In particular, the following activities and behaviors' arising from the definition of market manipulation shall be considered market manipulation[29]:

- acting in cooperation to secure a dominant position over the supply or demand of one or more Digital Tokens/Virtual Currencies, there by directly or indirectly keeping unchanged the transaction prices of Digital Tokens/Virtual Currencies;
- the sale of Digital Tokens/Virtual Currencies at the close of the market, resulting in misinformation of investors acting on closing prices;
- the benefit from the occasional or regular use of traditional or electronic media to express an opinion on a Digital Token/Virtual Currency or, indirectly, on its Issuer, after having previously held a position on this Digital Token/Virtual Currency;
- subsequently benefiting from the impact of the opinion expressed on the price of this Digital Token / Virtual Currency, without publicly disclosing and declaring the Conflict of Interest.

All DLT Exchanges, and DLT Trading Venues, determine and implement procedures and measures aimed at identification and prevention of market manipulation practices. In any event, DLT Exchanges or Trading Platforms shall inform the Competent Authority, based on the information to which they have access, of cases which they reasonably suspect constitute Market Abuse[30].

The law provides for sanctions and appeal procedures, for any act or omission resulting in a breach of provisions of the law. When imposing administrative measures, the authority must ensure that the measure is effective and preventive, and proportional to the causes which led to the imposition of an administrative fine[31].

4. Risks of the implementation of the new law in Albania

While virtual currency is welcomed in many parts of the world, some countries are concerned of its instability, decentralized nature, perceived threat to current monetary systems, as also of links to illegal activities such as drug trafficking and money laundering. Therefore, the regulation of the normative framework in this field with this law should be seen related to some aspects such as:

[29] Article 89, of Law no. 66/2020 "On financial markets based on distributed ledger technology"
[30] Article 91, of Law no. 66/2020 "On financial markets based on distributed ledger technology".
[31] Article 102, of Law no. 66/2020 "On financial markets based on distributed ledger technology".

- First, it relates to the current situation in Albania and the need to meet certain preconditions and standards that enable the effective functioning of financial markets based on distributed registry technology;

- Second, it is related to the increased risk of illegal transactions, money laundering and tax evasion[32].

The adoption of laws in this field is still a novelty for developed countries, while in Albania, direct steps are taken for their implementation without a proper evaluation. The implementation of such legal provisions, in a reality like ours, carries with it the risk of multiplying the negative risks that this innovation poses in developed countries. These risks can have social consequences within Albanian households and economic consequences, to the extent that they can shake the stability of the local currency, increase inflation or the exchange rate of the Albanian Lek (ALL) with foreign currencies[33].

Adoption of the legal framework and immediate start of its implementation, without proper preparation of monitoring and supervisory bodies, carries the obvious risk of creating space for the use of such financial markets by the organized crime, without effective opportunities for prevention, tracking and punishment. If such a situation occurs, it can damage the financial system as a whole, but also the investments of individuals in particular[34].

From the other hand:

- The adoption of the law without a proper analysis, needs some further amendments to the current legal framework, due to the fact that this law might not be in full harmony with the legal framework in force in Albania. For illustration: The very concept of trading in virtual currencies means trading without physical borders between countries, while when it comes to real estate, the legislation in force, depending on the type of real estate, contains restrictions regarding the transfer of ownership to a foreign citizen. Regarding the manner of transfer and registration of ownership, for illustration, of shares of a company or real estate, if the payment has occurred online, through a transaction made with virtual currencies, the non-harmonization of the law with the framework in force for the registration of ownership for certain categories of property titles, makes it difficult to register the new ownership, creating a great legal uncertainty for persons who may enter into these types of transactions.
- The law provides that[35], where the Issuer accepts FIAT Money in exchange for Digital Tokens/ Virtual Currency, he/she/it is obliged to open a bank account with an authorized banking institution. The FIAT money accepted by the Issuer must remain on separate accounts until the closure of the STO or ICO offer. But the law does not provide any specific regulation how responsible institutions should control the source of

[32] Accompanying reasoning of Decree no. 11518, dated 22.06.2020, of the President of the Republic of Albania "On the return of law no. 66/2020 "On financial markets based on distributed ledger technology", page 2. For more: https://www.parlament.al/ProjektLigje/ProjektLigjeDetails/51359. Last accessed 4.5.2022

[33] Accompanying reasoning of Decree no. 11518, dated 22.06.2020, of the President of the Republic of Albania "On the return of law no. 66/2020 "On financial markets based on distributed ledger technology", page 4. For more: https://www.parlament.al/ProjektLigje/ProjektLigjeDetails/51359. Last accessed 4.5.2022

[34] Accompanying reasoning of Decree no. 11518, dated 22.06.2020, of the President of the Republic of Albania "On the return of law no. 66/2020 "On financial markets based on distributed ledger technology", page 4. For more: https://www.parlament.al/ProjektLigje/ProjektLigjeDetails/51359. Last accessed 4.5.2022

[35] Article 49, of Law no. 66/2020 "On financial markets based on distributed ledger technology".

the deposit, the type of transaction, the control of money (whether it is money laundering, or not), and the fiscal obligation that arises from the transaction. There is no definition on how all these verification processes will be performed in this case. This lack of provisions to verify and control the above elements, creates insecurities and direct premises for avoiding the implementation of legislation in force in the country, regarding money laundering.

- The law provides only an article about taxation of transactions through Distributed Ledger, that sanctions: *The Natural persons and Legal entities, subject to this law shall comply with the relevant taxation applicable legislation in the Republic of Albania*[36]. But virtual currency transactions do not necessarily leave a mark. In these conditions, it is completely unclear how the collection of tax liabilities for these transactions will be made possible. Considering the very high values, over 1 000 000 Euros of transactions that can be performed, the inability to collect tax liabilities can lead to destabilization of the country's financial system.

5. Concluding remarks

In conclusion, we can say that a new law that regulates the activity through distributed registers, was definitely needed, but in any case, it would have been more recommended that the new legal framework:

- should have been approved after a thorough study of the effects of the application of the new law;
- should have been preceded by a major strengthening of institutional capacity to monitor implementation of the law;
- sufficient time should have been left after its approval, for the law to enter into force effectively and to start from its implementation.

In any case, time is needed to be able to understand the real effects of the law in the economy. Although the latest data made public[37], show a large number of virtual currencies production machines that have entered in Albania from the entry in force of the new law. Most of digital coins today in Albania are produced here. Given that it is a reality which cannot be stopped and cannot be turned back, Albania must have a strategy on how to regulate at least the manufacturing industry to turn it into a good for Albania and mainly the young people who deal with this. While its use in the economy will take some time despite the fact that Albania is among the first countries in Europe to adopt a law on cryptocurrencies[38].

Let us hope that Albania will not turn into a haven of abuse with virtual currencies. Mainly because referring even to the European Banking Authority (EBA), typically,

[36] Article 105, of Law no. 66/2020 "On financial markets based on distributed ledger technology".
[37] Article on ABCNEWS.AL "Mysteries of Bitcoin in Albania, evidence and areas where it is produced", 8 june 2021. For more: https://abcnews.al/1misteret-e-bitcoin-ne-shqiperi-deshmite-dhe-zonat-ku-prodhohet/. Last accessed 15.2.2022
[38] Article on ABCNEWS.AL "Mysteries of Bitcoin in Albania, evidence and areas where it is produced", 8 june 2021. For more: https://abcnews.al/1misteret-e-bitcoin-ne-shqiperi-deshmite-dhe-zonat-ku-prodhohet/. Last accessed 15.2.2022

crypto-asset activities do not constitute regulated services within the scope of EU banking, payments and electronic money law, and risks exist for consumers that are not addressed at the EU level. Crypto-asset activities may also give rise to other risks, including money laundering[39].

The European Supervisory Authorities (EBA, ESMA and EIOPA – the ESAs) warn consumers that many crypto-assets are highly risky and speculative. These are not suited for most retail consumers as an investment or as a means of payment or exchange, warning for their main risks, such as extreme price movements; misleading information; absence of protection; fraud and malicious activities[40].

The world is clearly divided when it comes to cryptocurrencies. In the future, there's going to be a conflict between regulation and anonymity. Governments would want to regulate how cryptocurrencies work. On the other hand, the main emphasis of cryptocurrencies is to ensure that users remain anonymous[41]. In the case of Albania, of course, the creation of a legal framework cannot be reprimanded, as the law must always precede when certain phenomena arise and spread. But on the other hand, to regulate a certain activity, it is not enough just to have a law in force, but a clear state policy is needed, altogether with public institutions that can effectively control the implementation of the law, in order to guarantee rights of citizens involved in such activities.

[39] The European Banking Authority (EBA), Reports on crypto-assets, 9 January 2019. For more: https://www.eba.europa.eu/eba-reports-on-crypto-assets. Last accessed 15.2.2022

[40] EBA, ESMA and EIOPA, Warning to consumers on the risks of crypto-assets, ESA 2022 15, 17 March 2022. For more: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Warnings/2022/1028326/ESAs%20warning%20to%20consumers%20on%20the%20risks%20of%20crypto-assets.pdf. Last accessed 15.2.2022

[41] Shivam Arora, What Is Cryptocurrency: Types, Benefits, History and More, 24 May 2022. For more: https://www.simplilearn.com/tutorials/blockchain-tutorial/what-is-cryptocurrency. Last accessed 15.2.2022

Legal challenges in the digital era: Protecting the trademark rights from online counterfeiters

Dr. Etlon Peppo – Prof. Assoc. Dr. Jola Bode

1. Introduction

Intellectual property rights ("IP rights") refer to the legal rights that are given to the creator or inventor to protect his creation or invention in accordance with the international and national law. These rights, which consist of human mind creations, have contributed enormously to the world and development of the society. IP rights are vital for their creator and the society in itself. Many companies rely in the enforcement of their IP rights, while the consumers can be assured about the trade origin and quality of the goods/services through the identification of IP rights.

Actually, IP rights are divided into two categories: Industrial Property, which mainly includes trademarks, industrial designs, patents, utility models, geographical indications, denominations of origin and/or other similar rights (plant varieties, integrated circuits or even trade secrets in some particular jurisdictions); and Copyright, which includes literature and artistic works.

All the above rights constitute a real and precious asset for their owners, and for that reason, a specific legal regime has been introduced to protect them from third party infringements. In fact, the protection of IP rights has been ensured in both international and national level. So, several international legal instruments, such as: TRIPS Agreement and Paris Convention, have been signed and ratified by a large number of states to protect IP rights and resolve trade disputes over intellectual property. On the other hand, states have adopted and enacted their own legal provisions to ensure an appropriate protection of these rights in line with their international obligations and national policy.

Legal protection of the intellectual property has significant importance for modern states and it has both global and national components. Global economic aspects of the IPR protection includes fulfilment of all basic principles of the multilateral conventions and adoption in the national legislation. Due to the changes in modern economy and business strategy, new legal tools of protection are introduced.[1]

[1] "Different legal aspects of the intellectual property rights"- EU and Comparative Law Issues and Challenges Series (ECLIC), Dijana Janković, University Josip Juraj Strossmayer of Osijek & Faculty of Law Osijek, 2017, Osijek, page 144, doi.org/10.25234/eclic/6526 (dated 25.01.2021).

Nowadays, the globalization of society and the huge impact of digital technologies have been broadly exploited to infringe the IP rights. In particular, the global pandemic situation has contributed to the development of online trade on the one hand and increasement of the risk for infringement of IP rights on the other hand. More specifically, the online sale of counterfeit goods has been significantly increased during this period. Infringers have broadly used and exploited the digital technologies to avoid detection and sell counterfeit goods in various parts of the world.

In light of the above, this paper is primarily focused on the criminal and civil legal remedies for the protection of trademark rights against the online counterfeiting activity. This kind of protection is essentially not only for the social and economic development of society, but even for the interests and rights of the consumers. The paper will so analyze the available remedies in combatting such illegal activity by pointing out the efficacy, advantages and disadvantages of both the criminal and civil legal remedies.

Further, this paper gives a particular attention to the importance of international legal instruments (i.e., the TRIPS Agreement and Paris Convention) in providing an adequate and effective protection of trademark rights. By analyzing the respective legal frameworks on this aspect, a special focus is put on the similarities and differences between the Albanian and Dutch legislation.

2. The importance of protecting trademark rights vs online counterfeiting

The legal concept of a trademark is broadly defined as a sign (or combination of sings) distinguishing the goods and/or services of an undertaking from those of other undertakings. In this regard, almost the same identical definition is found in the international or domestic law. But why is it so important to protect and register your own trademark? Which are the advantages and benefits from registering your own distinctive sings?

The importance of protecting IP was first recognized in the Paris Convention for the Protection of Industrial Property (1883). Countries generally have laws to protect IP for two main reasons:

• to give statutory expression to the rights of creators and innovators in their creations and innovations, balanced against the public interest in accessing creations and innovations;

• to promote creativity and innovation, so contributing to economic and social development.[2]

By a practical point of view, trademarks are found everywhere: in the Internet, at shops, markets, radio, TV, Facebook, Instagram, newspaper, etc. With respect to their nature and role, this paper underlines the fact that trademarks are important to be registered before the competent authorities because they do perform some essential functions in the course of trade:

- *Trademarks identify the source of origin of goods and/or services of a particular undertaking*: This function enables the consumers to choose their preferred products

[2] Understanding Intellectual Property (second edition). World Intellectual Property Organization, WIPO Publication, 2016, Geneva, page: 6

when buying certain goods or services, as well as the distinctive character of the company is evidenced.

- *Trademarks serve as a guarantee of quality for the concerned goods or services*: Consumers can rely on the quality of the goods or services based on their trademark. Moreover, the owner of a registered trademark may grant a license to the licensee by requiring the latter to respect and maintain the same quality standards.
- *Trademarks promote the sale of goods and the provision of services*: This function, also known as the communication function, enables the owners of trademarks to stimulate sales in the market through the associated trademark. Trademarks create interests and bring appeal to the consumers.

The owner of a registered trademark has an exclusive right in respect of the mark: the right to use the mark and to prevent unauthorized third parties from using it, or a confusingly similar mark, so as to prevent consumers and the public in general from being misled. The period of protection varies, but a trademark can be renewed indefinitely on payment of the necessary fees and on condition that the mark is used.[3]

In other words, a registered trademark enables to its owner to have the exclusive right to prevent third parties from using without authorization any identical or similar sign in the course of trading. More particularly, the EU Regulation 2017/1001 of the European Parliament and of the Council "On the European Union trademark" provides that it is also prohibited:

(a) affixing the sign to the goods or to the packaging of those goods;

(b) offering the goods, putting them on the market, or stocking them for those purposes under the sign, or offering or supplying services thereunder;

(c) importing or exporting the goods under the sign;

(d) using the sign as a trade or company name or part of a trade or company name;

(e) using the sign on business papers and in advertising;

(f) using the sign in comparative advertising in a manner that is contrary to Directive 2006/114/EC. [4]

The above provision has been almost identically introduced in the domestic jurisdictions of all the countries in the world, including the EU members and Albania.

Nowadays, one of the most common and illegal activities is counterfeiting. In this direction, the huge impact of technological developments and the new digital transformation have been broadly exploited to infringe the rights of trademark owners with the aim of making illegal profits. Moreover, the global pandemic situation caused by COVID-19 increased the risk of IP infringing activity and determined a new trend of the criminality in this field.

As a result, online counterfeiting is today one of the most significant issues that trademark owners and law enforcement agencies are dealing with everywhere in the world. Counterfeiters have perfectly exploited the new digital era by using various means and methods, such as: Internet, social media platforms and e-commerce, to sell and trade counterfeit goods.

This kind of activity is illegal and does infringe the rights of trademark owners or other entities that are authorized/licensed from them, while there are provided

[3] Understanding Intellectual Property (second edition). World Intellectual Property Organization, WIPO Publication, 2016, Geneva, page: 10

[4] Article 9 (3) of the EU Regulation 2017/1001 of the European Parliament and of the Council "On the European Union trademark"

different kinds of responsibilities (administrative, civil and criminal responsibilities) on the infringers based on the nature of their unlawful conduct. In that regard, various enforcement mechanisms and legal remedies are available to be used by the right-holders in combatting the counterfeiting activity.

3. International protection of the trademark rights: TRIPS Agreement and the Paris Convention

In the context of the international law, many authors affirm that IP rights enjoy a specific protection in the Universal Declaration of Human Rights (UDHR). Likewise, the World Intellectual Property Organization ("WIPO") has underlined in its manuals that intellectual property rights are safeguarded by Article 27 of the Universal Declaration of Human Rights.[5] In light of this provision, everyone has the right to use her/his rights deriving from the ownership of the intellectual property objects: Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.[6]

Furthermore, states have also cooperated with each-other in order to set some minimum standards and ensure the protection of IP rights at an internal level. The first achievement at the *level* of binding *international* law was the adoption of the Paris Convention for the Protection of Industrial Property ("Paris Convention"), which best reflects the efforts of states to protect the IP rights as a way for promoting the creativity and social-economic development.

With respect to the trademark rights, article 9 of Paris Convention deal with the seizure of those goods unlawfully bearing a mark. Pursuant to point 2 of the said article, *seizure shall likewise be effected in the country where the unlawful affixation occurred or in the country into which the goods were imported*.[7] In addition, the Convention further provides the obligation of countries of the Union to adopt effective legal remedies for ensuring the protection of trademark rights against infringement and unfair competition.

The Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS Agreement") represents another important legal instrument aiming to enforce the trade-related intellectual property rights by taking into account the differences in national legal systems. This Agreement outlines the specific objective of protection of IP rights in the context of the technological innovation and development, which is particularly important in the current digital era: *The protection and enforcement of intellectual property rights should contribute to the promotion of technological innovation and to the transfer and dissemination of technology, to the mutual advantage of producers and users of technological knowledge and in a manner conducive to social and economic welfare, and to a balance of rights and obligations*.[8]

Part II, Section II of the TRIPS Agreement is entirely dedicated to trademarks and the rights conferred by their registration, while Part III is specifically reserved to

[5] What is intellectual property?, World Intellectual Property Organization, WIPO Publication, 2020, Geneva, page: 2.
[6] Article 27 (2) of the Universal Declaration of Human Rights, 1948
[7] Article 9 (2) of the Paris Convention for the Protection of Industrial Property, 1883 (as amended)
[8] Article 7 of the Agreement on Trade-Related Aspects of Intellectual Property Rights

the civil, administrative and criminal remedies for the enforcement of intellectual property rights. In this view, all the member states shall adopt effective and adequate legal remedies against the infringement of IP rights.

In general, administrative and civil remedies are most commonly used by the trademark owners to demand compensation for an infringement, injunctions halting further infringements and other similar measures (including the imposement of administrative fines). However, taking into account the nature of the illegal activity of counterfeit goods, the border measures are deemed to be one of the most effective remedies available to the trademark owners.

In this regard, TRIPS Agreement puts the obligation on the member states to adopt the necessary procedures to enable a right-holder to lodge an application with the competent authorities and obtain the suspension by the customs of the release into free circulation of counterfeit goods. All the border measures and relation procedures are expressly provided in articles 51-60 of the agreement.

As regards the criminal legal remedies, which constitute an essential part of this paper, the TRIPS Agreement has the added significance of being the first international legal instrument that determine that states have the obligation to criminalize the infringement of intellectual property rights, in particular where they are committed willfully and on a commercial scale. In this regard, one of the key priorities for EUROPOL and other national law enforcement agencies is to combat the illegal counterfeiting activity.

Namely, article 61 of the TRIPS Agreements require member states to provide and apply for criminal procedures and penalties at least in cases of willful trademark counterfeiting or copyright piracy on a commercial scale.[9] Pursuant to the same article, criminal legal remedies shall necessarily provide the imprisonment and/or monetary fines. Other available and possible remedies include the seizure, forfeiture and destruction of the infringing goods.

In other words, it may be so stated that Intellectual Property crime is committed when someone willfully manufactures, sells or distributes counterfeit goods for commercial gain.

4. Online counterfeiters and the legal remedies for the protection of trademark rights – criminal or civil remedies?

As stated above, online counterfeiting represents a very serious risk for the rights and interests of the trademark owners. By exploiting the world of social media and e-commerce platforms, infringers have become very active in marketing counterfeit goods to a very large audience. This has obliged the trademark owners to seek and use all the possible remedies in combatting the counterfeiting and protecting their rights.

Furthermore, the counterfeiting activity and the infringement of trademark rights may pose even a higher risk for the consumers and the entire society in itself if the scope of this activity concerns specific kinds of goods, such as: pharmaceuticals, parts for automobiles and planes, food items, etc. In this regard, the US Department of Justice rightly asserts that the impact of today's IP crime is not limited to the

[9] Article 61 of the Agreement on Trade-Related Aspects of Intellectual Property Rights

economic challenges associated with piracy, counterfeiting, or trade secret theft. Inferior, unsafe counterfeits, ranging from electrical equipment to auto parts to pharmaceuticals, not only defraud ordinary consumers, but also can pose significant risks to their health and safety.[10]

With respect to this matter, this paper aims to briefly analyze the potential and available legal remedies for the protection of trademark rights with a focus on the criminal law. In addition to the specific IP laws, the Civil and Criminal Codes do also contain relevant provisions related to this subject matter. Many authors are predisposed to study the efficiency and applicability of civil remedies only, but we have tended to focus on the criminal remedies and believe that this legal remedy shall be always applied in all those cases dealing with counterfeit goods of a particular nature, such as: pharmaceuticals or food products for example.

Administrative fines seem to be not so effective in combatting the counterfeiting activity, while it is not the same as regards the border measures imposed by the customs authorities. Right-holders have the possibility to file customs application with the customs authorities to enable the identification and seizure of counterfeit goods infringing the IP rights. Likewise, the role of Market Inspectorate is essential to combat this illegal activity within the internal territory as the customs measures may be applied to borders only.

In these cases, right-holders can file an official application with the competent state authorities by providing the necessary information to identify the genuine goods and distinguish them from the counterfeit ones. This information includes, but it is not limited to: the distinctive features of the goods, information on the producers and traders of the goods, the place of production of the goods, images of the goods, etc.

As a matter of fact, trademark owners prefer to file civil actions against the infringers in order to cease the infringement and seek compensation for the damages. The civil remedies may include the possibility to file lawsuits, injunction requests or create deterrence. In particular, these remedies are mainly provided in the national IP law of each country. A special chapter of this IP law is generally dedicated to the legal remedies and their applicability criteria.

When the court finds that the defendant infringed a trademark, it may issue an order prohibiting the defendant to further infringe the trademark rights. Provisional measures and injunctions constitute other possible civil remedies to ensure the trademark rights and prohibit the infringer to continue the illegal activity.

In addition to the above, the civil legal framework includes the possibility of the trademark owner to remove from the civil circulation all the materials, instruments, devices and other means that are used to manufacture the infringing goods. As regards the counterfeit goods, including herein those counterfeit goods that are traded online, it is not sufficient to simply remove or detach the trademark/sign that is attached to these goods. The trademark owner may also ask for indemnification and request to have the court decision published in the public media at the expenses of the infringer.

Notwithstanding from the above, it seems that the globalization and the development of the technology has contributed to increase the online counterfeiting

[10] Prosecuting intellectual property crimes (fourth edition), US Department of Justice, Office of Legal Education Executive Office for United States Attorneys, 2017, page: 2.

activity. In particular, the use of social media and e-commerce platforms do now represent a higher risk for the trademark owners and the right-holders. For that reason, trademark owners often agree that the deterrence to trademark infringement may be ensured through criminal prosecution.

Furthermore, counterfeiting and IP crimes are often related to other criminal offenses, and therefore, it might be even more difficult to combat the illicit activity without a criminal prosecution of the case. Several reports and researches have evidenced that any use of money derived from certain types of IPR violations to fund specific forms of crime is considered money laundering.[11]

In addition, IPR infringements can also facilitate the commitment of other crimes such as: tax evasion, smuggling, organized crime, cybernetic crime, fraud, etc. The profits from the products infringing intellectual property has begun to exceed the profits from drugs and weapons on the profit/weight basis and always due to lower penalties.[12]

In this regard, we have to say that practical and complex problems may arise in applying criminal prosecution to online trademark infringement and counterfeiting activity. Despite these difficulties, the criminal legal remedies may be more efficient to be applied in case the civil measures are not sufficient to deter and prohibit the illegal activity of counterfeiting.

Upon the request of the trademark owner, the police office or the prosecutor shall investigate and initiate the criminal proceedings against the infringer of trademark rights once the latter is identified and all the necessary legal requisites for criminal prosecution are met. In many jurisdictions, the criminal prosecution for infringement of IP rights may be initiated only if a complaint is filed by a private party (i.e., the private prosecution).

In order to succeed in the criminal proceedings, the trademark owners should cooperate with the police officers/prosecutor and exchange all the information/documents in their possession. More specifically, in the case of online counterfeiting, the preserve of evidence is crucial for the outcome of criminal proceedings.

To illustrate the importance that the criminal prosecution of intellectual property crime bears for the economic system of a country, we would like to briefly present how this specific type of crime is approached and handled by the US authorities. The FBI's Criminal Investigative

Division's Intellectual Property Rights Unit ("IPRU") oversees its national intellectual property rights program, which includes dedicated FBI Special Agents responsible for investigating (i) thefts of trade secrets, (ii) manufacturing and

[11] Intellectual Property and White-collar Crime: Report of Issues, Trends, and Problems for Future Research, National White Collar Crime Center, 2004, https://www.ncjrs.gov/pdffiles1/nij (dated on 21.01.2021).

[12] Hetimi dhe ndjekja e veprave penale që lidhen me pronësinë intelektuale në Shqipëri: Manual për trajnimin e prokurorëve, gjyqtarëve dhe autoriteteve të tjera ligjzbatuese [*Criminal investigation and prosecution of the criminal offenses related to intellectual property in Albania: Handbook for training of the prosecutors, judges and other law enforcement agencies*], Mariana Semini-Tutulani, WIPO, 2020, Geneva, page: 14.

trafficking in counterfeit goods, and (iii) IPR infringement, which causes significant economic impact.[13]

In light of the above, we may conclude that there are several civil and criminal legal remedies to be applied against the infringers of trademark rights. Some remedies are more efficient, while others are more practical for the owners of trademark. However, combatting online counterfeiting is not always a simple task and the trademark owners should evaluate the best route to achieve the desired results in prohibiting or deterring the infringement. In this context, online takedown mechanisms may be also used to monitor and combat illicit activity involving the trade of counterfeiting goods in the social media pages or e-commerce platforms.

If the problem and its related counterfeiting activity is minor, the online takedown may constitute the most effective and costless action to stop the infringing activity. Meanwhile, these mechanisms may not be sufficient if the problem is persistent and more severe. In such cases, the civil or criminal actions should be followed to pursue the infringement matter.

But, in general, there is a distinct line between the administrative, civil and criminal sanctions that are applied against the infringers of trademark rights. For example, the Republic of China, as many other jurisdictions over the world, has defined a distinct line between the administrative and criminal sanctions for illicit counterfeiting of goods. Administrative punishments may be imposed according to relevant laws and regulations on common IPR violations that are inadequate to be deemed crime, and criminal punishments are imposed in the cases where serious harm has been done to the society and the amount involved in the violation or the loss caused to the victim reaches the threshold for prosecution.[14]

5. Trademark rights protection in Netherlands and Albania – similarities and differences

At the international level, most of the countries have signed a number of important legal instruments, such as: the Paris Convention, TRIPS Agreement or Madrid Agreement and its related Protocol. Furthermore, almost all the countries are now members of the World Intellectual Property Organization ("WIPO") and World Trade Organization ("WTO"). The signature, adoption and rectification of the said legal instruments constitutes a great achievement and guarantee for the international protection of trademark rights.

In addition to the above, states have also adopted their domestic legislation in the field of intellectual property rights to regulate these matters within their jurisdiction. Some states, such as Albania, have enacted a single specific law on industrial property and a series of bylaws for each specific IP right. On the other hand,

[13] Reporting intellectual property crime - A guide for victims of copyright infringement, trademark counterfeiting, and trade secret theft (third edition), US Department of Justice, Computer Crime and Intellectual Property Section, 2018, page: 10, www.justice.gov/criminalccips/.ccips-documents-and-reports (dated on 25.01.2021).

[14] "Intellectual Property Rights Protection through Criminal Justice in China, Current Situation and Prospects" Speech at the Third Global Congress on Combating Counterfeiting and Piracy, Xiong Xuanguo, 2007, Geneva, page:2, https://www.wipo.int/edocs/mdocs/enforcement/en/third_global_congress/third_global_congress_ref_f.pdf. (dated 20.01.2021).

many states have decided to enact a specific trademark law for the registration and protection of trademark rights, while separate laws have been enacted for the other kinds of IP rights (patents, industrial designs, etc.).

In light of the above, we first have to say that the IP legislation is generally based on the same principles and rules regulating the enforcement of rights. Owing to the accession in the international IP legal instruments, states have the obligation to regulate some specific areas in a particular way, as well as to ensure a minimal standard of protection and ensure the enforcement of IP rights.

For that reason, EU member states have almost entirely harmonized their domestic IP legislations in order to avoid convergences. Also, non-EU member states have harmonized and approximated their legislation in accordance with the *acquis communautaire* to obtain the same level of protection of IP right as the EU directives sets. Thus, we may find out a lot of similarities between the IP legislations of different countries in the world.

Without prejudice to the EU Regulation 2017/1001, this paper is briefly focused on the analysis of the main similarities and differences between the Albanian and Dutch legislations in view of the applicable legal remedies for the enforcement of IP rights.

The Albanian Law no. 9947/2008 "On Industrial Property" [as amended] ("Law no. 9947/2008") has been almost fully harmonized with the EU legislation. Therefore, as a consequence, almost the same civil legal remedies are provided by law no. 9947/2008:

- Filing a lawsuit for infringement with the Tirana District Court to cease the infringement (including the removal of infringing goods and other related means from the market) and ask for indemnification, as well as claiming the publication of the final court decision at the expenses of the infringer[15];
- The right to information regarding the origin and distribution network of infringing goods;[16]
- Filing a request to obtain provisional measures/injunctions against the infringer(s) with the Tirana District Court;[17]

In light of the above, article 348 of the Code of Civil Procedure determines that the Tirana District Court is the sole competent court for adjudicating legal disputes concerning trademark and other IP rights.

As regards the possibility to use other administrative legal remedies and involve the competent state authorities in the battle against this illicit activity, we would like to underline that the trademark owners and/or their authorized representatives are also entitled to:

- File a complaint with the Inspectorate of Market Surveillance in order to detect and then destroy the counterfeit goods that are traded within the internal market;
- File a customs application with the General Directorate of Customs in order to seize and then destroy the counterfeit goods infringing the intellectual property rights at the customs borders;

[15] Articles 184/a, 184/b and 184/c of Law no. 9947, dated 07.07.2008 "On Industrial Property" (as amended)
[16] Article 185 of Law no. 9947, dated 07.07.2008 "On Industrial Property" (as amended)
[17] Article 187 of Law no. 9947, dated 07.07.2008 "On Industrial Property" (as amended)

In addition to the above, the Criminal Code of the Republic of Albania[18] provides for criminal responsibility if IP rights are infringed to produce and trade counterfeit goods for commercial purposes. This criminal law provision is in line with the obligations imposed by article 61 of TRIPS Agreement, which has been duly rectified by the Republic of Albania. The offender may be punished by fine or imprisonment of up to 2 years.

On the other hand, no separate trademark law exists in the Kingdom of the Netherlands. Namely, the trademark law is governed by the Benelux Convention on Intellectual Property, the current version of which entered into force on 1 March 2019. The Benelux Convention gives the right to the trademark owner to use the registered mark in an exclusive manner and also prohibit third parties from using such sign without consent.

With the focus on the civil legal remedies provided by the Benelux Convention on Intellectual Property, we briefly analyzed the corresponding law provisions to find out the existing similarities and differences with the Albanian legal framework:

- The right to claim compensation for any prejudice the trademark owner has suffered. Unlike Albanian IP law, the Benelux Convention provides the possibility for the claimant to request the court to order that the ownership of infringing goods be transferred to the proprietor of the trademark upon the payment of a fixed fee;[19]
- Filing a lawsuit for infringement with the court and request to cease the infringement (including the recall from the channels of commerce, the definitive removal from the channels of commerce or the destruction of goods which infringe a trademark right, as well as, in appropriate cases, materials and implements principally used in the manufacture of those goods);[20]
- Filing a request to obtain interlocutory injunction against an alleged infringer or intermediary;[21]
- The right to information regarding the origin and distribution network of infringing goods;[22]
- Filing a request with the court to order the infringer to disseminate information concerning the decision[23];

The enforcement of registered trademark rights in Benelux is efficient. While there is no specialised court for general trademark disputes, most of the district courts and courts of appeal have judges who focus on IP matters. Due to its exclusive jurisdiction for EU trademark and design matters, the Hague District Court has highly specialised judges.[24]

Of course, the market surveillance and customs measures may be also used to combat the illicit activity of counterfeiting. Counterfeiting of goods is posing a critical challenge for the world economies and even for the safety of consumers in specific sectors. Therefore, the intervention of these authorities against this fraudulent and illicit activity does represent an essential need.

[18] Article 149/a of the Criminal Code of the Republic of Albania (1995)
[19] Article 2.21 of the Benelux Convention on Intellectual Property (2019)
[20] Article 2.22 (1) of the Benelux Convention on Intellectual Property (2019)
[21] Article 2.22 (3) and (5) of the Benelux Convention on Intellectual Property (2019)
[22] Article 2.22 (4) of the Benelux Convention on Intellectual Property (2019)
[23] Article 2.22 (7) of the Benelux Convention on Intellectual Property (2019)
[24] Viewed at//www.worldtrademarkreview.com/anti-counterfeiting/benelux (dated on 01.04.2021)

With respect to the criminal responsibility for committing an IP crime in the Netherlands, the Dutch Criminal Code provides different terms of imprisonment based on the crime scale. More particularly, section 337 (1) of the Criminal Code of the Kingdom of Netherlands provides a term of imprisonment not exceeding one year or a fine of the fifth category as a penalty against the infringer who intentionally imports, conveys in transit or exports, sells, offers for sale, delivers, hands out or has in store counterfeit goods, except in case when these goods are exclusively for personal use.

The penalty is increased to a term of imprisonment not exceeding four years or a fine of the fifth category if the criminal offence is conducted as a profession/business or is likely to cause danger to persons/property.[25]

6. Conclusions

Intellectual property rights, and in particular trademarks, are considered capital assets and enable their holders to have exclusive rights over them. For that reason, a special legal framework has been adopted in both an international and national level. On the other hand, we are all witnesses that the new digital era has been and is being broadly exploited to infringe IP rights. More particularly, the trademark rights have been and are still being broadly infringed via online through the sale of counterfeit goods in the social media platforms, webpages or e-commerce platforms.

While it is true that combatting this illegal activity is not a simple task, states have enacted several legal acts to enable right-holders to use criminal, civil and administrative legal remedies. The protection of trademark rights is essential for the social and economic development of the society, whereas the consumers shall be ensured about the trade origin of the goods/services and their quality.

As said above, several international legal acts, such as: the TRIPS Agreement and Paris Convention, have been signed and ratified by a large number of states to protect IP rights and resolve trade disputes over intellectual property. Moreover, states have adopted and enacted their own legal provisions to ensure an appropriate protection of these rights in line with their international obligations and national policies.

While the globalization of the society and the huge impact of digital technology is used as a common tool to infringe trademark rights, the global pandemic situation did recently contribute to the increment of risk for infringement of trademark rights. More specifically, the online sale of counterfeit goods has been significantly increased during this period. Infringers have broadly used and exploited the digital technologies to avoid detection and sell counterfeit goods in various parts of the world.

The legal concept of a trademark is broadly defined as a sign (or combination of sings) distinguishing the goods and/or services of an undertaking from those of other undertakings. In this regard, almost the same identical definition is found in the international or domestic law. In the terms of law, the owner of a registered trademark has an exclusive right in respect of the mark: the right to use the mark and to prevent

[25] Section 337 (3) and (4) of the Criminal Code of the Kingdom of Netherlands, 1881 (as amended)

unauthorized third parties from using it, or a confusingly similar mark, so as to prevent consumers and the public in general from being misled.

Online counterfeiting is today one of the most significant issues that trademark owners and law enforcement agencies are facing, while it does also represent one of the most common online IP crimes. Moreover, this counterfeiting activity and the infringement of trademark rights may pose even a higher risk for the consumers and the entire society in itself if the scope of this activity concerns specific kinds of goods, such as: pharmaceuticals, parts for automobiles and planes, food items, etc. We have seen that the internet access has been grown and nowadays people from all over the world can easily communicate with each-other.

Based on the nature of the unlawful conduct of the infringer and the type of infringement, the legislator has provided different kinds of responsibilities and measures: administrative, civil and criminal.

In the context of the international law, states have cooperated with each-other in order to set some minimum standards and ensure the protection of IP rights (including trademark rights in particular) at an internal level. The Paris Convention set the obligation of countries of the Union to adopt effective legal remedies for ensuring the protection of trademark rights against infringement and unfair competition, including the seizure of goods unlawfully bearing a mark.

On the other hand, Part III of the TRIPS Agreement is fully reserved to the civil, administrative and criminal remedies for the enforcement of intellectual property rights. In this regard, all the member states shall adopt effective and adequate legal remedies against the infringement of IP rights.

In general, administrative and civil remedies are most commonly used by trademark owners to demand compensation for an infringement, injunctions halting further infringements and other civil remedies. However, taking into account the nature of the illegal activity of counterfeit goods, the border measures (e.g., customs applications) are deemed to be one of the most effective remedies available to the trademark owners

As regards the criminal legal remedies, states have been obliged to criminalize the infringement of intellectual property rights, in particular where they are committed willfully and on a commercial scale (i.e., a legal obligation that is set by article 61 of TRIPS Agreement). Criminal legal remedies shall necessarily provide the imprisonment and/or monetary fines. Other available and possible remedies include the seizure, forfeiture and destruction of the infringing goods.

As a matter of fact, trademark owners prefer to file civil actions against the infringers in order to cease the infringement and seek compensation for the damages. The civil remedies may include the possibility to file lawsuits, injunction requests or create deterrence. Notwithstanding this, criminal legal remedies may be more efficient to be applied in case the civil measures are not sufficient to deter and prohibit the illegal activity of counterfeiting. In particular, it might be much easier to obtain judicial cooperation (e.g., gathering and sharing evidence) in combatting the illegal activity once the infringement is considered as a criminal offense as well.

In many jurisdictions, the criminal prosecution for infringement of IP rights may be initiated only if a complaint is filed by a private party (i.e., the private prosecution). In order to succeed in the criminal proceedings, the trademark owners

should cooperate with the police officers/prosecutor and exchange all the information/documents in their possession. More specifically, in the case of online counterfeiting, the preserve of evidence is crucial for the outcome of criminal proceedings.

In light of the above, we may conclude that there are several civil and criminal legal remedies to be applied against the infringers of trademark rights. Some remedies are more efficient, while others are more practical for the owners of trademark. If the problem and its related counterfeiting activity is minor, the online takedown may constitute the most effective and costless action to stop the infringing activity. Meanwhile, these mechanisms may not be sufficient if the problem is persistent and more severe.

In a comparison between the Albanian and Dutch legislation, we found that almost the same legal remedies are provided in respect of the above. Despite these similarities, the IP law professionals in Albania should learn from the experience and well-developed practice of the Dutch and EU law in order to increase the awareness and the level in combatting the illegal activity of online counterfeiting.

Recently, some IP Offices, such as EUIPO, have entered into agreements with e-commerce platforms to let and enable right-holders to report infringements. This tool would be certainly a further step in combatting and preventing the sale and distribution of counterfeit goods, but the adoption of more severe criminal sanctions in this field may be an additional effective tool to combat online counterfeiting activity.

Computer fraud according to article 143 / b of the albanian criminal code

Prof. Assoc. Dr. Dorina Hoxha –Markelian Koça Ph.D. Cand.[1]

1. Introduction

The criminal offense of computer fraud is provided for the first time in the Albanian Criminal legislation in article 148 / b, as a new provision by Law No. 10 023 date 27.11.2008. The needs dictated by the legislator were related to the development of technology and its use of the time. The Computer Fraud crime harms computers, bank computers, and computers connected to the Internet. It shields them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud.
In the cybercrimes field stands out computer fraud, which even though is a new article it has taken a considerable place in practice, but ambiguity can often be understood from the case law itself, regarding the constituent elements of this criminal offense, which are related closely with its structure. This criminal offense consists of extortion of property through the fraudulent use of actions in computer data or the operation of a computer system.
The purpose of this research is to analyze the structure of the criminal offense of computer fraud, the difference that it has with similar computer criminal offenses, which provide actions that seem somewhat similar to it in terms of criminal actions, the attitude of court practice in determining the forms of occurrence of this criminal offense as well as the needs of legal changes.
At the international level, Albania has ratified a series of conventions, although their initiative was much earlier, around the '80s.

2. Analysis of the structure of the criminal offense of "Computer Fraud" according to the provisions of Article 143 / b of the Albanian Criminal Code[2].

Computer fraud has the same structure and the same constituent elements of general fraud, it differs only that the fraudulent actions of the perpetrator are directed not to the passive subject, where there is no abuse of trust or lies, but to the computer system that belongs to him, through manipulation of this system.

2.1 Typology of actions that determine the objective side of this criminal offense.

Article 143 / b / 1 of the Criminal Code has objectively defined several ways by which this criminal offense can be committed, which seem to have a similarity between them. "Changing computer data" and "interference in the operation of a computer system" consists in modifying the regular operation of the computer, to enable certain actions that lead to consequences not at all desired by the holder of this right and unjustly obtained by the perpetrator of the criminal offense.

By computer system should be understood a set of means intended to fulfill every function necessary for the person, through the use of information technologies, which are characterized, through an action as "codification", "decoding", "registration" or memorization" through electronic pulses, in order to generate information[3].

"*Interference with the operation of a computer system*" means that the computer or computer system is in some way altered in its previously programmed elements, in hardware or software, so the only way to accomplish the author's objective, should be to change the system. From the way, how it is formulated from the legislator, it seems that there are two different ways of committing this criminal offense. By using the conjunction "or", it should be understood that we have to deal with different kind of ways to commit this crime, but it can dot be excluded that interfering with the operation of the computer can be considered as a preparatory action to change this data.

From the objective point of view, it is clear that we are dealing with interference in the operation of a computer network, where data is obtained illegally, which is distributed, for example, to customers through fraud as if it were their computer data. The two forms of committing this criminal offense, seem to be partially overlapping with each other, but they are nevertheless two different concepts and are applicable independently. I think that the legislator has foreseen this second form, to include all those actions that are impossible to summarize in a single notion, and that can have specific ways to be committed. Despite this provision, it must be accepted that the objective side of the criminal offense provided by Article 143 / b is more specified than in Article 143 of the Criminal Code, where "*lying*" "*and abuse of trust*" have a much more general character.

In most case laws, the importance is given to the *material object* of the action, whether the information system, specifying it in a much more accurate way and leaving a wider description of the actions which can be committed in several forms.

"*Interference in the operation of a computer system*" refers to the regular development of the process of data processing, reading, data transmission, and any process that has to do with its operation.

To understand when there is the intervention in the functioning of a computer system, it is necessary to refer to the results of the process, that is evaluated by the programmer or by the user. Each electronic processor, by entering certain commands, is programmed to perform one or more specific operations, where one input always responds to a result. By creating a change at the action, the agent modifies the computer process, causing the computer to produce a different result from the regular one. This behavior is characterized by a logic of interfering with the predetermined modes of operation of a system, unlike the second behavior which aims only at "data, information or programs" does not necessarily imply their manipulation.

To understand more accurately the intervention in the functioning of a computer system we are referring to the decision No. 261 dated 2.10.2013 of the High Court[4], from which it results that various persons who exercised commercial activity in the field of electronics, were enabled to intervene in the computer system, specifically the Internet, by destroying the codes and as a result, to enable the provision of illegal programs, the exclusivity of which has had only Company "X" in its packages. The defendants had electronic devices that enabled internet connection with the devices they sold, giving to the customers the opportunity to open television programs for which they were not licensed. The opening of these TV channels was coded by the companies that were licensed and offered the service in the market and the devices sold by the defendants were programmed to receive from the internet signal the decrypted codes that enable the opening of the programs of the defendants. Based on the technical data obtained from Company X, which manufactures the relevant equipment for the licensed companies, the Smart card for the "x" device was used illegally by the defendants, as an integral part of the computer network[5].

This includes the consumption of the criminal offense, because the defendants provided computer data illegally by licensed operators in the market, in order to provide third parties an unlicensed service and providing themselves illegally incomes. The activity of the defendants is related to the illegal acquisition of computer data and their entry into the Internet network through fraud, as they were owners of this data, certainly for the purpose of economic gain[6]. From the objective point of view, it is clear that we are dealing with interference in the operation of a computer network, where data is obtained illegally, which is distributed to customers through fraud as if it were their computer data[7].

Modification due to interference can be done at any stage of the processing data, both for the "purposes" for which the information system is intended and for its content. It may include, even indirectly, a manipulation of both the data intended to be processed later (input manipulation) and the instructions related to the specific

processing to which the data must be subjected (program manipulations) and recently data already regularly processed, but which must be decoded into a language understandable to man (manipulation of production). In relation to the immediate object on which the deceptive behavior falls, we can distinguish software manipulations, i.e. those that affect the logical component of the system, from the manipulations of the device, or those that affect the mechanical component of the same[8].

2.1.1 . " Phishing".

One of the ways of committing the criminal offense is called "Phishing". Specifically, the examination shows that "Phishing", is the act of attempting to copy information such as "username", "passwords", etc., through camouflage as legal entities during electronic communication on popular and social Internet addresses, addresses for conducting auctions etc., which are mainly used to seduce the public.

In the context of cybercrime, "Phishing" is introduced, consisting of a fraudulent "social engineering" technique aimed at stealing personal information (personal data; user ID and password for online checking accounts; credit card codes; etc.) utilizing the 'social' aspects of the Internet, in order to access home banking systems or current accounts and online services, to dispose of deposits through fraudulent banking operations and transfers to holders.

Phishing emails may contain Internet links to addresses that are infected with a computer virus. This method is mainly done through fake emails or "Chat" communications and often directs users to give their details to a fake website, which have the appearance of legitimate ones. This means that if the "victim" clicks, automatically, the system links to the address named by this person, which is located under the original address www.000webhost.com, in order to enter in the relevant fields his e-mail address or name of the user as well as the password. This data is automatically stored in a "TXT" data, according to the configuration made by the computer author himself. This "TXT" data is downloaded from time to time by him to view and receive all the details of the victims, who clicked on his address and wrote the e-mail address and the corresponding password.

For this reason, doctrine and jurisprudence agree that fraud committed with malware or other self-installing programs should be traced to the crime of computer fraud. Phishing hypotheses in which the victim secures their data by entering the link sent by email, on the other hand, are considered fraudulent in accordance with Article 134 / b of the Criminal Code. In the latter case, in fact, the victim is deceived by emails with forged logos and credible claims.

2.2 "Unjust economic profit" and "wealth reduction of a third party" according to an economic and legal meaning.

Once the typical behavior of computer fraud has been clarified, it is necessary to analyze the events in a naturalistic sense, etiologically connected to the conduct, provided for by the rule of art. 143/b of the Criminal Code.
In the crime of Fraud, at least three different events occur: the act of disposition of assets by the defrauded subject, which does not necessarily coincide with the passive subject of the crime (for example, the cashier of a bank who, misled on the identity of the account holder, carries out transactions not authorized by the account holder); the realization of an unjust profit by the offender; and, finally, the specular damage of others and consequent to the realization of the unfair profit. In addition to these events, according to a minority doctrine there would be a further one, consisting of the misleading of a subject (which is usually the one who carries out the asset disposal act).
In the case outlined by art. 143/b of the Criminal Code the unjust economic profit and other damage (property) are present.
As already stated, in fact, in art. 143/b of the Criminal Code, there is no reference to the induction into error of someone by 'tricks or deceptions' or to the performance of an asset disposal act (by the taxable person or by a third party). This deserves an in-depth study, in order to fully understand, the discriminating element between the crimes of fraud and computer fraud. As mentioned above, what clearly distinguishes the two crimes is the presence of a person misled, in the crime of fraud, which is not required by art. 143/b. In fact, if the crime of fraud art 143 needs necessary that someone should (therefore a natural person) be misled, by means of artifices or deceptions, in such a way as to obtain, thanks to this, his artificial cooperation (the fulfillment of an act of asset provision) the unjust profit, this element does not occur in the case under art. 143 b of the Criminal Code, in which the conduct is directed directly to the computer system.
After that, we can briefly analyze the two events of the crime of computer fraud, consisting of the realization of "unfair economic profit" or "property damage of others".
With reference to the notion of unfair profit, it is clear that, for the purposes of applying art.143/b, it is required that the profit be inherent in an unfair method of obtaining, in this sense it must be understood that the acting subject has moved in an area of illegality and that, therefore, has acted in a position of opposition to the legal system. It should also be added that the unfair profit can refer both to the perpetrator of the conducts or to a subject different than the him. In fact, the rule of art. 143/b, referring to an unfair profit procured 'to oneself or to others', expressly admits the criminal relevance of the hypothesis in which the achievement of the profit is attributable to third parties and not only to the offender.
On the nature of profit, the profit obtained through the commission of the crime of fraud (and therefore also of that of computer fraud), necessarily have an economic

nature because the Albanian legislator has excluded other kind of profits as moral of affective ones.

2.3 The legal and material object[9].

The juridical object protected from the crime of computer fraud cannot be seen exclusively in the circle of protection of property, despite the fact that the legislator has placed this crime at the chapter of the offenses against property and in the economic sphere. But it would be necessary to clarify that the secondary object provided by this provision is also the need to maintain the regularity of the operation of IT systems, as the computer system usage is increasingly widespread and usable in all important sectors of economic life, social and institutional of the country, with a focus on protecting the confidentiality of data.

Article 143 / b mentions a series of interests and relations that must be protected, which are also indirectly included in the structure of the criminal offense, which has special features in the field of all figures of the criminal offense of fraud provided by the criminal code or special laws.

Therefore, the provision mentioned in Article 143 / b of the Criminal Code undoubtedly constitutes an autonomous figure of the crime. But it is equally indisputable that in addition to the common features on the various figures of "deception", one must take into account the specific characteristics that characterize, even at a "technical" level, the particular "object" over which it appears the deceptive behavior. Therefore, it is worth mentioning the repeated assertion that the crime of computer fraud differs from that of fraud, because the fraudulent activity of the perpetrator does not involve a person, but the computer system belonging to the same, through its manipulation.

In order to clarify the scope of the conduct referred to in Article 143 / b of the Criminal Code, it is necessary to define precisely the notions and characteristics, of the "computer system" on which the operations are performed and the data of information or programs "on which the author intervenes. The legislature has tried to clarify the typical behaviors that distinguish it from traditional fraud in two different formulations, which can occur "in any way" and "by any way", and leaving a wide interpretation of these behaviors, to be adapted case by case.

Indeed, the provision also presents some features, in relation to the legal provisions of many other countries, such as the provision of a general notion of the "computer system" and the "data processing ". First, regarding the notion of "computer system", it should be noted that it is a quite general concept, capable of any system used for automated data processing that uses information technology.

The question may naturally arise if the computer system can include only personal computers? By computer systems, in fact, we mean any type of computer system of any type and size, including in this sense as writing systems for individual use or not,

and complex data processing systems capable of providing computing services and power for thousands of users, in "the whole national territory or even beyond the borders of the country".
The computer system includes "the total devices intended to perform any function useful to humans through the use (even partial) of information technology". According to this definition, the term "computer system" is extremely broad and includes a computer even in the traditional sense (home computer, monitors and any peripherals), which will be applied whenever there is a manipulative behavior in a device that performs an organizational and content processing function in an automated manner, regardless of its size.
Even according to the Albanian practice[10], a computer system also includes electronic devices that supply goods or services or ATMs on withdrawing money, or even a certain category of phone such as a smartphone. The reason why all these cases are included in the notion of computer system has to do with the effect that in these devices data processing is done, and the processor installed in them is able - thanks to the instructions given - to screen the user's legitimacy to receive the service, process received command, and possibly can modify, delete, or add custom functions. Therefore, it is appropriate to mention the decision of the High Court No. 30 dated 26.01.2012, where a POS terminal for making payments by customers through electronic cards cloned without electronic tape and not issued by banking services, will be considered a computer system.

2.4 The subjective element of this criminal offense.
Art. 16 of the criminal code establishes that "No one can be punished for a fact foreseen by the law as a crime, if he has not committed it with willful misconduct". In other words, with this provision the legislator has provided for the general rule according to which willful misconduct is the psychological element of crimes. Therefore, with reference to crimes, guilt and intentions can integrate the psychological element of the crime only where the incriminating law expressly provides for it. However, as regards the degree of criminal intent, the case provided for by art. 143/b of the Criminal Code it is compatible, by the very nature of the crime, both with intentional willful misconduct and even more so with premeditation.
The same can be said in reference to indirect willful misconduct (in which the subject represents himself as highly probable, if not certain, the outcome of his own conduct). On the compatibility of the crime of computer fraud with potential fraud (which constitutes, for those who make this further distinction, a very mild form of indirect fraud, characterized by the fact that the subject, representing the event of the crime as probable, or even as merely possible, he does not want it but accepts the risk of verification), it is observed that the specific context (the computer-virtual one) in which the criminal conduct is carried out suggests the opposite conclusion. And, in

fact, if, for example, one thinks of the behavior of altering the computer system and the scarce possibility of failure that it presents, one does not see how the offender can represent the outcome of such conduct as only probable or even merely possible, ending up replacing one's criminal will with the mere acceptance of the risk-crime.
Finally, the compatibility of the case of computer fraud with *specific fraud* must be excluded, given that the provision of art143/b of the Criminal Code, in omitting any express reference to the specific purpose to which the criminal conduct is addressed, requires only the existence of generic intent.

2.5 Time and place of committing, consumption of the computer fraud.
Article 76 of the Criminal Code has defined general rules regarding territorial jurisdiction, and it is provided that territorial jurisdiction is determined first by the place where the criminal offense is committed or where it was attempted to be committed or the place where the consequences have come[11].
In the conditions that a criminal offense is considered committed where the action or omission has been taken, even for the criminal offense of computer fraud, as a place of its commission and consumption will be considered where the subject has interfered in the computer function or has intervened computer data, regardless of where the central computer may be located.
Even computer fraud is consumed the moment the perpetrator obtains the illegal benefit, causing the reduction of wealth.

2.6 Qualifying circumstances and punishment.
The qualifying circumstances provided for the criminal offense of computer fraud are foreseen in four forms: when committed in collaboration, to the detriment of several persons, more than once or when it has brought severe material measures, providing for a relatively sanction determined from five to in 15 years imprisonment[12].

3. The difference between computer fraud with other figures of the Criminal Code.

In the course of this discussion, reference has been made more than once to the crime of fraud in relation to that of computer fraud. This is why a comparative analysis of the two rules is proposed aimed at highlighting the differential elements as well as those in common between the cases described respectively by Articles 143 and 143/b of the Criminal Code[13]. In this way, we will try to understand whether the crime of computer fraud constitutes a special case with respect to that of fraud or if, in fact, it should be considered as an autonomous crime. And with reference to this aspect, it is necessary to ask about the existence of a relationship from species to genus of the case of computer fraud compared to that of fraud. The doctrine is divided on this point. In

fact, according to a certain orientation, the crime envisaged by art. 143/b of the Criminal Code would constitute a hypothesis of a special crime compared to the general one of Fraud. However, this assumption cannot be accepted since the case of art. 143/b of the Criminal Code, with respect to the crime of Fraud, presents elements of autonomy such as to make it structurally impossible for the existence of a specialty relationship between the two criminal offenses. In particular, with respect to the case that governs the Fraud, in art. 143/b there is no reference to a bonded conduct, put in place, that is, by means of artifices or deceptions aimed at misleading the taxable person (or other third party) and making him carry out an act of asset disposal that otherwise would not put in place. And in fact, it should be reiterated, in the case of computer fraud the offender, far from misleading someone, in engaging in a free conduct (of alteration of the functioning of the computer or telematic system or of abusive intervention on data, information or programs in it contained), directs its fraudulent conduct directly on the computer or telematic system. And, therefore, the events of unjust profit and the damage of others derive directly from this conduct.

3.1 The concurrence of computer fraud and unauthorized interference in the information or telematics system, computer forgery[14].

The Albanian jurisprudence has distinguished computer fraud and unauthorized access to a computer system and has established, that the two crimes differ significantly and for this reason, they can formally concur together. Indeed, both the protected legal assets and the sanctioned conduct are divergent: the abusive access protects the computer domicile under the right to exclude others profile, while the computer fraud concerns the alteration of the data accumulated in the system for the purpose of perceiving an unjust profit. Moreover, the provision of the possibility of committing the crime of unauthorized access, the manipulation of the system is not required in the conduct of abusive access, because this is an element that characterizes computer fraud.

4. Conclusions.

In light of the considerations made upon, we can affirm that, computer fraud represents a concrete risk to Albania. It would therefore be appropriate for the Albanian legal system, given the continuous evolving technologies and their constant and almost, by now, necessary use in everyday life, prepare legislation that knows how to prevent, with adequate security barriers, cyber-attacks and, if necessary, take action promptly with technical measures when the first signs of massive violations show. The actual legislation is not sufficient to handle the new forms of computer fraud. In order to achieve this aim, it would therefore be useful, on the one hand, to have a larger one awareness and information, in order to provide adequate

knowledge of risks that can be run with the use of technological tools, on the other hand, a greater harshness of the penalties, in order to discourage computer hackers from placing criminal conduct in place. It would therefore be desirable for the legislator to revise the legislation on computer crimes, by providing for further specific provisions, an increase in penalties for these crimes that are now part of the new net-centric society and the inclusion of a new title in the penal code dedicated to them.

The existing legal and institutional framework has some ambiguities, which need to be addressed when completing the legislation, as modernization of the legislation and its periodic review to address cyber security related to the developments of cyberspace in Albania and harmonization with international legislation, in order for it to remain appropriate and effective. The current provisions are systematically distributed in different chapters and sections of the Criminal Code. This is due to the main criteria on followed for structuring the provisions in our criminal code, of the legal object and in order to this context, to facilitate the practical implementation and increase their effectiveness, it would be good for such criminal offenses to be included in a special law. Referring to Law no. 10023, of 2008, by which new provisions on cybercrime were included in our criminal code, should pay attention to the theoretical explanation of the circumstances of the implementation of the relevant provisions, as well as the illustration of practical forms, in which violations may be committed in order to avoid any ambiguity in the meaning and proper application of these provisions.

Artificial intelligence-based crimes: Are we heading towards an AI crime dominated future?

Ina Veleshnja Msc. –Elira Kokona Ph.D (cand.)

1. Introduction

When people think of artificial intelligence (AI) they immediately think of sci-fi movies in a distant future, where robots are the norm. However, as it turns out this distant future, that is being showed in cinematography, is not that distant after all, one could even say that it is happening now and we are living it, or rather have been living it for quite some time.

In 1996 a number of chess games were conducted by then chess world champion Gary Kasparov and a computer called "Deep Blue". Kasparov both won and lost against the machine, making headlines around the world and becoming the subject of documentaries and books. "Deep Blue" was a machine or rather an AI that could follow up commands and actually manage to beat in a chess game a world champion. Why is this story incredibly important and inspiring at the same time? Well the answer is simple. A man-made machine can perform tasks that are exclusive to human beings. Almost having an autonomous personality. Autonomy means different things in different contexts. In engineering autonomy means the possibility of a machine to operate without the help of a human being. In philosophy it means the ability to have a "conscience" and to act accordingly upon that. So, having autonomy is really a very important subject especially when we are talking about man-made machines that can beat world champion chess players.

Nonetheless, considering these incredible scientific and technological advancements, countries around the world are trying to regulate AI in an ethical way. At the time of writing of this paper, there are not many consolidated bodies of legislation that regulate AI around the world, but different countries are trying to come up with appropriate legislation and start building a "legal watch tower" over a fairly unexplored area of interest.

In February 2020 the European Commission proposed a white paper on "Artificial Intelligence – A European approach to excellence and trust"[1]. The aim of the paper was to encourage debate in all of EU member states, academics, civil society

[1] EU Commission white paper (2020): "On Artificial Intelligence - A European approach to excellence and trust" https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

and more on the ethical and proper usage of AI. Obviously, the European Commission wants to give a broad picture of AI, especially focusing on the benefits of AI, and why it is very important for citizens of all of the EU member states to know of this approach and how it can affect their lives. As it is known, white papers are the first step for the EU in coming up with legislation. A draft Regulation on Artificial Intelligence has been proposed by the European Commission, trying to pave the road for a legal, ethical, and safe usage of Artificial Intelligence in the European Union Member States.[2]

In spite of all of these legal initiatives we have yet to see a consolidated body of law that regulates AIs, as an autonomous subject of the law, which in turn requires a lot of careful planning by the lawmakers of every country in the world. On the other hand, there have also been cases of usage of AIs in illegal scenarios, making the whole process very complicated and equally dangerous for their victims. Besides being used to commit crimes, AIs have actually been used also in other cases around the world. One such example is the usage of armed drones, in war zones. There are a number of examples where AIs have been used for missions in warzones around the world and have raised a number of ethical questions. Can machines like these functions in accordance with international law? What ethical aspects are being put at risk in war-torn countries? And more importantly, how do they contribute to the loss of human and moral virtues in such cases? These are just a few of the questions that are being raised in these cases.

The following paper will try to divulge in the different methods/means on how artificial intelligence can be used to commit different type of crimes, ranging from impersonating someone to committing terrorist acts (Part one). The second part of the paper will focus on machine learning, how it does affect law (Part two) and lastly, we shall have a look on the ethical usage of Lethal Autonomous Weapons, also known as *LAWS*, in war zones. The paper concludes with some thoughts on the legal and ethical usage of artificial intelligence and what can be done by law enforcing agencies and lawmakers in order to better regulate the vast world of AI.

2. AI and criminality

2.1. How can artificial intelligence be used to commit criminal offenses?

Artificial Intelligence can be defined as a wide range of smart machines that can perform a multitude of tasks. When we say a multitude of tasks, we mean everything that involves or "typically require human intelligence".[3] In other words, if fed enough data, or given enough technological improvements, these machines can perform in ways almost similar to the human mind. Theoretically speaking AIs can potentially substitute humans altogether, in every field of life and since the day of this happening is not as farfetched as we would like to think, the criminal world is already making use of such technologies, to achieve their criminal intents.

[2] EU Commission proposal for a "Regulation of the European Parliament and of the Council, Lying Down Harmonised Rules on Articifial Intelligence (Artificial Intelligence Act) and Amending certain union legislative acts https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

[3] Built in "Introduction to AI" https://builtin.com/artificial-intelligence last accessed 20.10.2021

Many authors have tried to explain these phenomena and usually the mutual consensus is that since we live in a world that is highly connected, so will be also crime.[4] This means that our digital devices are connected with each other and as such, threats of cybersecurity and other such issues have been also increasing steadily. It is unimaginable that in today's world, a person does not have access to the internet or is not in possession of at least a single smart device. In this intricate web of connections from one side of the globe to the other, it is natural that crime and criminality will adapt to this new network, in order to achieve their criminal intent and secure the products of their illegal activities.

A. Deep fakes

When it comes to using Artificial Intelligence to help facilitate crimes the most common types are the ones that help to create a false perception on a specific situation. The most usual ones, are audio and video impersonation. These types of crimes happen, for example, when there is a cybernetic attack on the business email of a company. After a successful breach the perpetrator might impersonate a CEO (or other senior executive), of said company, in order to make the employees of the company authorize false payments or transfer of funds.[5]

The impersonation is so realistic that an employee has a genuine difficulty in realizing that they are falling victim of a very sophisticated scam. All the documents are very realistic, and when trying to personally contact the senior executive that gave the order to transfer a certain amount of money to a specific bank account, the voice, mannerism is also very highly duplicated, making it virtually impossible to detect that there is indeed something wrong.

Another way audio impersonation can occur is with the help of "deepfake audio". The best way to define a "deepfake audio" would be the cloning of a human voice that is potentially indistinguishable from a normal voice, through synthetic audio.[6] The technology used in such cases is so advanced, that the person being scammed has absolutely no idea they are talking to a criminal and will deliberately share all the details and information that have been requested.

Deepfake audios, are perhaps the most dangerous and sophisticated means of impersonating the voice of someone. In 2019, an energy firm from the United Kingdom was scamed out of 220.000$ from a call using deepfake audios. This incident is one of the first incidents believed to be related to deepfake AI technology cybercrimes in Europe.[7]

As impressive as the technology really is, it is equally impressive that we haven't come up with a clear set of solutions or softwares to detect and counter these

---

[4] Wilner, A. S. (2018). Cybersecurity and its discontents: Artificial intelligence, the Internet of Things, and digital misinformation. *International Journal*, *73*(2), 308–316. https://doi.org/10.1177/0020702018782496

[5] Ikeda, S. (2019). The cutting edge of AI cyberattacks: Deepfake Audio used to impersonate Senior Executives" https://www.cpomagazine.com/cyber-security/the-cutting-edge-of-ai-cyber-attacks-deepfake-audio-used-to-impersonate-senior-executives/

[6] Johnson, D. (2020). Audio Deepfakes: Can anyone tell they're fake? https://www.howtogeek.com/682865/audio-deepfakes-can-anyone-tell-if-they-are-fake/#:~:text=An%20audio%20deepfake%20is%20when,used%20to%20produce%20synthetic%20audio.&text=Additionally%2C%20because%20so%20many%20voice,be%20made%20even%20more%20indistinguishable

[7] Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

cases. Law enforcement agencies have a lot of difficulties on combating cybercrime and that happens potentially for two reasons. Firstly, technology evolves at a higher pace than our law enforcement agencies can adapt. Secondly, in order for a tech company to work and create a software that would potentially tackle deep fake audios or audio/video impersonations, they will need to have governmental incentives and/or legal guidelines that would direct the discourse directly to the problem and trying to come up with a solution for it. Basically the need for specific regulations is highly needed, especially when it comes to governmental guidelines and incentives.

B. Self-driving vehicles (potentially being) used in terrorist attacks

Another type of AI-related crime can be linked to driverless vehicles. At the time of writing of this paper, driverless vehicles aren't the norm (yet), however with the current technological advancements it won't take too long for these types of vehicles to become a part of our daily lives.

Tech companies such as Tesla have been producing driverless vehicles or completely self-driving cars quite a few years now. These vehicles can be used by terrorist groups to commit terrorist attacks all over the world. In 2016 attacks in Niece, France the ISIS didn't employ any bombs or sophisticated robots for their attack. They used a very ordinary white truck that had been rented a few days before the attack, which was then used to kill 86 people and injure hundreds more.[8] So the hypothesis in this case is that, in the not-so-distant future terrorist act committed with the help of self-driving vehicles is far from fantasy.

These vehicles are intelligent enough to drive you around, avoid heavy trafficked roads, self-diagnose if they have mechanical issues and even order parts for themselves online. In other words, these vehicles can replace the human driver almost at full capacity. What happens, however, if the vehicle is used by a terrorist group(s) to commit acts of terror worldwide? Ideally speaking, the self-driving car doesn't need a human at all to function at full capacity, so it can (potentially), be used in coordinated terror attacks. Companies that produce these types of vehicles need to have outstanding technology to "kill switch", vehicles in hypothetical cases such as the one described above. On the other hand, we need clear legal guidelines that have to regulate self-driving cars and how to use them in a trustworthy and safe way for ourselves and our community.

C. Malware installation in order to procure information

As the name suggests these types of crimes are related to the installation of malware in digital devices, in order to gain information that might be profitable to the people involved. Usually these types of crimes happen when, someone receives a very "believable" message from a bank or other financial institution. Believing that this message is genuine the person falling for this scam might reveal sensitive information such as passwords, security questions etc, information that otherwise would not be disclosed. Artificial Intelligence could be used in such cases to create even more believable messages, thus resulting in a large-scale extortion.

[8] Nice attack: What we know about the Bastille day killings (2016) https://www.bbc.com/news/world-europe-36801671

3. Machine learning and their constant "battle" for autonomy

Since the dawn of social media, everyone working in giant technology companies such as Facebook, Google, Instagram, You Tube and more, had only one main purpose: How to use new technologies and make profits out of them. It quickly became clear that the best way to make a profit out of non-charging internet services like social media, was to keep people entertained and have them spend as much time in front of their screens as possible. In other words, the profit these companies were trying to achieve is our basic human attention span. The more time a person spends on their phones checking their social media accounts, the more "feeding the machine" happens.

Basically, the AI algorithm behind the content being circulated on social media, will try to make the basic user spend as much time on social media as possible. The efforts to do this go to the extremes and social media platforms, work tirelessly in order to create new and improved ways in order to make people stay.

As time went by, the social media AI got so sophisticated through the process of machine learning that even to this day, senior executives in these platforms have no idea how it is going to maneuver content to be appealing to their users.[9] Social media AI is taking a life on its own, trying all the time to appeal to the users, keep them entertained and keep them scrolling.

So, what happens when social media is used to manipulate and radicalize people into making extreme acts in their daily lives when AI are becoming such a determining part of it?

Unfortunately, this scenario as far-fetched as it might sound has become a reality a number of times. AI that were created to keep our attention in whatever social media of our choice, "realized" that content related to conspiracy theories, was the content that kept our attention more on the screens. So, it started suggesting more and more content like that, resulting in an increased number of radicalized individuals that shared these "fake news" and then lead to violence acts.

The most famous yet unfortunate episode of social media radicalization is the Capitol insurrection in Washington DC, USA. As it was later discovered a lot of people that took part in the insurrection on January 2021 and that were later arrested, had all been regular believers in QAnon, a far-right organization that spreads conspiracy theories and misinformation. All the people arrested and charged for the insurrection had in common QAnon. They had all been following the organization online, in the corners of the world wide web, and when finally, the time was "appropriate", they stormed the Capitol, resulting in 5 deaths, a great number of damages and theft of personal electronic equipment of Congressmen.

Numerous studies have been conducted on the spread of misinformation on the internet. What has been concluded is that fake news spreads at least 6 times faster than "true news". "Fake news" is 6 times faster or rather 6 time more at advantage as compared to true news. This conclusion was achieved by an MIT study from 2018[10]

[9] For more information please access https://www.thesocialdilemma.com/, last accessed 30.03.2021

[10] For more information please access https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308 , last accessed 30.03.2021.

on "true news". It turns out that "true news" takes roughly 6 times longer to reach 1500 people, compared to fake news.

The above numbers depict quite a depressing scenario. We saw how social media can brainwash people, yet there is still a lot that needs to be done in order control and regulate these very problematic occurrences.

Appropriate legal measures need to be introduced in order to regulate the spread of completely false information on social media and also appropriate measures need to be taken when it comes to the usage of AI in these platforms. Every company's final goal is the maximization of profit, that is one of the foundation principles of business, however what do these big tech companies need to do when their platform is used to spread messages of hate or violence? A bigger vigilance should be conducted by the "human factors" of these platforms, so that if the content that is being recommended by the AI is dangerous or harmful, it has to be removed from the platform entirely. Everyone that possesses an account that is used for these purposes, should be banned for life, reported to the police, etc. These are but some of the measures that can be pursued, nonetheless big tech companies can find even more innovative ways to secure their platforms from such harmful messages and also not infringe their profits along the way.

3.1. AI in court proceedings

Automated systems have been used in since the early 90s in the USA. More specifically, these systems are used in court proceedings, to evaluate defendants (that are accused of a certain crime)[11], on how likely they are to reoffend. After being done with the evaluation, the automated system then scores the defendant a certain amount of points. If the defendant scores high, that means they are highly likely to reoffend the same type of crime again in the future. If they score lower than the threshold established, the defendant is considered (very) unlikely to reoffend the same type of crime in the future. This evaluation can then be taken under consideration by the court when deciding the final sentence of the defendant. This process does rise a few eyebrows, considering that the evaluation is done solely by the automated system and the score is given out by the automated system. No human factors are part of this process (besides the engineers that created the system in the first place), and the defendant themselves. The question raised here is, can a machine actually administer justice? How fair can it be? How ethically can it behave? And more importantly, how can we make sure that there is no violation of the basic human rights and procedural rights during this whole process?

In the case *Loomis v. Wisconsin*[12], the judge gave a harsher sentence to Loomis since the automated system[13], evaluated Mr. Loomis with a high potential for recidivism and such he was denied the possibility of parole. Mr. Loomis challenged this decision and required a copy of all the data, scores and questions done during the evaluation by the automated system. He argued that taking a decision in such cases, violated his constitutional right for a due process. However the Wisconsin Supreme

[11] Considering the type of crime, there are a number of automated systems that are specialised in a certain crime. For example sexual crimes have a different automated system than crimes against property etc.
[12] Loomis v. Wisconsin https://harvardlawreview.org/2017/03/state-v-loomis/ last accessed 19.11.2021
[13] COMPAS CORE "Assessment and case planning" http://www.northpointeinc.com/files/downloads/Risk-Needs-Assessment.pdf last accessed 19.11.2021

Court, argued that Mr. Loomis right for a due process was not violated (even though the methodology used for assessment wasn't disclosed neither to the court nor to Mr.Loomis), since the court decided on additional factors too, and not only on the assessment of the automated system. This is a very important case regarding AIs in court proceedings. AIs are being used as tools helping in determining recidivism based on metadata and machine learning.

The Loomis case was one of the first, and surely enough courts around the world will follow suit and start using these systems in their decision-making process. It is imperative that the systems be fed unbiased, ethical and reasonable metadata, so that the defendant can be evaluated as objectively as possible. Also, the court should taken into account other factors too and not only the recommendation of the automated system when deciding the fate of the defendant in criminal proceedings. A human needs to give the final verdict in sensitive cases such as criminal court proceedings. Contrary to the US experience, in the EU article 22 GDPR gives the right to a data subject to object to a decision based solely on automated processing which produces legal effects concerning him or her or significantly affects him or her. This provision could limit the use of AI in Court proceedings unless this is explicitly authorized by Union or State law or there is the explicit consent of the data subjects.

4. Ethical aspects of "Lethal autonomous weapons systems" *LAWS*

"Lethal autonomous weapons systems" also known as LAWS, are armed weapon systems that will engage in combat in war zones. These machines can operate on land, air, water, under water and even in space. The machines are capable of adapting and learning the environment they are operating, as well as opening fire by their own initiative.[14]

It is safe to say that this type of autonomy rises quite a few ethical concerns. The first one being the proportionality and distinction. Can machines that are programmed to kill a specific target manage to uphold the proportionality and distinction principle? There is a great debate on LAWS, with many discussing that since these are machines it is easier for them to uphold ethical principles during times of war, and others stating that this is not entirely true, and arguing that machines do not possess any moral compass and as such it is very difficult for them to make ethical decisions during war times.

Author Heather M. Roff argues that LAWS undermine the principle of proportionality in times of war. The argument that machines can be used because they are capable of conducting a "clean killing", as in trying to defend from the enemy is a very far-fetched thought, since there is no clean killing in war.[15]

Various international organization with a focus on human rights, have appealed to governments worldwide against the usage of LAWS, because it seriously breaches international laws on war. Using LAWS in war is not always a proportional

[14] Roff.M.H (2015) "Lethal Autonomous Weapons and Jus Ad Bellum Proportionality", https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1006&context=jil

[15] See Roff. M. H (2015) "Lethal Autonomous Weapons and Jus Ad Bellum Proportionality", pages 11-13 https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1006&context=jil

mean to the threat at hand. Since we are talking about autonomous machines that will conduct killings according to a program, this can result in a number of issues. Firstly, civilians are at a high risk from LAWS. There have been numerous reports of civilians being caught in the fire from a LAWS operation. Secondly, LAWS can (potentially) be hacked. This is a highly dangerous situation as it creates a premise for these very sophisticated weapons to fall on "bad hands", posing an incredible threat to everyone. However, the biggest threat that comes from LAWS is a potential AI global race.[16]

If one country makes the necessary technological advancements to produce substantial developments in LAWS, other countries will try to make advancements in this field so that they aren't left behind, thus creating a global AI race. The repercussion of a global AI arm race is almost dystopian. If it were to happen, it would mean that our world would not be the same anymore. The world has already changed 3 times when it comes to weapons systems: first with the invention of gunpowder, second with nuclear weapons and third with a potential AI arm race.

Many countries worldwide are against LAWS in general, as the negatives outweigh the positives. However, there are also a great number of countries, global superpowers that think differently. At the moment we can only hope that an Artificial intelligence race war, is just a far-fetched concept and we can be prevented from ever occurring in the future.

5. Conclusions

Criminals are using AIs to facilitate their illegal operations. Through the help of these automated systems it is becoming clearer and clearer that lawmakers and law-enforcement authorities around the world are in dire need to catch up with them.

Alternatively, when it comes to automated systems that can potentially replace human beings altogether, the effects bypass the traditional human rights. Using automated systems in court proceedings, has been going on since the early 1990s. It still has to overtake every court room in the planet, yet there are clear signs that it will happen, sooner or later. In the meantime, we have to regulate the automated systems, so that there won't be issues that violate basic human rights, like due process, presumption of innocence, etc.

Artificial Intelligence has also found its usage by the military. Using AIs to surveil, target and open fire related to a specific target, has raised a number of issues regarding fairness and proportionality of war. These weapons should be better regulated and used only when they are really and truly needed. If we start to routinely use them for every conflict ever, there are premises of crimes against humanity being consumed.

[16] See Ariel Conn "The risks posed by lethal autonomous weapons" https://futureoflife.org/2018/09/04/the-risks-posed-by-lethal-autonomous-weapons/, last accessed 06.04.2021.

Corporate and Criminal Law in syndemic scenario in the Italian Jurisdiction: False Statements and "Stellionatus"

Andrea Pantanella Ll.M.[1]

1. Introduction - The Italian System coordinates: from the new Bankruptcy Code to the corporate financing system

"*…I intend to relate one hundred tales or fables or parable or stories -- whichever you choose to call them -- as they were told in ten days by a band of seven ladies and three young men during the time of the recent plague, and also certain songs sung for their delight by the said ladies…*".[2] Such a metaphor being allowed, Decameron's young storytellers, leaving Florence to escape the spreading plague and gathering in an old inn telling novels to each other, may well represent Corporate and Criminal Law expert's isolated position. Scientific debate has justifiably looked elsewhere: strictly referring to the field of law, attention has been focusing on the crucial balancing between right to health and (limitations to) personal freedoms; or on the inmates' wretched situation in detention centres; or even on the undefended positions healthcare professionals are bound to work in.[3]

Actually, as is sadly known, present scenario is characterized by the spreading of Covid-19 pandemic which, what is more, is hitting social communities already dramatically affected by a long-lasting economic, social and environmental crisis.

In this difficult syndemic framework, Corporate and Criminal Law experts are also called upon to give their contribution. Undoubtedly, a particularly complex and challenging task. Their difficulties were pretty blatant even before coronavirus spread worldwide: they were basically requested to act as "tightrope walkers", pushed by the outdated Bankruptcy Law (R.D. n. 267/1942) on one side and by the problematic entry into force of the new Bankruptcy Code on the other. Today this task is further complicated by the impending new and even more serious economic crisis connected with Covid-19 pandemic.

Different fields of study are consequently increasing in number: corporate and bankruptcy criminal law state-of-the-art; aspects of criminal law liability, with reference to funding ensured to firms by Decree Law n.23 of 8 April 2020, the so called Decreto Liquidità; possible criminal law liability models able to effectively react to the major obstacles the Criminal Law of Economics will soon have to face, deriving in particular to corporate crises.

[1] Temporary research fellow at Sapienza – Università di Roma
[2] Giovanni Boccaccio, *The Decameron*, tr. Richard Aldington
[3] Castronuovo, *Modelli causali o medelli precuazionali*, in *La Legislazione penale*, 10 maggio 2020.

As for the first field of study, it is necessary to identify the actual extent of the new Bankruptcy Code within the criminal side of the matter. As is known, in order to face the "*ante*-pandemic crisis", the Legislator made the decision to reform existing legislation in this area by introducing the new Bankruptcy Code.[4]

Despite the heralded intention not to affect Bankruptcy Law in terms of criminal law aspects, the Legislator-reformer has quietly introduced important amendments, among which those concerning Crimes of False Statements, resulting in the creation of an actual mini-system and in the enhancement of the legally protected right of correctness and accuracy of company information.

As for the second field of study, in light of the fact that the so called "Decreto Liquidità" failed to introduce specific types of crimes, it is necessary to clarify which crimes already provided for by Italian legal system are to be considered relevant in this context. A first answer might be represented by False Statements Crimes committed by entrepreneurs for the purpose of receiving funds granted by the State and guaranteed by SACE; different conclusions could be reached when considering as relevant more serious crimes, such as Misuse of Public Subsidies Crime and Aggravated Fraud Crime.

As of the third field of study, the analysis will focus on the present system resilience to the impact Covid-19 pandemic will have on today's already strongly compromised economic system. On the one hand, *de iure condito*, it is necessary to examine the ways through which the system, although hesitant and defective, could resist. On the other, *de iure condendo,* a general reform in this area is to be taken into consideration in order to ensure more updated incriminating patterns compliant to the Italian Constitution principles, as well as to those established by the European Union and the European Convention of Human Rights.

2. Effects on False Statements Crimes deriving from the introduction of the new Bankruptcy Code

2.1. Amendments concerning False Statements Crimes and removal of criminal liability in connection with the economic feasibility assessment

In this regard, it should be mentioned the memorable reform which through Legislative Decree n.14/2019 led to the introduction of the Bankruptcy Code.[5] It is worth noticing that the introduced amendments have only regarded the civil aspects, leaving criminal aspects essentially unchanged: as expressly established by the so called Legge Delega n. 155/2017 "relevant criminal provisions should be adapted only in terms of vocabulary, without prejudice to the very substance of crimes". The Legislator's intent was to further amend the system of corporate crisis settlement procedures, avoiding to affect criminal law issues.

---

[4] LO CASCIO, *Il codice della crisi di impresa e dell'insolvenza: considerazioni a prima lettura*, in *Il fallimento*, 2019, p. 263 ss.; D'ATTORRE, *Prime riflessioni sulla delega al Governo per la riforma della disciplina della crisi di impresa e dell'insolvenza*, in *Riv. soc*., 2017, p. 519 ss.; RANALLI, *Le procedure di allerta e di composizione assistita della crisi: insidie ed opportunità*, in *www.ilfallimentarista.it.;* STANGHELLINI, *Il codice della crisi di impresa: una primissima lettura (con qualche critica)*, *Il Corriere giuridico*, 4/2019, p. 449 ss.

[5] GAMBARDELLA, *Il codice della crisi di impresa: nei delitti di bancarotta la liquidazione giudiziale prende il posto del fallimento*, in *Cass. Pen*., 2019, p. 488 ss.; ALESSANDRI, *Novità penalistiche nel Codice della crisi d'impresa*, in *Riv. It. Dir*., 2020, p. 1821 ss; CHIARAVIGLIO, *Le innovazioni penalistiche del Codice della crisi di impresa e dell'insolvenza: alcuni rilievi critici*, in *Le società*, 4/2019, p. 445 ss. CAVALLINI, *La bancarotta patrimoniale tra legge fallimentare e codice dell'insolvenza*, Cedam, 2019.

Needless to say that, given the close connection between crimes and bankruptcy procedures, this target could not be fully achieved because the amendment of the latter could not fail to affect the former leaving them unaltered. Changes have consequently occurred, as one might well expect, both directly and indirectly (with certain concerns regarding their constitutionality).

Before analysing the amendments concerning false statements crimes, it is worth mentioning two major changes of a general nature:

i) firstly, the elimination of the term "fallimento" (bankruptcy) replaced by the sentence "liquidazione giudiziale" (liquidation by court order);

ii) secondly, the new definition for "State of Crisis", which represents the Arrangement with creditors basic prerequisite, as the "state of economic and financial difficulty making debtor's insolvency likely" and later, based on Decree-Law n.147 26 October 2020 (Amending Decree), as the "economic and financial imbalance making debtor's insolvency likely".

In fact, both amendments are likely to bring about an actual shift in the whole matter perspective, together with practical changes. Consider just the fact that with the elimination of the term "fallimento" (bankruptcy) it should no more be correct to say "bankruptcy crimes"; it can be taken as a provocation but, as a consequence, it would be more correct to refer to them as "corporate crisis and insolvency crimes".

Moreover, the decision to make a definitely clear distinction between State of Crisis (prerequisite for the Arrangement with Creditors) and State of Insolvency (prerequisite for bankruptcy/liquidation by court order) has important implications, too.

The new Bankruptcy Code (art. 2, par. 1. (a)) defines the term "crisis" as the "economic and financial imbalance making debtor's insolvency likely to occur, which manifests itself in form of a corporation prospective cash flow inadequacy to meet its planned obligations on a regular basis", whereas art. 160, par. 3, Italian Bankruptcy Law, merely provided that "State of Crisis means also State of Insolvency".

As for the Legislator's inertia towards Criminal Law aspects of Bankruptcy Law, it is worth noticing that False Statements crimes are one of the very few aspects the Legislator seems to have been focusing on. So true is it that within the new Code one may see sort of a "mini-system" of False Statements Crimes. Crimes regulated by art. 341, 342, 344 and 345 of the new Bankruptcy Code can be considered in this perspective.[6]

As already mentioned, the delegating Legislator's aim was to avoid modifying criminal offences, except for necessary adjustments connected to the introduced amendments to bankruptcy procedures. Apparently, such an intent has been kept with only referring to the new art. 341 of the new Bankruptcy Code regulating False Statements Crimes to gain access to the Arrangement with Creditors procedure or to debt restructuring or moratorium agreement procedures, given that it has basically the same scheme as art. 236, par. 1 of Bankruptcy Law.

Actually, minor changes were made, but they were not substantial. The same cannot be said about the new art. 342 new Bankruptcy Code regulating False Statements Crimes committed by professionals, within which, along with the introduction of new cases, possible future action of abolishing nature (*abolitio criminis*) seems even to emerge.[7]

[6] CHIARAVIGLIO, cit., p. 445 ss.

[7] PANTANELLA, *Professionista attestatore e responsabilità penale: la dimensione "temporale" e "spaziale" dell'art. 236-bis l.fall.*, in *Cass. Pen*., 2019, cit., p. 802 ss.

Unlike art. 16, Law n. 3/2012, art. 236-*bis,* Bankruptcy Law, does not specify which are the relevant types of statements to be considered as criminal offences. In particular, failure to give such information has traditionally led to believe that professionals could be charged with False Statements and Reports Crimes when the relevant conduct had as its object statements or reports concerning both data truthfulness and economic feasibility.[8]

In fact, compared to the wording of art. 236-*bis* Bankruptcy Law, in art. 342 of the new Bankruptcy Code, the Legislator decided to further describe the professional's conduct to be considered criminal providing for his/her criminal liability when omitting to report relevant information or when reporting false information "with regard to the truthfulness of data contained in the crisis plan proposed by the entrepreneur or in the attached documents".

According to such crime new wording which excludes the economic feasibility assessment, criminal conduct would consequently be limited only to the data truthfulness assessment; in other words, an actual partial *abolitio criminis* resulting in the application of art. 2, par. 2, Italian Criminal Code would seem to emerge.[9]

This regulatory option appears to be clear and precise and its *ratio* may lie in the knowledge that the economic feasibility assessment represents an actual evaluative statement and, as such, cannot be strictly considered false or true, as opposed to descriptive statements.

However, such deliberate decision by the Legislator, although "abstractly" reasonable, should be considered "concretely" unlawful in terms of constitutionality: the delegating law ("*legge delega*"), in fact, did not provide for anything about it, giving rise to legitimate doubts in terms of excessive delegation.

2.2. The new crimes in terms of False Statements in debt discharge procedures and in terms of False Statements by members of the corporate crisis settlement panel (Organismo di Composizione della Crisi di Impresa, OCRI)

The following analysis focuses on the new crimes referred to in arts. 344 and 345 new Bankruptcy Code, namely "False statements Crimes in debt discharge procedures" and "OCRI members' False Statements Crimes".[10] The former crime may actually be considered not entirely new, in that it partially reproduces art. 16 of the Act on Over-indebtedness.

In this respect, however, it is worth noticing that the Article second -paragraph represents in fact something new, in that law punishes the insolvent debtor who submitted false or altered documentation in order to use the debt discharge procedure (or afterwards).[11]

Furthermore, due consideration should be given to the Legislator's decision to follow the same approach as that taken for False Statements and Reports Crimes. In this connection, in the Article third paragraph, which incriminates false statements by members of the corporate crisis settlement panel, the feasibility assessment virtually disappears, (along with any reference to the professional), whereas it is expressly provided for in the present wording of art. 16 of Law n. 3/2012.

---

[8] GAMBARDELLA, cit., p. 289; NIGRO-VATTERMOLI, *Diritto della crisi di imprese*, cit., p. 375. FIORELLA-MASUCCI, *Gestione dell'impresa e reati fallimentari*, cit., p. 134 ss.

[9] ALESSANDRI, cit., p. 1857.

[10] Cfr. GAMBARDELLA, *Il codice della crisi di impresa: nei delitti di bancarotta la liquidazione giudiziale prende il posto del fallimento*, in *Cass. Pen*., 2019, cit., p. 488 ss.; ALESSANDRI, cit., p. 1857 ss.

[11] SALERNO, *La riforma della crisi di impresa*, cit., p. 64 ss.

As for the rest, the Crime description coincides with what provided for in the second paragraph of Law n. 3/2012: this is a crime involving a concrete harm, to protect creditors' interest to receive correct information. Since it is committed by a member of the corporate crisis settlement panel, this crime is always to be considered as a special offence (the so called "*reato proprio*"); whereas typical conducts continue to consist of the conduct of making false statements.

The Legislator seems to have adopted the same criterion also for the Crime of False Statements by OCRI members, punishing false statements "as far as truthfulness of data contained in the debtor's plan or in the annexed documents is concerned". The Crime in question is actually new within the Criminal Law panorama - the Legislator's choice being dictated by the need to provide for specific criminal liability referring to emerging new professional figures connected to corporate crisis settlement procedures. Moreover, it is worth noticing that this crime too is based on False Statements and Reports Crimes referred to in art. 341 new Bankruptcy Code.

2.3. The mini-system of False statements Crimes under the new Bankruptcy Code

2.3.1. Common features of the mini-system of False Statements Crimes

The Legislator seems, in fact, to give discreet importance to the Crimes of False Statements in the context of the corporate crisis discipline, to the point of creating an autonomous mini-system; despite the historical immobility that prevails with reference to the criminal side of the matter.

However, it is necessary to distinguish the mini-system of False Statements Crimes from the Crime of False Statements to Obtain Eligibility to Use the Arrangement with Creditors Procedure, referred to in art. 236, Bankruptcy Law (art. 341 of new Bankruptcy Code). This crime undoubtedly represents a very relevant point of reference, both as it constitutes the first example of a False Statements Crime within the Bankruptcy Law, and as it takes into account procedures other than bankruptcy.

However, there are too many differentiating elements from the other crimes under consideration. As we have seen, in fact, the legal object appears to be geared towards protecting mainly the Administration of Justice and only indirectly the Property Interests of Creditors. In addition, the active subject is also different, which in this case is the entrepreneur and not various professional figures with specific certification tasks. Finally, the same relevant conducts, linked as we have seen to particular purposes, appear so specific that they cannot be combined with those of False Statements.

The same cannot be said with regard to the other crimes examined so far: False Statements and Reports Crimes *ex* art. 236-*bis* Bankruptcy Law (art. 342 of new Bankruptcy Code), False Statements Crimes by members of the Over-indebtedness crisis settlement panel *ex* art. 16, par. 2, l. 3 of 2012 (art. 344, par. 3, new Bankruptcy Code) and False Statements by OCRI's members *ex* art. 345 of the new Bankruptcy Code.

These criminal offenses, in fact, have various common characteristics to the point that a mini-system can be hypothesized. The mini-system in question first of all shares the interest protected by law. If it is true that we are faced with Crimes of False Statements, it would be an understatement to limit the discussion to the sole interest of Public Trust. Indeed, it seems that the interest protected by law is something else: that is, the Interest of

Creditors in Receiving Correct Information; interest that is instrumentally protected by the correct functioning of bankruptcy procedures[12].

Another feature in common is represented by the typical conducts built - with the exception of the false statements crimes referred to in art. 344, par. 3, new Bankruptcy Code, which incriminates the more general conduct of "making false statements" - according to the classic scheme of dual behaviour: commissive, with the releasing of false information; omissive, failing to report relevant information.

Well, the use of this dual behaviour demonstrates that Corporate Crisis Criminal Law has become fully aware of the qualitative and quantitative dimension of the widespread phenomenon of corporate information falsification: in this area too, in fact, information must possess the double character of truthfulness and completeness.[13] But the discussion does not end with the above mentioned profiles.

Indeed, there are further points of convergence between the crimes in question, especially with reference to the concept of relevance of false statements and, consequently, to the criminal liability model of danger crime. Although possible syntactic ambiguities, the requirement of relevance is expressly included only with reference to crimes referred to in Articles 342 and 345 of the new Bankruptcy Code; therefore, the reason for the exclusion is not understood, especially with regard to the specific crime referred to in art 344, par. 3, new Bankruptcy Code.

Actually, the relevance of the - false or omitted - information introduces, as mentioned, the concept of "materiality", of Anglo-Saxon origin, and represents a feature that must necessarily reside, if the crimes in question are to be provided with the necessary degree of harm.[14] Notoriously, this concept was born, more precisely, in the context of the US legal system after the economic depression resulting from the collapse of Wall Street, in particular by means of the 1933 Securities Act and the 1934 Securities Act. Materiality finds its own definition and its development by merit of case law, typical of Anglo-American legal culture[15] which reconstructs the concept of materiality in a purely objective sense, to be related to the abstract subject of the reasonable investor: in this regard, the information is relevant in the case in which it is able to influence the judgment and choices of the reasonable investor.[16]

It is therefore necessary, in order to return to the Italian legal system, that the information has a deceptive capacity: the information must be significant, it must therefore be specifically suitable for affecting the correct performance of the procedures.[17] Here, therefore, that False Statements Crimes appear to be constructed according to the criminal liability model of the concrete danger crime: the active subjects' conduct, on the basis of an evaluation of posthumous prognosis, must have been able to concretely alter the decision-making process of creditors.[18]

---

[12] ALESSANDRI, *Profili penali delle procedure concorsuali*, cit., p. 94 ss.; GAMBARDELLA, *Condotte economiche e responsabilità penale*, cit., p. 287.

[13] PEDRAZZI, *Diritto penale III, scritti di diritto penale dell'economia, problemi generali di diritto penale societario*, Giuffrè, 2003, p. 76.

[14] FEDERICI, *Il mendacio bancario: un difficile bilanciamento tra tutela anticipata della correttezza e trasparenza dell'informazione societaria e la necessaria offensività della condotta*, in *Cass.pen.*, 2019.

[15] Cfr. *TSC Industries v Northway Inc*, 426 U.S. 438 (1976), oppure *Basic Inc v Levison*, 485 U.S. 224 (1988).

[16] STRADER, *Understanding White Collar Crime*, LexisNexis, 2002, § 10.5.

[17] PEDRAZZI, *Diritto penale III, scritti di diritto penale dell'economia, problemi generali di diritto penale societario*, cit., p. 768 ss.; NUVOLONE, *Il diritto penale del fallimento e delle altre procedure concorsuali*, Giuffrè, 1955, p. 301.

[18] POGGI D'ANGELO, *Sul modello d'illecito e le sue conseguenze in tema di bancarotta fraudolenta prefallimentare*, cit., p. 3959 ss.

2.3.2 The enhancement of the interest protected by law of Information Correctness

Von Liszt noted that "the history of criminal law is the history of the interests of humanity elevated to interests protected by law; the criminal law of a given period is the balance taken from the book of the human give and take ".[19] In this sense, the interest protected by law is elevated to a parameter through which to investigate a specific historical period and, consequently, the related criminal law, if it is true that "the penalty is placed at the service of interests protected by law".[20]

It is on the basis of these considerations that the interpreter moves towards becoming aware of the pre-eminent role attributed within our legal system - at least until the aforementioned pandemic - to the protected interest of the Correctness and Truthfulness of Company Data. We can see a clear trend followed by our corporate crisis system: the system that is (*rectius*) outlining, or at least that "is (was) about" to take shape, is based precisely on the interest protected by law of Information Correctness.

In this sense, both the amendments to the existing False Statements Crimes and the introduction of new ones can be read: it is perceived as central to focus criminal law response to corporate crisis on a general correctness of the information flow that must be guaranteed at all levels, involving all the players who enter the game, starting with the entrepreneurs themselves or the administrators up to professional subjects outside the company structure.

Therefore, the criminal law system of the corporate crisis and insolvency seems, by now, aiming at building itself on three fundamental interests: the objective of protecting the "honest, but in difficulty" entrepreneur was added to the first, traditional interest, of protecting creditors' assets;[21] and now, together with these, the correct use of company information also seems to be added. In front of such a context, the interpreter is already called upon to rule, with his task of establishing the stability of the system outlined so far with the reality that (suddenly) is about to change.

3. Criminal profiles of funds granted to companies by the "Decreto Liquidità"

3.1 Notes on the system of funds granted by the State and guaranteed by SACE S.p.A.: the conditions and the concept of corporation "state of difficulty"

Article 1 of the so called "Decreto Liquidità" (Legislative Decree 23/2020) provides that "in order to ensure the necessary liquidity for companies based in Italy, affected by the COVID-19 epidemic, other than banks and other subjects authorized to provide loans, SACE S.p.A. grants guarantees until 31 December 2020, in compliance with European legislation on State subsidies (...), for financing in any form to the aforementioned companies".

Specifically, these loans amount to 200 billion euros, a figure from which 30 billion euros must be deducted for the support of small and medium-sized enterprises, including self-employed workers and freelancers with VAT numbers ("who have fully used their ability to access the Fund referred to in article 2, paragraph 100(a), of Law no. 662/1996.[22] These guarantees, of course, are issued only in the event that a series of certain conditions are met, among which the one reported in art. 1, paragraph 2(b) of the Decree in question,

[19] VON LISZT, *La teoria dello scopo nel diritto penale*, Giuffrè, 1962, p. 32 ss.
[20] *Ibidem*, p. 32.
[21] Art. 4.1. Directive EU n. 1023/2019; Regulation EU n. 848/2015; Recommendation of the Commission EU del 12/03/2014.
[22] Recommendation of Commission EU n. 2003/361/CE

according to which, in order to access the requested loan, the beneficiary company must comply with a double order of constraints:

i) as of 31 December 2019, do not fall into the category of "companies in difficulty" pursuant to Regulation (EU) no. 651/2014 of the Commission of June 17, 2014, of Regulation (EU) no. 702/2014 of June 25, 2014 and of Regulation (EU) no. 1388/2014 of December 16, 2014;

ii) as of February 29, 2020 not to be included among non-performing exposures in the banking system.

These presuppositions, especially the first one, cannot escape the criminal interpreter's eye, as "pathological" conditions of the company are recalled, which are absolutely unusual within the criminal law lexicon. In Criminal Law of economics, it is customary to deal with the notions of a State of Crisis, a State of Insolvency or a State of Distress[23]. What is highlighted in the crime analysed makes, on the contrary, reference to a particular "State of Difficulty" to be inferred on the basis of the aforementioned EU Regulations.

In order to accurately determine the parameters on the basis of which a company can be considered "in difficulty", it is necessary to refer to the provisions of EU Regulation no. 651 of June 17, 2014, which, in art. 2, establishes that a "company in difficulty" is understood to be one that complies with at least one of the circumstances provided for by the Legislator.[24]

3.2. Relevant criminal offenses. From the model of False Statements Crime to that of Fraud Crime: enforcement uncertainties and a return to the medieval stellionatus

After having reviewed, in a very brief way, the fundamental steps of the system provided by the Decreto Liquidità for the financing of companies affected by the Covid-19 epidemic, it is necessary, in order to trace the repercussions of a criminal nature, to begin from a starting point: the legislator has not provided for specific crimes.

On the one hand, the absence of an *ad hoc* criminal legislation aimed at sanctioning possible abuses contributes to increasing a framework already characterized by uncertainties and interpretative difficulties, but, on the other, does not exclude the possibility for crimes, already present in our legal system, to emerge. As far as the correct identification of the crimes contained in the Criminal Code is concerned, the question arises in terms of legal certainty and compliance with the fundamental Principles of Legality and Determination (as well as Precision, particularly in its Accessibility component, which, as is well known, is gaining ever greater importance in the light of the development of supra-national law). Actually, we find ourselves in the presence of more candidates as, abstractly, our legal system provides for many crimes that could well be considered relevant in this area.

The first model of criminal offense that is highlighted is represented precisely by False Statements Crimes which, as we have already noted, are gaining ever greater importance within the corporate crisis criminal law framework.[25] The Decreto Liquidità itself, in the first paragraph of art. 1-*bis*, expressly refers to the fact that requests for new loans must be supplemented by a self-certification referred to in art. 47 of Presidential

[23] GAMBARDELLA, *Condotte economiche e responsabilità economiche*, cit., p. 208 ss.; D'AVIRRO- DE MARTINO, *I reati di bancarotta societaria*, Giuffrè, 2013, p. 136 ss.

[24]Regulation UE n. 702/2014; Regolation UE n. 1388/2014.

[25]SIENA, *Problemi vecchi e nuovi delle false dichiarazioni sostitutive*, *in Diritto Penale Contemporaneo*, 3/2020, p. 237 ss.

Decree (D.P.R.), December 28, 2000, n. 445. Consequently, the first crime taken into consideration is represented by the so-called False Self-Certification pursuant to art. 76 of the Presidential Decree n. 445 of 2000: common crime that incriminates false statements, creation of false documents or their use in the cases provided for by the aforementioned Presidential Decree n. 445 of 2000. With regard to penalties, reference should be made to the matters established by the Criminal Code and by special laws.

With reference to the crime of False Statements in self-certifications, it cannot be denied that the Italian case law system is firm in considering as relevant False Certification Crimes committed by a private person in a public act, referred to in art. 483 of the Criminal Code, or the Crime of False Certification or Statements issued to public officials on identity or personal qualities, pursuant to art. 495 of the Criminal Code.[26]

However, during the application phase of the criminal scheme referred to in the aforementioned false self-certification crime to statements provided for by art 1-*bis* of the Decreto Liquidità, the first important difficulties emerge, connected to a double order of factors: first of all, the basic fragility and rigidity that characterize laws and regulations concerning False Statements Crimes; secondly, the peculiarities of documents and certifications required from companies which appear perhaps incompatible with a judgment of falsehood and, consequently, with the aforementioned system of False Statements Crimes.

From this point of view, it appears appropriate to remember that our legal system constructs false statements crimes according to an extremely fragmented case-law scheme: not all false statements made to public officials or to persons in charge of public services are considered crimes; but only those that integrate the details of one of the crimes provided for by the legal system. In other words, false declarations are criminally relevant only if they are expressly provided for by an incriminating law.[27]

On the other hand, regarding the data to be certified, undoubted problems arise both with reference to statements on the existence, in a period of time prior to the epidemic, of a going concern status of a business; both with reference to statements concerning the use of the funding to support personnel costs, investments or working capital employed in production plants and entrepreneurial activities located in Italy.

Business going concern status, as we have seen, consists in the assumption of the hypothesis of normal business operation destined to last over time. In essence, it is a prognostic assessment and, consequently, it requires a particularly accurate and challenging evaluation by the financing entities, especially with a view to simplification and speed, fundamental in the emergency context.

Well, on the one hand, this requirement represents a necessary element of the company balance sheet and, as such, in normal situations, it must be considered compatible with an evaluation aimed at establishing correspondence to the concept of "true", understood as “legally true”; on the other hand, given that we are in an extraordinary situation such as that of a real syndemic, the prospective judgment presents, on closer inspection, considerable doubts and uncertainties, precisely because of the unavailability, at present, of truly reliable rational standards.[28]

---

[26] PENCO, *Autodichiarazione Covid-19 e reati di falso: inapplicabile l’art. 483 c.p. se la dichiarazione mendace consiste nella mera manifestazione delle proprie intenzioni*, in Sistema penale, 12 gennaio 2021.

[27] PELISSERO, *Covid-19 e diritto penale pandemico. Delitti contro la fede pubblica, epidemia e delitti contro la persona alla prova dell'emergenza sanitaria*, in *Riv. It. Dir. Proc. Pen*., 2020, p. 513 ss.

[28] MUCCIARELLI, cit., p. 10; SIENA, *Problemi vecchi e nuovi delle false dichiarazioni sostitutive*, in *Diritto Penale Contemporaneo*, cit., p. 257.

The other aforementioned statement (that on the use of the funding to support personnel costs, investments or working capital employed in production plants and business activities located in Italy) also seems incompatible with the system of False Statements Crimes. In this sense, as acutely observed, it would seem that we are faced with a real declaration of will and not with a declaration supplementing a statement of truth, which would place this crime outside the area of False Certification Crimes.

Moving on to another crime which, in the abstract, could be relevant, by virtue of the characteristics of the financing procedure envisaged by the Decreto Liquidità, reference must be made to the Crime of the so called *mendacio bancario* (deliberate provision to Banks of False Information and Data), *ex* art. 137, par. 1-bis of the Testo Unico Bancario (Consolidated Law on Banking), which punishes the person who, in order to obtain credit concessions, provides the bank official with false information or data on his/her own economic situation.[29]

Such a crime represents a danger offense, being completely irrelevant that there is an actual damage to the banking institution; the Court of Cassation stressed that the rule is aimed at protecting in advance the Correctness and Loyalty in relations between the bank and the customer, regardless of the actual granting of credit and therefore of a property damage to the institution.

The outlined picture appears, in truth, much more complicated, since, together with the False Statements Crimes quickly reviewed, further crimes could well be called into question, such as the Crime of Undue Receipt of Public Funds to the Detriment of the State, referred to in art. 316-*ter* of Italian Criminal Code, or even the Crime of Aggravated Fraud to obtain public funds, pursuant to art. 640-*bis* of the Criminal Code.

The issue, therefore, presents considerable exegetical complexity: on the one hand, due to the traditional debate about the obscure relationships between the model of falsehood and the model of fraud and, consequently, between False Statements Crimes and Crimes of Fraud; and on the other, due to the complex relationship between the Crime of Undue Receipt of Funds to the Detriment of the State and the Crime of Aggravated Fraud to obtain public funds *ex* art. 640-*bis* of the Criminal Code.

However, there are still considerable difficulties for those who try to clear their mind as regards the tangled distinction between False Statements and Fraud Offenses: the boundaries between the two crimes still remain uncertain. Right within the obscure meanders of interpretation, any funding obtained through deceptive requests is inserted; with evident loss in terms of legal certainty and, consequently, of free self-determination on the part of the subjects who have to make the requests for funding.

A situation of uncertainty that almost seems to bring the hands of history back to the Middle Ages, when the ambiguous and obscure crime called "*stellionatus*" was in force (which alluded to a reptile with changing and iridescent colours depending on the light); a legal entity that, as noted by Franco Cordero, represented a multivalent crime, which designated "evil facts" fluctuating between forgery, theft and fraud.[30]

Returning to the problem of the exact legal qualification of deceptive behaviours used to obtain funds introduced by the Decreto Liquidità, the first problem that arises is the relationship between False Statements Crimes, in particular False Certification Crime

[29] FEDERICI, cit., p. 4051 ss

[30] CORDERO, *Procedura penale*, Giuffrè, 2012, p. 14; GARGANI, *Dal* corpus delicti *al* tatbestand, Giuffrè, 1997, p. 118 ss.; MIRTO, *La falsità in atti*, cit., p. 8 ss.

referred to in art. 483 of the Criminal Code, and the Crime of Undue Receipt of Funds to the Detriment of the State pursuant to art. 316-*ter* of the Criminal Code.

In this regard, it seems possible to exclude a formal concurrence of crimes, having to recognize that we are faced with a mere apparent concurrence of crimes: the case-law of the Court of Cassation, in fact, now seems to be peaceful in believing that the crime referred to in art. 316-*ter* of the Criminal Code absorbs false statements crimes provided for in art. 483 of the Criminal Code, as the use or issuing of false declarations or documents is an essential element for its configuration.

The last obstacle to overcome is, therefore, represented by the classic difficulty of correctly unravelling the relationship between the Crime of Undue Receipt of Funds to the Detriment of the State and Aggravated Fraud. After decades of jurisprudential conflicts, on this point, the Court of Cassation has clarified that the Crime of Undue Receipt of Funds to the Detriment of the State is in a subsidiarity relationship with that of Aggravated Fraud for obtaining public funds, like which, and unlike the crime of misuse of public subsidies, it is abstractly configurable even in the case of undue payment of welfare contributions. Therefore, the residual and less serious crime referred to in art. 316-ter, which unlike that referred to in art. 640-*bis* of the Criminal Code also absorbs the False Certification Crimes provided for by art. 483 Criminal Code and Use of a False Document provided for by art. 489 of the Criminal Code, can only be configured when there are no grounds in the conduct for assuming that fraud crime was committed.

The element that, on closer inspection, lacks is represented precisely by the induction into error of the person subject to the conduct, or by Carneluttian "mise en scene". Therefore, the Crime of Undue Receipt of Public Funds differs from that of Aggravated Fraud, aimed at obtaining the same, due to the failure to include, among the constituent elements, the misleading of the financing body, since the latter is called only to take note of the existence of the self-certified requirements and not to carry out an independent verification activity.

Precisely the financing methods under analysis seem to lead towards the crime mentioned above, compared to the more serious one of the aggravated fraud pursuant to art. 640-*bis* of the Criminal Code; a conclusion that appears to impose itself - even in the aforementioned uncertainty - as the most reasonable, given that, in order to speed up the financing process, the lending banks are not obliged to carry out specific checks on statements, certificates and requirements concerning the requests by the entrepreneurs in difficulty.

4. Conclusions: old, current and future needs for reform. The importance of the "Digital Era"

After outlining the challenges of the Italian legal system: at first, the pre-pandemic economic crisis, and, at a later time (in an understandably quick way), the crisis caused by the emergency from Coronavirus, finally, we can try to move some conclusive reflections. As we have seen, the legislator, placed before the first situation, considered it appropriate to introduce the new Bankruptcy Code, without however modifying, even to a minimum extent, the penal system; among the few innovations, however, it was noted how the catalogue of False Statements Crimes has been increased, confirming the tendency to enhance the interest protected by law of Information Flow Correctness even in the context of corporate crises.

Placed instead before the second (even more serious) situation, the legislator, correctly moved by absolute needs of promptness and speed of execution, intervened by providing for a financing system guaranteed entirely by the State, but neglecting to introduce a specific crime, with the consequent enforcement uncertainty due to the uncertain boundaries that exist between False Statements Crime, Misuse of Public Subsidies Crime and Fraud Crime.

Well, it is easy to understand how the phase in which we find ourselves is delicate and important: criminal law must come into play in a decisive way. Indeed, it is necessary to ensure an equitable distribution of exceptional funds, so as to avoid that entrepreneurs find themselves forced into the yoke of usury or that businesses fall into the hands of organized crime.

Furthermore, it is now clear to all interpreters that it is necessary, once and for all, to have the courage to reform the entire criminal system of the corporate crisis and insolvency: one can no longer ignore the creation of a modern legislative apparatus which is able to face the difficult times ahead. As is well known, and in doctrine, the discipline of corporate crisis and insolvency criminal law has an extremely old-fashioned structure with models that are now worn by time, incomplete and no longer consistent with reality.

In this perspective of reform, the entire system of Criminal Law on the matter should be definitively rethought in order to conform to the new reality of laws concerning corporate crisis and insolvency. As has been authoritatively affirmed, in such an area, the criminal law instrument is called upon to preside over interests protected by law imposed (if not created) by the civil legislator.[31]

In this sense, the autonomy of the criminal law instrument is undoubtedly limited and conditioned: it is the civil institutions that indicate degrees of relevance and roles of conflicting interests. Therefore, it would be necessary to abandon a system solely anchored to the sole protection of the creditor's assets (as well as to the *par condicio creditorum*), to embrace a system which, alongside this protected interest, also emphasizes the new need to rescue companies in difficulty (avoiding liquidation and dissolution), as well as the protection of the Correctness and Truthfulness of Corporate Information.

A general rethinking that could start from a topographical change: one could distinguish, on the one hand, the Crimes inherent to Corporate Crisis and, on the other, those inherent to Insolvency. In general, Bankruptcy Crimes should be re-designed, coherently with the new *equilibria* established on the civil side and, above all, in full compliance with Constitutional Principles.

A central aspect of the reform should be represented by the introduction of new incriminating patterns that are more responsive to the Principle of Harm and Culpability. In this sense, it would be useful to assess whether crime with naturalistic event and damage could be effective also with reference, for example, to the crime of fraudulent patrimonial bankruptcy (unlike crime of fraudulent bankruptcy on documents), for which compatibility with this pattern seems difficult, as it reflects a more advanced protection of rights to the receivables; therefore, it would risk losing a good part of its effectiveness, if one wanted to ask for something more than a simple exposure to danger).

Another Crime to be thoroughly and carefully examined is represented by the so called Bankruptcy Crime resulting from Fraudulent Operations as referred to in art. 223, par. 2, n. 2, bankruptcy law (art. 329, par. 2, let. *b*, new Bankruptcy Code): a residual crime

[31] ALESSANDRI, cit., p. 1820 ss.

but posing as a real and true unintentional offense. Further analysis should be carried out on the much disputed crime of the so called "bancarotta da concordato preventivo" (Bankruptcy Resulting from Arrangements with Creditors), *ex* art. 236, par.2, Bankruptcy Law (art. 342, par. 2, new Bankruptcy Code): this crime prerequisites sound highly outdated and of uncertain constitutional legitimacy and the relevant sanctioning burden should, at the very least, be eased so as to clearly distinguish this crime from bankruptcy crime.

One of the possible ways to prevent the risk of crimes, in particular corporate and bankruptcy crimes, is represented by innovating company structures, consistently with the technological and digital evolution underway today so massive and impressive as to characterize our era as the 'digital era'. Technological and digital evolution has in fact allowed the proliferation of new channels and devices.

Indeed, in addition to helping to prevent the risks of committing crimes which would lead to the cessation of business activities (which must be averted, precisely in light of the dramatic crisis the world has presently fallen upon), through digitization the benefits for companies would be manifold. In this sense, in fact, it would be possible to sell on the market through e-commerce platforms, communicate with customers via social networks, entertain commercial contacts through a delocalized sales network, work in teams made up of members of different companies and geographical position, break down costs for energy resources through Smart Energy, improve production, storage and shipping logistic processes, automate production machines and equipment, collect or make payments through smartphones or payment cards.

All processes are potentially involved in digitization, all company activities could benefit from it and the company could achieve a significant improvement in the quality of work. The model to be adopted to start a Digital Transformation process requires extreme flexibility of the entire organization. If the organization is flexible, the systems must also allow it to be reactive and fast, allowing a direct dialogue with users, thus tracing the flow of information, a key concept of the modern and future management control in which it will be possible to convey 'real-time' information from different applications, continuously integrating the corporate value system. Management control allows company activity to be monitored by analyzing internal data and is able to quickly and selectively provide data that allow for a final and budgetary analysis.

Precisely the improvement of internal data analysis systems and, above all, of the information flow transparency, could represent the turning point to minimize the risks of committing corporate and bankruptcy crimes, with the consequent saving of many companies, otherwise destined to go out of business or to be liquidated.

The Penal Juridical Defence against acts of xenophobic and racist nature committed through computer systems

Dr. Ylli Pjetërnikaj[1] - Prof. Dr. Altin Shegani[2]

1. Introduction

Some member countries of the Council of Europe already have in place suitable legal mechanisms for combating racism. Nevertheless, there are difficulties for fighting racism spread through Internet due to the nature of communication and the legal obstacles for implementing the provisions of "hate speech". That is why it became indispensable to create an instrument of binding nature throughout the Council of Europe countries. Taking into consideration the Action Plan adapted at the Second Summit (Strasburg, 10-11 October 1997), and in order to seek common responses to the new technologies' development, and based on the values and standards of the Council of Europe, the Additional Protocol "On the criminalization of the acts of racist and xenophobic nature committed through the computer systems" was approved in January 2003.

The purpose of the Additional Protocol is to add to the provisions of the Convention on the cyber-crime so that all the acts of racist and xenophobic nature committed through the computer systems could be penalized.[3]

The second chapter of the Additional Protocol provides for the measures that should be taken at a national level, concretely speaking, the material provisions that should be foreseen as penal offences, such as the dissemination of racist and xenophobic materials through a computer system, the threat based on racism and xenophobia, the offence of a racist and xenophobic nature, the considerable nihilism, the approval or justification of genocide, or crimes against humanity, as well as the support and incitement of such phenomena.[4]

[1] Prosecution Office at First Instance Court of Lezha, Albania, ylli.pjeternikaj@pp.gov.al
[2] Professor of Criminal law (Special Part), Faculty of Law, University of Tirana, Albania, altin_shegani@yahoo.com
[3] The Additional Protocol "On the criminalization of the acts of racist and xenophobic nature committed through computer systems", 2003.
[4] The Additional Protocol "On the criminalization of the acts of racist and xenophobic nature committed through computer systems", 2003, articles 3-7.

The Republic of Albania, with Law no. 9262, dated 29.07. 2004, ratified the Additional Protocol of the Cyber-crime Convention "On the criminalization of the acts of racist and xenophobic nature committed through computer systems".[5] With the ratification of the Additional Protocol, Albania undertook the responsibility and obligation to criminalize the acts of a racist and xenophobic nature committed through the computer systems.

In the framework of these obligations Law no. 10023, dated 27.11.2008 was approved, by means of which the following penal offences have been added to the Penal Code:

- The dissemination of materials favouring genocide or crimes against humanity through the computer;[6]
- The dissemination of racist and/or xenophobic materials through a computer system;[7]
- The threatening with racist or xenophobic motives through a computer system;[8] and
- The insult with racist or xenophobic motives through a computer system.[9]

This paper will focus on analysing the degree of harmonization of the 2008 legislative intervention with the provisions of the Additional Protocol to the Cyber-crime Convention. The analysis will be followed by detailed doctrinal and practical treatments of the elements of these types of criminal offenses, in the problems identified during their application by the jurisprudence in Albania, as well as internationally.

2. General aspects and concepts on cyber racism

The acts of a racist or xenophobic nature committed through computer systems, due to their intensity and the negative consequences, have contributed for the creation of the phenomenon known as cyber-racism. This phenomenon refers to the racism which is being manifested by means of internet throughout the world.[10] It includes words, images and symbols posted on social media services,[11] games on internet, fora, messages' services or dedicated 'hate sites'.[12] Cyber-racism includes a wide spectrum of behaviour for as far as the seriousness and specifics are concerned, beginning from, for example, a

[5] Law no. 9262, dated 29.07.2004, which ratified the Additional Protocol of the cyber-crime Convention "On the criminalization of the acts of racist and xenophobic nature committed through computer systems".
[6] Penal Code,1995, article 74/a.
[7] Penal Code,1995, article 119/a.
[8] Penal Code, 1995, article 84/b
[9] Penal Code, 1995, article 119/b
[10] Gail Mason and Natalie Czapski, Regulating cyber-racism, *Melbourne University Law Review* (vol 41:284, 2017), 294.
[11] Danielle Keats Citron, Fulfilling government 2.0's promise with robust privacy protections' (2010) 78 *George Washington Law Review* 822, 824 n 12; Citron and Norton (n 4) 1439 n 22.
[12] Brendesha M Tynes et al, Online Racial Discrimination and the Protective Function of Ethnic Identity and Self-Esteem for African American Adolescents' (2012) 48 *Developmental Psychology*, 343, 344.

humoristic hidden racist material marked as "humour"[13] in order to transmit threats and violence incitement towards individuals or specific groups due to their race.[14]

Cyber-racism represents its own specific challenges, especially the penal juridical defence from it. The material posted on internet can be found anywhere and is more or less permanent. The information can be disseminated instantly, continuously and globally, reaching much bigger audiences than it can reach in a non-virtual world.[15] Furthermore, when the material is published on internet, it remains "memorized" or "saved", and potentially can be reached through the search engines and can easily be copied or duplicated.[16]

The removal of a material with a racist content from a platform does not guarantee its permanent deletion from the cyber space. This has made that the "cyber hatred" be described as a permanent damage towards the "target group members".[17]

"Racist and xenophobic material" is any written material, any image or any other representation of thoughts or theories which favours, disseminates or incites hatred, discrimination or violence against an individual or group of individuals, based on race, colour, origin, national or ethnic origin, or religion, if it is used as a pretext for any of these factors.[18]

The written material includes any kind of book, magazine, status or message on social networks; whereas the image includes drawings, paintings or pictures/photos.[19] The representation of thoughts or theories relates to any form of display in the outer world; without limiting to, we can mention as examples the filmic or melodic materials.

A worldwide accepted definition of racism constitutes an analytic difficulty which is determined by the fact that the race categories are social in themselves, without a strong empirical foundation.[20] The concept of race is used in the contemporary policies and legal instruments in order to define the perceived differences between groups of people based on the physical and social characteristics such as the colour of skin, ethnic and national origin.[21] Racism began to be used as an umbrella term to refer to a combination of values,

---

[13] Simon Weaver, 'Jokes, Rhetoric and Embodied Racism: A Rhetorical Discourse Analysis of the Logics of Racist Jokes on the Internet' (2011) 11 *Ethnicities* 413, 431.

[14] Kim Stephens, 'Mariam Veiszadeh Now the Target of US Anti-Islam Site', *The Queensland Times* (Ipswich, Queensland, 25 February 2015) <www.qt.com.au/news/mariam-veiszadeh-now-target-us-anti-islam-site/2555598/>, archived at <https://perma.cc/RE95-TD4U>.

[15] General Television Corporation Pty Ltd v DPP (Vic) (2008) 19 VR 68, 88 [70].

[16] AHRC, 'Human Rights in Cyberspace' (n 21) 16.

[17] Citron and Norton (n 4) 1452, citing Jeremy Waldron, 'Dignity and Defamation: The Visibility of Hate' (2010) 123 *Harvard Law Review),*1597, 1601, 1610.

[18] The Additional Protocol Protocol "On the criminalization of the acts of racist and xenophobic nature committed through computer systems".2003, article 2/1.

[19] Yaman Akdeniz, *"Racism on the Internet",* Council of Europe Publishing, (December 2009), 81.

[20] Robert Miles and Malcolm Brown, Racism (Routledge, 2nd ed, 2003); Yin C Paradies, 'Defining, Conceptualizing and Characterizing Racism in Health Research' (2006) 16 Critical Public Health 143, 144.

[21] OSCE Office for Democratic Institutions and Human Rights and the International Association of Prosecutors, Prosecuting Hate Crimes (Practical Guide, 2014) 29, 30.

behaviours and conducts which exclude people from the society on the basis of their race, ethnicity, cultural practices, national origin, and in some cases religious belief.[22]

The racist speech, be it through language, images or symbols, is a tangible expression of racism. This is why the penal defence against it is justified with the reasoning that it causes considerable individual damage to the sense of dignity, wellbeing, and safety of the receiver,[23] as well as group damage to the targeted community that can interpret such expressions as a sign of intolerance and victimization.[24] We may say that racism accounts for a moral failure to treat the others in an equal, just and dignifying way.[25]

The cyber racism represents itself as a new challenging problem, especially at the border-line of the respect for the freedom of expression as a fundamental human right. In this aspect, the European Court of Human Rights (ECtHR) has identified a number of forms of expression which are considered as violating the European Convention of Human Rights. Such are: racism, xenophobia, anti-Semitism, aggressive nationalism and discrimination of minorities or of emigrants.[26]

The freedom of speech, while it is especially valuable in democracy, does not allow speeches that favour racial discrimination and hatred, regardless the medium used. Freedom of speech is treated as a two-fold right. First, it is the right to send, transmit and express opinions and ideas of any kind; and second, it is the right to search and receive information in any form.[27] The boundaries of this freedom are defined by that which is defined as "hate speech".

The meaning of the term "hate speech" is explicitly defined in the Recommendation no. R (97)20 of the Committee of Ministers of the Council of Europe on the "hate speech", in 1997. In the Appendix of the Recommendation it is emphasized that the "hate speech" must be understood as a notion which includes all forms of expression by means of which the racial hatred, xenophobia, anti-Semitism or other forms of hatred are disseminated, incited, promoted or justified, and which are based on non-tolerance, including here even the non-tolerance expressed in the form of the aggressive nationalism and ethno-centrism, the discrimination and the hostility towards the minorities, migrants and persons of emigrant origin.[28] Hate speech means manifestation of hate towards a

---

[22] Y Paradies et al, Building on Our Strengths: A Framework to Reduce Racial Discrimination and Promote Diversity in Victoria (Report, 2009) 7., si dhe Andrew Jakubowicz, 'Hunting for the Snark and Finding the Boojum: Building Community Resilience against Race Hate Cyber Swarms' (Conference Paper, 40 Years of the Racial Discrimination Act 1975 (Cth) Conference, 19–20 February 2015) 105, 106–8, archived at.

[23] Sentencing Advisory Council, Sentencing for Offences Motivated by Hatred or Prejudice (Report of Advice, July 2009) 1 [A.4], quoting Manitoba Department of Justice, Policy Directive: Hate Motivated Crime (Guideline No 2:HAT:1, June 2008) 5 , archived at.

[24] Paradies et al (n 11) 36. See also Gabrielle Berman and Yin Paradies, 'Racism, Disadvantage and Multiculturalism: Towards Effective Anti-Racist Praxis' (2010) 33 Ethnic and Racial Studies 214, 215–18.

[25] Tim Soutphommasane, 'Racism is a Moral Issue' (Speech, Society of Australasian Social Psychologists Conference, 11 April 2014) , archived at.

[26] Recommendation No. R 97 (20) of the Committee of Ministers of the Council of Europe on "hate speech ".

[27] Elena Mihajllova, Jasna Baçovska, Tome Shekerxhiev, "Freedom of speech and hate language", (Polyesterday, Shkup 2013), 7.

[28] Recommendation no. R (97) 20 of the Committee of Ministers to Member States on "Hate speech", in http://rm.coe.int/1680505d5b ; accessed on 14 May 2017.

definite group and it is used to insult and offend a person due to his racial, ethnic, or religious affiliation; or towards another group where this person belongs to.[29] The purpose of using such speech is the manifestation of hatred, violence or contempt against an individual or a group due to group affiliation.

3. The computer dissemination of materials that are pro genocide or crimes against humanity

The criminalization provided by the Albanian lawmaker[30] for the acts of denial, significant minimization, approval or justification of genocide or crimes against humanity, is almost the same with that defined in the Additional Protocol.[31]

The purpose of the drafters of the Additional Protocol was the criminalization of the expressions which deny, significantly minimize, approve or justify the acts which constitute genocide or crimes against humanity. The most important and significant conducts which caused genocide and crimes against humanity occurred during the period 1940 – 1945.

Since that time, other cases of genocide and crimes against humanity occurred, which were strongly motivated by different ideas and theories of racist and xenophobic nature. This is why the drafters considered as indispensable the need for not limiting this provision only to the crimes committed by the Nazi regime during World War II and determined as such by the Nuremberg Tribunal, but also to the other crimes of genocide and crimes against humanity determined by the other international tribunals set-up since 1945 through relevant international legal instruments (such as the Resolutions of the U.N. Security Council, multilateral treaties, etc.) as for example, the International Courts of Justice set-up for ex-Yugoslavia, for Rwanda, the Permanent International Court of Justice, etc.

This penal norm aims at clarifying that facts which are historically and clearly proven should not be denied, significantly minimized, approved or justified, so that they cannot support such disgusting ideas. Regardless of the fact that the hypothesis of the penal norm in the Albanian Penal Code has provided for the term "acts which constitute genocide or crimes against humanity", without conditioning it with the recognition of such acts by final decisions of international tribunals, the evaluation whether these acts are of such nature should initiate from their recognition as genocide and crimes against humanity. The later must be an object of judicial recognition, and not of academic evaluation, or historical opinion. This is why the Additional Protocol is so attentive to recognize as such only those determined by final and compulsory decisions of the International Military Tribunal, deriving from the London Agreement of April

[29] Elena Mihajllova, Jasna Baçovska, Tome Shekerxhiev, "Freedom of speech and hate language", (Polyesterday, Skopje 2013), 24.

[30] Penal Code, art. 74/a which provides for that: "Delivering to the public or intentionally distributing to the public, through computer systems, of materials that significantly deny, minimize, approve or justify acts that constitute genocide or a crime against humanity, is punishable by three to six years in prison".

[31] The Additional Protocol Protocol "On the criminalization of the acts of racist and xenophobic nature committed through computer systems".2003, article 6/1.

8th, 1945, or of any other international tribunal created by the relevant international instruments whose jurisdiction is recognized by the Party states.

This shows that Holocaust represents a true cultural explosion, beyond the typical penal cases.[32] This heritage, whose consequences continue even today and humanity should continue to deal with, constitutes a "pedagogical" purpose for humanity. After Holocaust, there was a clear-cut cultural and judicial reaction towards war crimes, genocide and crimes against humanity. Although it was a statement of personal responsibilities of the individuals, the magnitude of this event and the endless list of the victims required another response, if not a collective government responsibility, at least a "responsibility" which goes beyond the "German guilt".[33]

The penal-juridical defence is done to memory, it is born from it and it is the other side of a collective guilt, not only a German one, but also of the anti-Hebrew East and West, because the Holocaust was only the final act, the "logical" one of 2000 years of persecution. The historical memory can constitute a political "value", or a "good", but it cannot be defended (neither it can be criminalized) as a lawful interest, not even at the level of the European law. The results of a scientific research cannot be included in the penal defence of a state with regard to their content. Science presumes falseness, whereas the penal defence of a declaration presumes just the opposite.[34]

Nevertheless, due to the specific characteristics of Holocaust, a delicate but crucial difference is observed between the denial of the genocide and the denial of the other crimes. This type of penal offence aims at penalizing the offering in public or the intentional dissemination in public of the materials favouring genocide and crimes against humanity. The offering in public or the dissemination include any way that enables for the materials to be reachable and easily accessible for everyone. The computer systems have made the offering in public or dissemination very easy. The material can be spread through social networks, on dedicated websites, or on webpages.

For the effect of the legal qualification, the coming of the consequences from the act is not required, or that the denial or minimization be done with the purpose of inciting hatred, discrimination or violence against each individual or group of individuals. It is enough that the person be conscientious for the importance of the action he is doing, of the content of the material he is disseminating, and he must wish to accomplish the act.

---

[32] Massimo Donini, Negazionismo e Protezione Della Memoria" (L'eredità dell'Olocausto e la sua sfida per l'etica pubblica e il diritto penale. Conferenza Internazionale di Tbilisi organizzata dall'Università Statale di Sokhumi nei giorni 29 novembre-1 dicembre 2018 sul tema "Topical Issues of Crime of Genocide and Human Rights Protection"), 4.

[33] K.Jaspers, The Question of German Guilt (1946), trad. it. La questione della colpa. Sulla responsabilità politica della Germania, Milano, 1996; H. ARENDT, Collective Responsibility (1987), in Responsibility and Judgment (2003), trad. it. Responsabilità collettiva, in EAD., Responsabilità e giudizio, Torino, 2004, 127 ss.; G. ANDERS, Nach Holocaust, 1979, trad. it. Dopo Holocaust, 1979, Torino, 2014.

[34] G. Werle, Der Holocaust als Gegenstand der bundesdeutschen Strafjustiz, in Neue Juristische Wochenschrift, 1992, 2529 ss., 2535; G. WERLE, T. WANDRES, Auschwitz vor Gericht. Völkermord und bundesdeutsche Strafjustiz, München, 1995.

The jurisprudence in Albania has been very insufficient. The prosecution office has had cases when it has conducted penal prosecution for such acts as referred by the judicial police. So, in the First Instance Prosecution Office of Tirana, a penal proceeding has been registered for the penal offence of "Computer dissemination of materials favouring genocide or crimes against humanity". This penal proceeding has started regarding notes posted on Facebook with the following content: "*Je etais (I was) Charlie Hebdo, now I' m Harry S. Truman!" This serves as a response to those who get indignant by my idea to make Islam disappear by hitting Mecca and Medina with atomic bombs. Mecca and Medina together have 3 million inhabitants. If in Hiroshima and Nagasaki 300 thousand Japanese people were killed in order to eradicate the Japanese militarism, it is not a big tragedy to kill 3 million Arabs in order to eradicate the origin of Islamic terrorism. NATO needs a Truman to think in this way, strategically. For this reason: I' m Harry S. Truman. /K.M"*

The citizen K.M. has confessed that he has written that in Facebook, and according to him, this posting had a study purpose and is a citing from President Truman, in order to see the reaction of the Albanian community. The prosecution decided to terminate the penal proceedings arguing that, firstly, there should exist the act that constitutes genocide or crimes against humanity, recognized as such through court decisions. The posting made in this case was considered as expression of opinions, in the framework of the freedom of expression of the individual.[35] In this concrete case, since the attacks on Hiroshima and Nagasaki have not been recognized internationally as crimes against humanity, then it is absent the "act that constitutes genocide or crimes against humanity", as an indispensable condition for the application of the penal responsibility.

In its jurisprudence, the European Court of Human Rights (ECtHR) has stressed in a definite way that the denial or the review of "historical facts clearly proven, such as Holocaust, the defence of articles 10 and 17 of the ECHR will be dropped".[36] The Court assesses that, in this judicial case, the defendants did not try to deny or review that which they themselves referred to in their publication as "Nazi troika and the persecutions", or "German barbarism and plenipotentiary". By describing the policy of Philippe Pétain as "extraordinary capable", the authors of this text, on the contrary, are supporting one of the conflictual theories in the debate on the role of the head of Vichy government, the so-called "double-game" theory.

In conclusion, the Court considers the penal punishment of the defendants as non-proportional, and as such, un-necessary in a democratic society. That is why there was a non-application of article 10 of the ECHR, which defends the freedom of expression. The jurisprudence of the European Court of Human Rights is consolidated in the statement that the speeches which are irreconcilable with the proclaimed values guaranteed by the Convention do not get protected by its article 10. Some examples of such speeches include the denial of

[35] Decision on th etermination of the penal proceedings no. 1840, dated 25.10.2016, of the Prosecution Office at teh First Instance Court of Tirana.

[36] Case of Lehideux and Isorni v. France (55/1997/839/1045) judgment Strasbourg, 23 September 1998.

Holocaust, the justification of pro-Nazi policies, the association of all Muslims with the serious terrorist acts, the considering of the Hebrew people as the "source of devils in Russia".[37]

In the jurisprudence of other countries there have been some cases where elements of this type of crime have been evidenced. So, *Töben* case is evidenced in Australia. This case has to do with a German-Australian citizen who had a website in Adelaide Institute of Australia. The Federal Court declared him guilty and ordered the deletion of the material from the website. According to the Court, *Töben*, with the publication of this material, had offended and humiliated the Hebrew groups in Australia through the denial of Holocaust.[38]

In Canada, it is another case known as *Zundel* case.[39] Ernst Zundel, a German citizen, who lived in Canada, is considered as one of the most active disseminators of neo-Nazi propaganda worldwide. He used the mail, telephones, email, media and internet for this purpose. The Canadian Tribunal of Human rights assessed that the publication of materials which denied Holocaust in Zundel-site exposed the Hebrews to hatred and humiliation. According to it, internet is the most effective means of disseminating such material. It was also emphasized that hatred cannot be tolerated wherever it is, on internet or not.[40]

4. Dissemination of racist and xenophobic materials through computer system

The type of the criminal offense entitled *"Dissemination of racist or xenophobic materials through the computer system"*[41] was included in Section VII of Chapter II, which has as a group objective the protection human dignity and moral, by placing it in a chronological order after the penal offence of "Insulting" foreseen in article 119 of the Albanian Penal Code.

This categorization is done by the lawmaker considering that its direct objective is the guaranteeing of the sense of personal dignity, of health, of the fundamental rights of each individual or group of individuals, who have been targeted by using as a pretext their race, colour, origin, national or ethnic origin, or religion.[42]

The penalization techniques of this kind of penal offence are clearly defined in the Additional Protocol, asking for the effect of the application of penal liabilities the performance of such acts like dissemination, or otherwise offering in public the racist and xenophobic material through a computer system.[43]

---

[37] Lehideux and Isorni v. France,; Garaudy v. France (dec.), no. 65831/01; Norwood v. the United Kingdom (dec.), no. 23131/03; Witzsch v. Germany (dec.), no. 7485/03, Judgement of 13 December 2005, Pavel Ivanov v. Russia (dec.), no. 35222/04, Judgement of 20 February 2007.

[38] Jones v. Toben (2002) FCA 1150.

[39] R. v. Zundel, (1992) 2 SCR 731, 1992 CanLII 75 (SCC).

[40] R. v. Zundel, (1992) 2 SCR 731, 1992 CanLII 75 (SCC).

[41] Penal Code, art. 119/a, which provides for that: "*Delivering to the public, or intentional distribution to the public, through computer systems, of materials with racist or xenophobic content, constitutes a criminal offense and is punishable by a fine or up to two years of imprisonment."*

[42] Ismet Elezi, "*Penal Justice (Special Part)",* 173.

[43] Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), paragraph 27.

The act of "dissemination" refers to the active spread of the racist and xenophobic material to the others, whereas "making available" refers to the placement on internet of the racist and xenophobic material so that it can be used by others. These terms tend to include even the creation and establishment of hyper-links in order to facilitate the availability of such materials.[44]

The term "for the public" makes it clear that the private communications or the communicated or transmitted expressions through a computer system are beyond the area of this provision. Such expressions or communications, as for example, the traditional forms of correspondence, get protected by article 8 of the ECHR.[45] Whether a communication of racist and xenophobic nature is considered as a private communication or dissemination for the public, it should be defined on the basis of the circumstances of the given case. In general, the thing to be taken under consideration is the purpose of the sender, so that the message is taken only by the pre-determined receiver of the message. The presence of this subjective purpose can be defined by a number of objective factors, such as the content of the message, the technology used, the safety and security measures applied, as well as the context in which the message is sent. When such messages are sent at the same time to more than one receiver, the number of receivers and the nature of relationship between the sender and the receiver/s is a key factor for determining whether such a communication can be considered as a private one.[46]

The exchange of the racist and xenophobic material in the chat-rooms and the posting of similar messages in the news groups or discussion groups are examples of the placement of this material as available for the public. In such cases the material is accessible for everyone. Even in cases when having access to the material would require an authorization through a password, the material is accessible for the public when such authorization would be given to anyone who complies with some criteria. In order to define whether the availability or the dissemination was intended for the public or not, the nature of the relationship between the persons involved should be taken into consideration.[47]

The cases of exchange of racist and xenophobic material in chat-rooms, or posting similar messages in the news groups or discussion groups can be mentioned as examples that illustrate the making available of the material for the public. In such cases, the material becomes accessible immediately after being posted for every person who visits these sites.

There exist opinions that in the cases when discussion groups of a certain number of individuals are created on-line, the publication of racist and xenophobic material

[44] Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), paragraph 28.

[45] Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), paragraph 29.

[46] Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), paragraph 30.

[47] Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), paragraph 31.

cannot be considered that it is for the public. This is due to the fact that the forums can appear as groups of limited membership. In such cases the relationship between the parties prevails over the number of receivers in defining whether the material has to be considered for the public, or not.[48] The act of dissemination or making available is considered as criminal only if the purpose addresses the racist and xenophobic character of the material.

The determining of the penal liability for such actions sometimes becomes difficult because the authors of such acts justify themselves with the freedom of expression. Nevertheless, the jurisprudence of ECHR stands by the statement that the use of "hate speech" does not enjoy protection by article 10 of the Convention,[49] because it does not comply with the proclaimed values guaranteed by the Convention. The European Court of Human Rights reasons that the acts which are irreconcilable with democracy and human rights undoubtedly pursue objectives that are prohibited by article 17 of the Convention, so that they do not benefit from article 10.[50]

The conviction and the ideas of the web-sites' owners or of a political leader who publishes xenophobic statements face an immediate social need for protecting the rights of the communities. This position is held by the jurisprudence of Belgium in the *Féret* case. Daniel Féret was a member of Belgium's Parliament and the leader of the National Front in Belgium. During the electoral campaign he had disseminated leaflets with the slogan "*Stand up against the Islamification of Belgium*". Féret was sentenced by the national Court for incitement of racial discrimination. He claimed the violation of freedom of expression before the European Court of Human Rights.

The European Court of Human Rights assessed that the sentence was justifiable in the interest of preventing the breach of public order and defending the rights of others, concretely speaking the rights of alien immigrants. According to the position of the Court, the comments made by Féret contained evident responsibility for causing the feeling of disbelief, refusal or even hatred against alien citizens, especially amongst the less informed public. His message, sent in the electoral context, contained a strong echo and explicitly incited racial hatred. The Court decided that the sentence didn't violate article 10 of the Convention.[51]

Another case is that of *Williem against France*,[52] which had to do with the call for a boycott to the Israeli products by a city Mayor, through the municipal web-site. The Mayor was sentenced according to the national French legislation on charges of provoking discrimination. The case went up to the European Court of Human Rights, claiming the violation of article 10 of the Convention (freedom of expression).

The European Court of Human Rights assessed that the arguments given by the French Court to justify the interference to the freedom of expression, as claimed by the

---

[48] Jennifer Schweppe, Dermot Walsh, *"Combating Racism and Xenophobia through the Criminal Law"*, Centre for Criminal Justice, University of Limerick, September 2008. 157

[49] Gündüz v. Turkey, Application no. 35071/97, Judgement of 4 December 2003.

[50] Garaudy v. France. Application no. 65831/01, Inadmissibility Decision.

[51] Féret v. Belgium, Application no. 15615/07, Judgement of 6 July 2009.

[52] Willem v. France, Application no. 10883/05, Judgement of 16 July 2009.

defendant, had been "important and sufficient" for the purposes of article 10. The incitement of acts of discrimination by an elected public official through the official web-site of the town-hall does not make part of the free discussion of a case which has general public interest.

The discriminating nature of the political messages is aggravated by the fact that they are published on internet, and consequently is punishable.[53] The offering in public and the dissemination of materials of racist and xenophobic content not only that bring grave consequences to the concrete individual and to the group they are addressed, but also to the society in general. Such materials violate the principle of equality and non-discrimination, which are protected and guaranteed by the fundamental legal act of a country, the Constitution. The offering in public and dissemination of such materials potentially incites the violence and crime, motivated by racism and xenophobia.

5. Insult and Intimidation with motives of racism or xenophobia through the computer system

The type of the penal offence entitled *"Insult with motives of racism and xenophobia through the computer system"*[54] was also included in Section VIII of Chapter II of the Albanian Penal Code, which has a group object the protection of human moral and dignity, by placing it in a chronological order after the penal offence of "Insult" provided for in article 119 of the Penal Code. The direct object of protection is the protection of honour and dignity of the persons who belong to a certain race, nationality, ethnicity or religion.[55] The penal juridical protection covers only the public insult of a person or a group of persons due to the fact that they belong to, or is thought to belong to such a group because of the specific characteristics.[56]

The term of "insult" refers to any insulting or offensive expression which prejudices the honour or dignity of a person.[57] The formulation of the norm in itself makes it clear that the insult is directly connected to the affiliation of the insulted person or group of persons and is committed based on such motives. The passive subject in this penal offence is not insulted as an ordinary individual, but as a member of a concrete community with which he shares specific characteristics of identity.[58] The insult of an individual who belongs to a certain ethnic, racial or religious group for other personal

---

[53] Willem v. France, Application no. 10883/05, Judgement of 16 July 2009.

[54] Penal Code, art. 119/b, which provides for that: "*The Intentional public insult, through a computer system, done to a person due to ethnicity, nationality, race or religion, constitutes a criminal offense and is punishable by a fine or imprisonment of up to two years."*

[55] Ismet Elezi, "*Penal Justice (Special Part)",2015*. 174.

[56] Yaman Akdeniz, *"Racism on the Internet",* Council of Europe Publishing, December 2009, 83.

[57] Council of Europe, European Treaty Series - No. 189, Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems paragraf 36.

[58] Elena Mihajllova, Jasna Baçovska, Tome Shekerxhiev, "Freedom of speech and hate language", Polyesterday, Skopje 2013, 35.

reasons which do not have to do with his affiliation will be qualified according to article 119 of the Penal Code, which provides for the simple and ordinary insult.

Differently from the case of threatening, the insult expressed in a private communication is not covered by this provision.[59] This is so because the public character of the insult is missing in private communication. The public, as a constituent element of the penal offence, represents the need for the insult to be heard or viewed not only by the victim, but also by third persons. If we were going to draw a parallel with the provision that the lawmaker has done for the ordinary insult, the public character can be considered as a worldwide commission of the penal offence.

The objective side element, which is necessary per the legal qualification, is the medium for committing the insult through a computer system due to the motive of racism and xenophobia. The jurisprudence of Albania has known cases of such penal offence. Whereas the Cassation Court of Italy, in connection to the moment that this penal offence is committed, emphasises that the insult through computer systems gets perfected at the moment that the message (the email, web or chat) is perceived by the damaged subject or the other third-party subjects.[60]

In its jurisprudence, the European Court of Human Rights has argued that article 10 of the Convention (freedom of expression) does not guarantee an unlimited freedom of expression, especially when the information published can cause consequences to the reputation and the rights of individuals.[61]

In the case of *Renaud v. France*, which had to do with the penal punishment of the defendant for defamation and public insult of a city mayor on the webpage of the association where he was a member of and a webmaster, as well, the European Court of Human Rights found breaches of article 10 of the Convention (freedom of expression), because the punishment of the defendant was non-proportional to the legitimate purpose of defending the reputation and the rights of the others.[62] Nevertheless, the on-line publication of personal attacks which surpass that which can be considered a debate on the ideas is not protected by article 10 of the Convention.[63]

In the case of *Pihl v. Sweden*, the defendant had been subject to insulting comments on-line, published anonymously in a blog. He claimed that the non-profit-organization which administered the blog was responsible for the comment. The defendant's claim was not accepted by the Swedish Court, so that he took the case to the European Court of Human Rights, because, according to him, the Swedish Court has failed to guarantee his honour and dignity. The European Court of Human Rights assessed that request as unacceptable and clearly non-based,[64] reasoning that in such cases equilibrium between the right of the individual respecting his private life and the right of freedom of expression of each individual or group that administers an internet portal should be

[59] Yaman Akdeniz, *"Racism on the Internet",* Council of Europe Publishing, December 2009, 83.
[60] Corte di Cassazione, Sezione. V penale, Sentenza 27 Dicembre.2000, n. 4741.
[61] Fatullayev v. Azerbaijan, Application no. 40984/07, Judgement of 22 April 2010.
[62] Renaud v. France, Application no. 13290/07, Judgement of 25 February 2010.
[63] Tierbefreier e.V. v. Germany, Application no. 45192/09, Judgement *of 16 January 2014.*
[64] Pihl v. Sweden, Application no. 74742/14 , (decision on the admissibility).

reached. In this aspect, the European Court of Human Rights noticed that the national authorities had reached a just equilibrium in refusing to charge with responsibility the non-profit-organization for the anonymous comment. This came as a result of the fact that the comment had been insulting, but it didn't have any "hate speech" or incitement of violence.

The European Court of Human Rights has considered the right of the individual to "insult and disturb"[65] the others. So, even a category of insulting expressions enjoy protection from the freedom of speech. On the other hand, this Court has emphasized that it can be considered as necessary in a democratic society the sanctioning or prevention of all forms of expression that disseminate, incite, promote or justify intolerance.[66] So, there is a dividing line between the "right to insult" and the "hate speech" which is assessed case by case.

The penal criminalization of the insult for racist and xenophobic motives not only that shows the border line between what is allowed and what is prohibited, but also highlights that which is judged in the society and that which is accepted. The penal treatment of such behaviours aims at conveying the message that equality and respect for cultural differences (of the identity) constitute the highest values of the society.[67]

The Albanian Law no. 10023, dated 27.11.2008 "On some additions and changes to the Criminal Code"[68], added the figure of the criminal offense entitled "*The threat of motives of racism and xenophobia through the computer system*".[69] This penal offence was included in Section I of Chapter II of the Penal Code, which has as its group object the protection of the life of the individual, placing it in a chronological order after the penal offence of "Threatening", foreseen by article 84n of the Penal Code. The direct object of protection is the protection of the life and health of the individuals who belong to a certain race, nationality, ethnicity or religion.[70] The penal juridical protection covers only the threatening through a computer system of a person or group of persons due to the fact that they belong, or are thought to belong, to a group distinguished by the specific characteristics.[71]

The active subject of this penal offence is motivated by the prejudices against a group where the victim is part of, concretely speaking against a racial, ethnic, or religious group. This penal offence represents the characteristics of threatening foreseen by article 84 of the Penal Code. The provision requires that the threatening fulfil the criterion of gravity/seriousness, i.e., it should imply severe injury or murder.

---

[65] Handyside v. the United Kingdom, Application no. 5493/72, Judgement of 7 December 1976.

[66] Erbakan v. Turkey, Application no. 59405/00, Judgement of 6 July 2006.

[67] Elena Mihajllova, Jasna Baçovska, Tome Shekerxhiev, "Freedom of speech and hate language", Polyesterday, Shkup 2013,. 36.

[68] Law no.10023, dated 27.11.2008 "On some additions and changes to the Penal Code", art. 12.

[69] Penal Code, art. 119/b, which provides for that: *"Intentional public insult, through a computer system, done to a person due to ethnicity, nationality, race or religion, constitutes a criminal offense and is punishable by a fine or imprisonment of up to two years."*

[70] See: Ismet Elezi, *"Penal Justice (Special Part)"*, 2015, 174.

[71] Ismet Elezi, *"Penal Justice (Special Part)"*, 2015, 174.

Whereas according to the explanatory report of the Additional Protocol, the notion of "threatening" could be referred to a threatening which creates fear to the persons to whom it is addressed that they would suffer a grave penal offence, as for example, a threat to their life, personal security or integrity, heavy damage of property, etc., or to their family members. It is up to the Party states to determine what a grave penal offence could be.[72] As it is mentioned above, Albania has defined that a grave penal offence could be murder or severe injury of the person.

The threatening should be addressed to a person for the reason that he/she belongs to a certain group which is distinguished by race, colour, origin, national or ethnic origin, or religion, if it is used as a pretext for any of these factors, or a group of persons which is distinguished by any of these characteristics.[73] There is not any limitation that the threatening should be public. This offence also covers the threatening from private communications.[74]

The elements that differentiate the threatening with racist and xenophobic motives from the threatening in general are the medium used, the computer system and the motive of threatening, as mentioned above and defined as belonging to a certain race, ethnicity, nationality, or religion.

6. Conclusions

The legislative intervention in Albania, regarding the qualification as 'criminal offenses' of the distribution of racist and xenophobic material through a computer system, the threatening with racist and xenophobic motives, the insulting with racist and xenophobic motives, the denial, substantial minimization, approval or justification of genocide or crimes against humanity, was in harmony and almost identical to the directions set out in the Additional Protocol to the Cyber-crime Convention.

The type of the criminal offense of "computer distribution of pro-genocide or crimes against humanity materials" aims at making it clear that facts which have been historically proven should not be substantially denied, minimized, substantiated or justified in order to support these disgusting theories and ideas. Despite the fact that the hypothesis of the criminal norm of the Albanian Penal Code has foreseen the term "*acts that constitute genocide or crime against humanity*", without conditioning it with the recognition of these acts as such by final and binding decisions of international courts, and the assessment whether these acts are of such a nature, should be the starting point for recognizing them as genocide or crimes against equality. The latter should be the object of judicial recognition, and not just the object of academic evaluation, or historically established opinion.

---

[72] Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), paragraph 34.

[73] Yaman Akdeniz, *"Racism on the Internet",* Council of Europe Publishing, December 2009, 83.

[74] Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), paragraph 35.

The dissemination of racist or xenophobic materials through the computer system for the purpose of applying criminal liability requires that they be addressed to the public. Private communications or expressions communicated or transmitted through a computer system are outside the scope of this provision. The communications or expressions such as traditional forms of correspondence are protected by Article 8 ECHR. Whether a communication of racist and xenophobic material is considered a private communication or a dissemination to the public should be determined on the basis of the circumstances of the case. Basically, what needs to be considered is the sender's intention that the message will only be received by the default recipient. The presence of this subjective intention can be determined based on a number of objective factors, such as the content of the message, the technology used, the security measures implemented, and the context in which the message is sent.

The threat with racist or xenophobic motives refers to a threat that creates fear in the persons to whom the threat is directed, that they will suffer the commission of a serious criminal offense, such as affecting the life, personal safety or integrity, serious damage to property, etc., either of the victims, or their relatives. It is at the discretion of the states that are part of the Cyber-crime Convention to determine what constitutes a serious criminal offense. Albania has determined that the 'serious crime' will refer to murder and serious body injury.

Artificial Intelligence in the Courtroom: A question of Humanity and Necessity

Renis Sheshi M.sc.

"In a properly automated and educated world, then, machines may prove to be the true humanizing influence. It may be that machines will do the work that makes life possible and that human beings will do all the other things that make life pleasant and worthwhile."

Isaac Asimov - Robot Visions

1. Introduction

Isaac Asimov, considered by many to be the father of science fiction is the author who invented the term 'Robot' which is in widespread use today when referring to machines capable of mimicking human behaviour. Asimov envisioned a utopian society in which machines performed many of the tasks considered physically demanding, containing a high risk of injuries, tedious or repetitive whereas human productivity was to be confined in jobs and tasks requiring imagination and creativity.

The world of today is on the right track to making this utopic vision of the world a reality, but automatization brings many risks. Technology, if not carefully managed, can turn a dream into a nightmare and what can initially be implemented to free human beings and our creative minds, can eventually turn into an enslaving element.

As of now many of our daily activities are being performed by Artificial Intelligence-powered software. Artificial Intelligence (AI), has been described as *the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. The term is frequently applied to the project of developing systems endowed with the intellectual processes characteristic of humans, such as the ability to reason, discover meaning, generalize, or learn from past experience.*[1]

We have implemented AI systems in many fields of life, we have AI driving our cars, managing our schedules, our houses. It is even being proposed to build an entire city run by AI. Danish architecture firm BIG and Chinese tech company Terminus are

[1] Copeland, B. (2020, August 11). Artificial intelligence. Encyclopedia Britannica.

planning a smart city development run entirely by AI in the south-western Chinese city of Chongqing.[2]

Because of their reliability and their mind-boggling capabilities at storing and analysing data we have come to trust them and utilize them for a multitude of tasks. As these machines are becoming more and more complex and capable of performing tasks previously considered a monopoly of the human mind, our dependency on them is growing exponentially.

Today we have even come to trust our defence systems and our satellites to AI powered software. The expansion of this technology has not left untouched one of the most traditional places, the courtrooms. With the deployment of AI in the courtrooms a main concern is arising. To what extent can the tasks in the courtrooms normally reserved for human beings be transferred over to AI systems? Can and should AI act as judges?

2. Methodology

Our knowledge of Artificial Intelligence in courtrooms is largely based on very limited data. Although the development of technology has been incremental there is not sufficient data to extrapolate concise results. To satisfy the need of this paper, a desk research has taken place to locate cases of implementation of AI in courtrooms and observe their results, at the same time raising ethical questions of further usage. Consequently, to further investigate these questions I have chosen an atypical methodology to fill the gaps of missing quantitative and qualitative data, the Mixed Method Research (MMR).

This paper will use the mix method sequential explanatory approach (Hesse-Biber, 2010) where after the collection of available quantitative data, I will explain in-depth qualitative approach and analyse the factors that fuel the need for Artificial Intelligence in justice deliberation and to what degree it affects humanity in courtrooms all over the world. I believe that a data-driven evaluation is intrinsic to evaluate the role of Artificial Intelligence and its limitations (Creswell & Clark, 2018). By combining quantitative and qualitative data it will enhance description and deeper understanding of the research phenomena (Johnson & Onwegbuzie, 2007).

The first set of data investigated evaluates cases of Artificial Intelligence implementations as a worldwide phenomenon, their merit on evaluating the cases and delivering justice by minimizing the time and raising efficiency, like the case of Australia, a system of AI called the Split-Up system is being implemented by some family law courts. The system uses neural networks to assist judges in their decisions regarding divorce settlements. It incorporates 94 relevant factors to establish what percentage of the common pool each party should receive and uses rule-based reasoning as well as neural networks.

While the second set of data dives on the ethical perspective of this new "tool" appraised for efficiency over humanity. Estonia is taking the implementation of AI in the courts to a higher level. They are experimenting with replacing human judges with machines. In this case, AI would not assist the court in the decision-making process, it

[2] Umberto Bacchi, Reuters December 3 2020, https://www.reuters.com/article/china-tech-city-idUSL8N2IJ24L

would issue a decision. By balancing two sides of the same coin, I offer a unique perspective on the question of AI in courtrooms.

3. Technology in the courtroom

A courtroom is a place built upon the concepts of tradition and stability. It is in that physical and administrative space where the fate of peoples' property, liberty, qualifications, employment etc. are decided. In the courtrooms all around the world, the protection but also the infringement and limitation of human rights including the most fundamental of them such as *the habeas corpus* are ultimately decided. Therefore, predictability comes a long way in ensuring trust in the exercise of justice. Change is the enemy of predictability and hence courts are reluctant to change.

However, lack of change means lack of progress and lack of progress risks making any institution, courts included, highly inefficient. To address the risk of inefficiency courts must change and utilize the advances in technology to be of better service to their users and society as a whole.

Courts in many countries are overloaded with cases. This is especially true in developing nations. These nations usually have rapidly growing populations and are often lacking in infrastructure. A growing population is logically translated into an increase in cases to be adjudicated by the courts be they civil, administrative or criminal cases and not enough personnel or adequate infrastructure to ensure proper case flow. Thus, making the implementation of technology vital for their operation.

To not take advantage of the significant boost in efficiency and quality the utilization of AI provides means to unrightfully deny people better judicial processes and a higher quality of administration of justice. That is why the implementation of Artificial Intelligence capable systems is a necessity and necessity almost always breeds innovation. This is exactly why many courts around the world are in a process of utilizing digital technology to boost efficiency and quality as well. The cutting edge of this technology being of course Artificial Intelligence.

In courts, AI-powered software is being used for what they excel at, analysing and compiling huge amounts of data and drawing conclusions from this data. Their capabilities make them of great use in the management of cases. Specialized software can create statistics, highlight trends from them and provide advanced search options which find specific patterns in the data gathered from cases or other sources of information.

AI can even be used for example to assess applications regarding the fulfilment of formal legal criteria. Since these criteria can be listed and easily checked, AI can even perform this task better than humans can since they are less prone to mistakes and of course lack fatigue.

However, software and hardware used in such applications are hardly deserving of the title AI. AI by definition must be capable of mimicking human intelligence, arriving at conclusions and even learning by itself. That is why it can be used for much higher purposes in the courtroom. AI can be a great assistant to judges. It can analyse court precedents, all the data regarding a certain case and come to a conclusion that can be used as a recommendation for the judges adjudicating the case.

In Australia, a system of AI called the Split-Up system is being implemented by some family law courts. The system uses neural networks to assist judges in their decisions regarding divorce settlements. It incorporates 94 relevant factors to establish what percentage of the common pool each party should receive and uses rule-based reasoning as well as neural networks.[3]

Up to this point, the implementation of AI does not give way to any philosophical questions regarding Humanity, it is merely an instrument for the courts to better perform their duties. However, even this utilization holds a risk for possible violations of human rights. To account for this growing risk CEPEJ (European Commission for the Efficiency of Justice) Adopted on the 4th of December 2018 the "European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment".

This charter provides a major step forward in acknowledging the new reality of AI systems in the courtroom but also in trying to mitigate the risks to human rights. The charter introduces five principles on the use of AI in Judicial Systems and their environment:

1. Respect for fundamental rights. Ensure that the design and implementation of artificial intelligence tools and services are compatible with fundamental rights.

2. Non-discrimination. Specifically prevent the development or intensification of any discrimination between individuals or groups of individuals.

3. Quality and security. In the processing of judicial decisions and data, use certified sources and intangible data with models conceived in a multi-disciplinary manner, in a secure technological environment.

4. Transparency, impartiality and fairness. Make data processing methods accessible and understandable, authorise external audits

5. Under user control. Preclude a prescriptive approach and ensure that users are informed actors and in control of their choices

These principles mainly regard the processing of data by AI and do not cover more ethical and philosophical questions of usage of AI's. These advanced uses are covered in Appendix I of the charter in an In-Depth study on the use of AI in Judicial Systems. However, states generally have a large margin of appreciation when it comes to areas still debated by science and philosophy, the use of AI being one of these.

3.1 Risk of Bias

The "European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment" in Appendix II differentiates between four types of AI usage, uses to be encouraged, uses requiring considerable methodological precautions, uses to be considered following additional scientific studies and uses to be considered with the most extreme reservations. Such classification provides both a prediction and a safeguard against future AI uses that can negatively impact human rights in the courts. It acknowledges the fact that the implementation of AI can greatly aid courts but can also hamper justice by biasing the process.

This is one of the main threats presented today by the utilization of AI-powered software in support of the court activity. Since this technology can still be considered in its infancy, many algorithms can provide inaccurate results. Such results cannot be

[3] Zeleznikow, John & Stranieri, Andrew. (1995). The split-up system: integrating neural networks and rule-based reasoning in the legal domain. 185-194. 10.1145/222092.222235.

double-checked by human counterparts without the risk of losing the convenience and speed of utilizing software in the first place. They are also usually readily accepted as accurate because machines are considered to be highly reliable, do not act in self-interest and simply follow programming.

For example, the use of algorithms in criminal matters to profile individuals is one type of utilization that the Ethical Charter of CEPEJ strongly discourages because a purely statistical approach can and has led to wrong results.[4] Another issue is the fact that people in charge of administering justice do not have the proper insight regarding the manner this AI-powered software operates in the first place and thus cannot properly assess the risk of bias presented by their usage.

In 2016 the NGO ProPublica analysed an algorithm called COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), in use in the United States of America to assist judges in calculating the risk of recidivism for an offender. When a criminal defendant in Broward County, Florida for example was first booked in jail they filled a COMPAS questionnaire. The questionnaire is then inputted in the COMPAS software to generate a core predicting the "Risk of Recidivism" and "Risk of Violent Recidivism." COMPAS scores for each defendant ranged from 1 to 10, with ten being the highest risk.

The analysis conducted by NGO ProPublica discovered that COMPAS software was racially biased. Defendants of African descent were often predicted to be at a higher risk of recidivism than their counterparts of European descent. According to the study, the software mistakenly labelled as low risk defendants of white skin colour who re-offended within the next two years almost twice as often as re-offenders of dark skin colour. The analysis also showed that even when controlling for prior crimes, future recidivism, age, and gender, black defendants were 45 percent more likely to be assigned higher risk scores than white defendants.[5]

It is possible that since 2016 the software has been updated to remove these biases but the study highlights the risk that AI-powered software can present. A judge confronted with the risk of recidivism assessment score by the COMPAS software has no way of knowing that the score is biased and cannot check the process himself. The results coming from a machine can also be treated as more convincing than the evidence presented by the defendant to counter those results since the general opinion is of machines being more reliable than people.

AI-powered software is the cutting edge of innovation in the courts and as such can provide immense benefits but all new technologies hold many risks if not carefully and sensibly applied. A fair and unbiased trial procedure can be adversely affected by flaws in the algorithms as shown above thus making it imperative for careful and intense scrutiny of any such utilization, especially in criminal cases.

4. AI and Law Firms

[4] European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment, CEPEJ, The Council of Europe, pg 73.

[5] Jeff Larson, Surya Mattu, Lauren Kirchner, Julia Angwin ``How We Analyzed the COMPAS Redicivism Algorithm". https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm. https://www.propublica.org/article/technical-response-to-northpointe

AI is being implemented by other members of the courtroom as well. Law firms around the world are utilizing AI to perform many tasks, previously performed by human legal specialists. The American Bar Association lists six categories of tasks that AI is currently performing in the legal arena. [6]1. E-Discovery, 2. Expertise Automation 3. Legal Research 4. Document Management 5. Document analytics and generation 6. Predictive Analytics.

1. E-Discovery, means surveying and analysing several documents and identifying those relevant to a search criterion inputted by the user.

2. Expertise Automation, enables automated answers to simple legal questions. A client can input a question regarding the application of a law, e.g legal requisites for a specific type of contract and the AI-powered software would search its legal database and provide an answer.

3. Legal Research. By taking advantage of the ability of computers to store and analyse huge amounts of data including laws and regulations, research on various topics such as applicable legal provisions can be performed more efficiently.

4. Document Management. Law firms have large databases of information and legal documents such as contracts. These documents need to be managed so that they can be quickly located and retrieved when needed.

5. Document analytics and generation. The software can be used to assist lawyers in drafting high-quality legal documents by using their analytic capabilities on laws, regulations and precedents.

6. Predictive Analytics. This is the most advanced use of AI by law firms and the most debatable one. AI software can be used to analyse all relevant court decisions on a specific issue and based on the inputted facts of the case and other relevant factors such as the judge assigned to the case predict the likely outcome.

The usage that falls under the last category, "Predictive Analytics" is sometimes perceived as abusive. The nation of France has even gone as far as to criminalize such behaviour. Article 33 of the Justice Reform Act is stated that:

"No personally identifiable data concerning judges or court clerks may be subject to any reuse with the purpose or result of evaluating, analysing or predicting their actual or supposed professional practices."[7]

The Constitutional Council of France, the body responsible for approving the Reform for Justice in draft form while assessing whether the above-mentioned prohibition would be constitutional, noted the concerns that the use of such analytics of decisions on a judge-by-judge basis could facilitate strategies to choose courts and judges, which would likely alter the functioning of justice.[8]

In my opinion, such a decision is unwarranted. Judicial decisions are to be made public in all cases, and as such can be studied, analysed or evaluated at will. The predictability of court decisions greatly serves justice. Specific judges are what makes

---

[6] Anthony E. Davis, "The Future of Law Firms (and Lawyers) in the Age of Artificial Intelligence", 02 October 2020. https://www.americanbar.org/groups/professional_responsibility/publications/professional_lawyer/27/1/the-future-law-firms-and-lawyers-the-age-artificial-intelligence/

[7] Law nr. 2019-222 of 23rd March 2019 of programme 2018-2022 for the justice reform, accessed https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000038261761, (non official translation)

[8] McCann FitzGerald LLP, "France bans analytics of judges decisions" 21 June 2019, https://www.mccannfitzgerald.com/knowledge/technology-and-innovation/france-bans-analytics-of-judges-decisions.

up the court and their decisions cannot be considered as a private matter. The criminalization of this practice in my opinion goes against the best interest of justice. As to the concerns that by highlighting specific professional practices of judges it can be used to alter justice by choosing a specific judge in order to increase the chances of obtaining a favourable decision it can be easily addressed by the means in which cases are assigned. If cases are assigned to judges randomly through a lot system, whether it be electronic or manual, then predicting his decision does little to help the litigant gain an unfair advantage. The process of switching judges by withdrawing the case and then presenting it again, can also be eliminated by having the same original judge adjudicate this same case as long as there are no grounds for his/her exemption.

The anticipation of court decisions through AI-powered software is however still in its infancy but even much more advanced AI can fail to analyse the reasoning process behind decisions. As such they cannot anticipate a possible change of judicial practise, or the forming of a new precedent, they can only draw results from the facts of a certain case compared to similar cases and the decision which the specific judge has issued on those cases. This setback was identified in the study carried out by the University College of London on ECHR decisions.[9] According to the study, the formal facts of a case were the most important predictive factor but the accuracy of predictions was on average 79%. Albeit being a high percentage it is far from being certain and since the reasoning behind the decisions cannot be computed, an important determining factor is left out of the equation.

The tool however provides many valuable uses to the courts and as the authors of the study argue a predictive system may be used to rapidly identify cases and extract patterns that correlate with certain outcomes. It can also be used to develop prior indicators for diagnosing potential violations of specific Articles in lodged applications and eventually prioritise the decision process on cases where violation seems very likely. This may improve the significant delay imposed by the Court and encourage more applications by individuals who may have been discouraged by the expected time delays.[10]

5. AI as Judges

Some countries are taking the implementation of AI in the courts to a higher level. They are experimenting with replacing human judges with machines. In this case, AI would not assist the court in the decision-making process, it would issue a decision.

Estonia is one of these countries. In 2019 the Estonian Ministry of Justice tasked a team of experts with designing a "robot judge", an AI that can adjudicate small claims disputes of less than 7000 euros. The litigants can upload the files and information regarding their case and the AI would then issue a decision based on them.[11]

Arguments in favour are many. Magistrates are of very limited numbers. Mainly because they require special training, must meet very strict criteria and are also

[9] Aletras N, Tsarapatsanis D, Preoţiuc-Pietro D, Lampos V. 2016. Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective. PeerJ Computer Science 2:e93 https://doi.org/10.7717/peerj-cs.93

[10] Ibid.

[11] Joshua Park, Harvard International Review, 03 April 2020, https://hir.harvard.edu/your-honor-ai/

considered demanding in terms of financial and supportive treatment. By being human, they are also prone to fatigue. There is a limit of cases a judge can adjudicate per day without affecting the quality of the proceedings. They are also, as all we humans are, mistakable. A judge, no matter how experienced or capable, can fail to notice details, data, or even come to a wrong conclusion or better put a conclusion which he would not have come under different circumstances and which is considered wrongful by him or superior courts.

There is also the question of partiality. Despite all guarantees to the contrary, the many control mechanisms, humans tend to highly value self-interest and social connections. All of these shortcomings are addressed by substituting human judges with AI. Machines are extremely reliable, once they are properly programmed, errors are highly improbable.

They are also impartial. They have no self-interest and thus make for more reliable and trustworthy courts. Trials are also much more predictable since winning is only a matter of calculations, case facts and legal provisions. Parties do not have to take into account the human factor, the fact that the judge might not have eaten properly, slept properly, or his emotional state being affected by other external factors.

In this regard, Artificial Intelligence capable systems make for great judges. However, these artificial judges are not without flaws. AI is not impervious to bias. Software is built by humans, and the core beliefs of the programmers can affect the software and the way it operates. The software makes a decision based on the information inputted and this too can include various biases. The risk of bias is even more pronounced because machines do not act in self-interest and simply follow the programming and they are generally regarded as completely impartial. This makes biases in their operation even harder to detect since no one expects them to exist in the first place. But software is built by humans, and the core beliefs of the programmers can affect the software and the way it operates. AIs are sometimes self-learning but even that process has to be initially taught to them, thus making it possible for the programmers' mentality and beliefs encoded into the software.

Another risk of biasing comes from the data pool. Any software, even an extremely advanced AI needs to be fed information and data for it to operate. Biases could be found in this data and thus leading the AI to false conclusions contaminated by the information pool it has been fed. AI also has limited reasoning capabilities. AI mimics human intelligence and reasoning but cannot replace them. Even the most advanced software and computer in the world, at present, cannot achieve the depth of human reasoning.

Another drawback that comes with the utilization of AI to replace human judges is the input process. The data from the case pending adjudication must be inputted in a specific format that can be read by the software. The form of the documents as well as the entire trial procedure must be built to suit the needs of machine processing as opposed to human convenience.

All of the previously analysed problems can theoretically, eventually be addressed with further advances in AI technology and a better understanding of their utilization, despite the various inconveniences for human users that can arise by tailoring the trial procedure to adjudication by machines.

Some of the problems might be addressed by providing a two-tier system with the first tier being adjudicated by an AI judge and the decision then reviewed by human judges in the second tier. This system however would still be disputable because human judges in the second tier would be biased in their decision-making process by the decision issued in the first instance. As previously analysed in the article people tend to trust AI and law specialists are also at an inability to thoroughly understand and check the algorithms to be able to spot any possible biasing in them. The biasing in the programming of the AI judges in the first tier would then be passed on to the human judges in the second one, making for a flawed judicial verdict of two instances, which would then be even harder to contest and analyse for flaws. It would however diminish the possibility of software and a human mistake by making the verdict a collaboration of software and human judgement.

5.1 The human judgement

One crucial issue regarding a non-human judge that quite possibly cannot be resolved by advances or adaptation, is the inability to fully replicate the human judgement. The process of arriving at a verdict or judgement about a case is in itself strictly human and one of the highest and most complicated intellectual operations a human mind can perform and as such, it cannot be replicated by an artificial system.

A human judge decides through a complicated intellectual process that involves not only information regarding the case or knowledge of the legal provisions but also reflects his core beliefs and the way he perceives the world and society. Most importantly a judge makes a decision based on empathy. It is not enough to simply calculate by comparing the facts in a case against a legal background. A judge has to understand the personality and behaviour of the parties involved.

A human judge can detect a lying witness or a generally untrustworthy one, he can detect ill intent in the actions of a party but most importantly he can understand them, all of the people in a dispute in the various roles they assume as a defendant, plaintiff, witness, attorney, prosecutor because he is one of them. A human judge shares the same basic instincts and many of the emotions and drives with all other participants in a trial.

Finally, he has to understand what led the litigants to the choices they made up to the dispute. Because in understanding he differentiates between valuable members of the society, people who are generally good and act in good faith but happen to make a bad choice in a certain moment under certain influences of events and those who act based on antisocial intents. The difference between the two is more pronounced in criminal trials and translated in the type and length of the punishment but is also applicable in civil matters regarding liability and amount of pecuniary compensations for example.

An AI-based system no matter how advanced will always lack empathy because it will always lack a basic understanding of what it is to be human. An understanding of human emotions and perception. The other crucial issue regarding the substitution of human judges is a philosophical and sociological one. It is a matter of enforcing a judgement. To adjudicate a case does not mean to merely issue a decision, it also means to enforce that decision and to enforce a decision that has implications for the rights and property of the parties involved is to exert sovereignty and power over human beings.

It means to enable a machine through a digital procedure in many cases to limit the rights of human beings, to remove their property, to deprive them of their freedom etc. When a party loses a trial, the decision comes under intense scrutiny by it and to allow a machine to issue the decision can be perceived by the losing party as being denied dignitary treatment.

This makes the process of adjudication fundamentally human because only humans and on very limited and special occasions can exert power over other humans. Court decisions also carry with them a great deal of symbolism. It is through them that society as a whole expresses its mentality, its perception of itself and the way it regards various behaviours. Society is human and cannot be duly represented by software because the software is unable to fully implement a human society's constantly evolving opinion on punishable behaviour. Laws and regulations provide a guideline and a stringent one for the judges to implement, however, there is always ample room for interpretation when applying them in a specific case, to a specific person. A machine can be programmed to follow and strictly implement the laws and regulations in a given situation but is unable to make those fine differentiations between similar cases and to adjust its decision accordingly. No two people are alike and no two cases are the same despite the similarities that many may share. It is exactly in these small details that the mentality of a judge reflecting that of the entire society he belongs to, affects the case and makes the human judgement superior.

6. Conclusions

The utilization by the courts around the world of the best that current technological advances can offer is a necessity to keep up with the growing population and number of cases. To utilize technology to the full extent is to fulfil an obligation to society for a better and more efficient judicial system. AI-powered software is the cutting edge of digital technology and is helping courts around the world to better manage the cases, assess legal criteria and even support judges in the decision-making process. However, this technology is still in its infancy and if not managed carefully can lead to biases and unfair trials.

Law firms are also utilizing AI for a myriad of legal tasks enabling them to substitute several human legal specialists with software that can accomplish the same tasks much more swiftly and without the limitations of human beings. This utilization is also not without risks, and raises concerns for alteration of justice by picking specific judges in order to have a better chance of a favourable verdict. Such a problem can however be addressed by implementing a few administrative changes in the administrative process of case assignment.

The utilization of AI in the court should however be restricted to it acting as an assistant to the human judge. The substituting of human judges with artificial ones, in our opinion does not conform with the fundamentally human nature of the judicial system. Despite the many advances in AI, substituting human judgement with algorithmic ones is improbable and presents a risky deviation from the standard of humanity to be expected in judicial verdicts. The advantages offered by artificial judges in terms of impartiality and effectivity fall short of accounting for the lack of empathy,

risk of software bias, breach of symbolism and overall lack of humanism in a process designed by humans for humans.[12]

AI as an assistant to the judge is a more preferred scenario offering fewer risks and raising fewer philosophical and sociological questions about the monopoly of the human mind in exercising sovereignty and authority over fellow humans. It also adheres to the fundamental structure of our human society and paves the way for a more efficient and fair judicial system.

[12] Candidate for judge at the School of Magistrates of Albania. He graduated from the Law Faculty of the University of Tirana with a M.Sc in Criminal Law in 2018 and a bachelor in law in 2016, renissheshi@yahoo.com.

Questioning of the witness and the defendant by technological means

Prof. Assoc. Dr. Klodjan Skenderaj and Arbesa Kurti M.sc.

1. Introduction

Evidence with witnesses is provided for in the Albanian Code of Criminal Procedure as one of the types of evidence. The object of evidence is any fact related to the charge, guilt, conviction of the defendant, civil liability and the facts on which the application of procedural norms depends. The witness is asked about the facts that are the object of evidence and he/she cannot testify about the moral position of the defendant, except when the case is related to facts that are valid for determining his personality in relation to the criminal offense and social danger.

As a rule, the evidence may extend to the relationship of kinship and interests that exist between the witness and other parties or witnesses, as well as to the circumstances, the verification of which is necessary to assess his or her credibility. The witness is questioned about certain facts and s/he cannot testify about what is said in public nor express personal opinions, except when they cannot be separated from the evidence for the facts.

However, the Code of Criminal Procedure also provides for cases of questioning of the defendant where the rule is that the defendant is asked if s/he makes a request or when asked and s/he gives consent to be questioned. As a rule, the defendant is questioned at the hearing, but there are special cases when the defendant is questioned remotely through audiovisual links, according to international agreements ratified by law. In this paper, we will analyze the cases of questioning with special techniques or remote questioning of both witnesses and defendants, i.e. cases when they are not present at the court hearing.

The paper will analyze the ways of questioning witnesses and defendants according to the provisions of the Code of Criminal Procedure, referring at the same time to the national and international legal framework

ratified by Albania, regarding the use of technology tools to perform these procedural actions. It should be noted that the use of technology tools should not infringe on one of the fundamental rights enjoyed by the defendant in criminal proceedings, such as the right to defend and challenge evidence before a trial panel.

By applying the qualitative and quantitative method, the legal analysis will be combined with concrete examples of questioning witnesses and defendants by technological means, in order to identify the problems and give concrete recommendations for improving the situation.

2. Questioning of juvenile witness and defendant

The questioning of the juvenile witness is provided by the Albanian Code of Criminal Procedure (the Code). Thus, it is provided that the questioning of a juvenile witness under the age of 14 is done without the presence of the judge and other parties in the environment in which the juvenile is, and when possible, through audiovisual means. Therefore, in this case, in the question of minors under 14 years of age, when possible, depending on the audiovisual equipment, it is provided that his/her testimony be made not in the courtroom but in the environment where the juvenile is.

It is obligatory for the juvenile to be questioned through a psychologist or teacher, not in the presence of the court and the parties. This provision is intended for the psychological non-harm of the juvenile from article 361/a of the Code.

On the contrary, the questioning of a juvenile witness aged 14 to 18 is carried out through the presiding judge, thus making it possible to guarantee the dignity and personality of the juvenile, especially in cases where we are dealing with juveniles and victims of crime. The presiding judge is acquainted with each question in advance - without informing the juvenile about it - and then, under the obligation to avoid the wording that causes the juvenile coercion, emotions or even suggestion, the presiding judge addresses the juvenile questions so as not to disturb his/her peace.

Pursuant to Article 155 of the Code, every person has the capacity to testify, except for the mentally and physically ill people, who are unable to testify, as well as excluding those who are incompatible with the duty of witness. In this respect, the juvenile also has the capacity to testify, being potentially likely to be a witness.

Thus, the rule in favor of the juvenile is provided, providing that the audiovisual means bring without distorting the knowledge of the juvenile. Furthermore, if the juvenile was questioned during the preliminary

investigation and his/her statements were recorded by audiovisual means, they are used as evidence, if the defendant and the defense counsel give their consent, thus being formed as acts that can be read and entered into the proceedings.

Whereas for the statements given by the juvenile during the preliminary investigations, recorded by audiovisual means can be processed with permissible readings, if the defendant's defense counsel had the opportunity to question the juvenile through a psychologist, educator or expert. In this respect, the practice rightly argues that:[540] "*... the testimony given by the minor A.F. before the court was conducted in the presence of the psychologist. In court, the juvenile was questioned by the parties in the process in a different environment from the room where the defendant was staying (without visual contact) due to the negative impact that the direct presence of the defendant could have on the testimony that the juvenile had to give, but her questioning has been conducted with an audiovisual link, enabling the defendant and the prosecutor to see the juvenile witness from the monitor located in the courtroom where the defendant was present, at the time when she was giving her testimony and together they asked the witness question in view of their procedural position. The request for testimony from the juvenile in another courtroom was submitted by the prosecution. The request was also supported by the defense. The testimony given by the witness was technically realized within the court through an audiovisual link respecting the legal requirements provided by Article 361 / 5-7 of the Code of Criminal Procedure as well as the legal requirements provided by Article 8 / a of the Law "On the organization and the functioning of the Serious Crimes Courts...*"

Furthermore, in another case it was reasoned that[541]: "*... the decision of the Court of Appeal of Durres, against which the defendant E.K. is appealing, is legally unsubstantiated. In erroneous application and non-compliance with the criminal procedural provisions, the Court of Appeal of Durres has changed the decision of the Elbasan Judicial District Court and found the defendant guilty. Thus, contrary to Article 152 of the Code of Criminal Procedure, the Court of Appeals has given a predetermined value to the report made by the citizen D.C. This report was drafted by the Judicial Police Officers in violation of the provisions of the Code of Criminal Procedure. Specifically, the Judicial Police Officer who received the report, in the conditions when the reporter was a minor, had to respect certain rules for obtaining the juvenile's testimony, namely the requirements of Article 361/5 of the Code of Criminal Procedure, for the questioning of minor witnesses, so to take the report to this citizen in the presence of parents or specialized persons, such as psychologists, teachers, etc. Contrary to this provision, the report was received in the presence of a Judicial Police agent named D.K.*"

While in the case of questioning the defendant, the rule is that he is questioned at the hearing in the presence of all parties participating in the

[540] Decision no. 77, dated on July 19, 2017 of the Court of First Instance for Serious Crimes, Tirana
[541] Decision no. 23, dated January 20, 2010 of the Criminal College of the High Court

process. Therefore, the defendant is asked if he makes a request himself or through his defense counsel, while if he is asked to be questioned, he must give consent to be questioned. This is because in case the defendant does not ask to explain or be questioned, he cannot be forced to state. This and in function of the right he is provided with that if he does not ask to be questioned then he cannot be forced to be questioned, in other words he has the right not to be questioned.

Meanwhile, in cases when the defendant asked to be questioned by the prosecuting authority, he must ensure his presence at the hearing in order to proceed with the receipt of statements. However, even in cases where a defendant wants to be questioned, we may find ourselves in a situation of various obstacles, which make it impossible for him to be present at the hearing. In these circumstances, it is provided that a defendant in a related proceeding, prosecuted or serving a sentence abroad for another criminal offense, in cases where his extradition is refused can be proceeded with his interrogation remotely via audiovisual link, according to international agreements. In these cases, the obligation is that the foreign state where the defendant is located must guarantee the participation of the defendant's defense counsel at the place where his interrogation takes place. This is in function of the right that the defendant is provided with to be assisted by a lawyer, where the latter is also the guarantor of the defendant's rights in the criminal process. If the prosecuting authority does not guarantee the presence of the defendant's defense counsel, then the sanction may be the absolute invalidity of the procedural action of taking evidence, which in this case is the question of the defendant.

This invalidity may affect the entire criminal process and consequently may lead to the invalidity of the decision taken at the end of the trial. Thus, the presence of the defendant's defense counsel must be understood so that the latter has an effective opportunity to assist the defendant by guaranteeing an effective and legal defense in defense of the interests of the defendant he represents.

The Code of Criminal Procedure provides for an express case of absolute invalidity of procedural acts, i.e. when the provisions related to the summoning of the defendant or the presence of defense counsel when it is mandatory, are not respected. To this end, in order to avoid undermining the due process of law, the Courts must take care to strictly comply with the legal provisions.

3. Remote Testimony

Paragraph 7 of Article 361 of the Code provides for the possibility of obtaining evidence remotely. Thus, the witness can be questioned remotely,

inside or outside the country, through the audiovisual link, respecting the rules of international agreements but also the provisions of the Code of Criminal Procedure. In case of remote interrogation, the person authorized by the court is required to stay at the place where the witness is located and verifies his/her identity, as well as takes care of the regular conduct of the interrogation and the implementation of protection measures. These actions should be reflected in the minutes. It is also envisaged that remote interrogation may be carried out in the case of a victim of a sexual offense, a victim of a trafficking offense or an offense committed within the family if the victim so requests.

In the case of remote interrogation of a witness who is abroad, the procedure is initiated by means of an international notarized instrument, as a form of mutual legal assistance in criminal matters. Thus, pursuant to Law no. 10193, dated December 03, 2009 "*On jurisdictional relations with foreign authorities in criminal matters*", local authorities through the traditional instrument of letter of formalities can address foreign authorities in order to question the witness, defendant or expert, also through development of hearings by telephone and audiovisual connections.

The procedure followed in these cases is that the Ministry of Justice, after giving way, forwards the acts to the district prosecutor where the letter must be executed through the General Prosecutor within 10 days from the receipt of the acts. But in urgent cases, the Ministry of Justice may forward the acts to the district prosecutor, while notifying the General Prosecutor. The District Prosecutor then submits the request to the court to dispose of the execution of the writ of summons by decision according to the rules of the Code of Criminal Procedure. However, beyond the above-mentioned rule, it is provided that[542] the letter of intent can be forwarded directly through domestic and foreign judicial authorities, in cases of urgency. The above-mentioned law also stipulates that the domestic judicial authority, at the express request of the foreign judicial authority, provides information on the time and place of execution of the summons. In these cases, the court may allow representatives of foreign judicial authorities to take part in the taking of evidence and to direct questions to the person being questioned, in accordance with the rules of the Code of Criminal Procedure.

Regarding remote questioning, or in other words, the conduct of remote hearings, it is envisaged that they may be telephonic or audio-visual. Domestic judicial authorities may request foreign judicial authorities to remotely question a witness or expert abroad, by telephone or audiovisual. It should be noted that the request of domestic judicial authorities to foreign authorities must meet certain conditions which are

[542] This rule is stipulated by Article 15 of Law no. 10193, dated on December 03, 2009 "On jurisdictional relations with foreign authorities in criminal matters"

identified as follows. Thus, the request must contain the name of the local judicial authority and the persons who will conduct the hearing, as well as the reasons why it is not possible for the witness to attend the hearing in person.

It should be understood that the court should take measures that even if the witness is called and did not appear then, to address the request to foreign judicial authorities for their questioning abroad on behalf of the Albanian state or the remote questioning of the witness located abroad, via telephone or audiovisual connections.[543] However, even in this case, the witness must give consent to carry out this form of taking evidence. If the witness does not give his /her consent, the audiovisual connection cannot be made, just as the foreign judicial authority cannot be questioned.[544]

On the other hand, in cases when a letter of intent is submitted to the Albanian authorities for execution by a foreign authority, the same rule is provided, where the local judicial authorities execute the letter of intent in cases when: first, the witness or expert does not want or has no opportunity to submits to foreign judicial authorities, and has given consent for the hearing to take place in this form; secondly, when the competent court has approved the request of the requesting state for the conduct of the hearing in this form. The remote questioning of witnesses or experts is carried out by local judicial authorities in compliance with the rules of international agreements and the provisions of the Code of Criminal Procedure.

4. Special interrogation techniques

Article 361 / b of the Code provides for special interrogation techniques by protecting the collaborator of justice, the protected witness, the infiltrated person and the witness with a hidden identity. Protected witness also called "the witness of justice", - pursuant to Article 3, paragraph 2 of Law no. 10173, dated October 22, 2009 "*On the protection of witnesses and collaborators of justice*", as amended - implies a person who, as a witness or injured person makes statements or testifies to facts and circumstances that constitute evidence in a criminal proceeding and that, because of these declarations or testimony, is in a dangerous situation.

Meanwhile, the collaborator of justice is a person who is serving a criminal sentence or is a defendant in a criminal proceeding for crimes committed in collaboration, who is in a dangerous situation, due to

[543] Islami H., Hoxha A., Panda I., "Commentary on the Criminal Procedure", amended, page 567, Morava Publishing House, Tirana 2012

[544] The notification of the witness must be done through a letter of intent in accordance with the "European Convention on Legal Aid in the Criminal Field" and the Additional Protocol, ratified by the Assembly of the Republic of Albania with Law no. 8498, dated on June 10, 1999

collaboration with justice, statements or evidence of facts and circumstances that constitute object of evidence in the same criminal proceeding or in a related proceeding.

An infiltrator or undercover person is a judicial police officer or agent involved in a criminal group to individualize members of the group and gather the information needed to investigate and detect serious crimes, concealing cooperation with the police or his / her duty as a police officer. A secret witness (witness with a hidden identity, anonymous witness) is the person who testifies against the defendant who is accused of committing serious criminal offenses such as acts with terrorist intent, terrorist financing, concealment of funds and other assets, which finance terrorism, etc., in cases when the witness protection program is not implemented.

In cases where a secret witness will be questioned, a special way of interrogation is provided where the prosecutor submits a request to the presiding judge in an envelope marked "Confidential: secret witness". The prosecutor's request also sets out the reasons for the need to use one or more of the specific interrogation techniques. It is only the presiding judge who has been informed about the true identity of the secret witness and verifies the capacity and incompatibility with the duty of the witness. The court examines the request of the prosecutor in the deliberation room and decides with a reasoned decision within forty-eight hours from the submission of the request.

In the case of a secret witness, the court, pursuant to paragraph 2 of article 361 / b of the Code of Criminal Procedure, orders the taking of appropriate measures to make it possible for the face and voice of the person not to be distinguishable by the parties. This means that the court must take all technical measures not to distinguish the face of the witness but also the use of technological means to change the true voice of the secret witness.

5. Victim Questioning

A victim of a criminal offense is a person against whom a criminal offense has been committed or on whom the consequences of the criminal offense are aggravated. Thus, it is provided that the victim of the criminal offense enjoys a number of procedural rights where it is generally stated that he has the right to seek prosecution of the perpetrator, to communicate in the language he understands, to choose counsel, to seek at any time information on the state of the proceedings, as well as to submit requests to the proceeding body, to be notified of the non-initiation of the proceedings, the termination of the case, the beginning and the end of the trial, etc.

However, one of the rights enjoyed by the victim of a criminal offense is to be heard by the court, even when neither party has requested that she be called as a witness. A juvenile can also be a victim of a criminal offense, and in these cases, it is a juvenile victim. In the case of a juvenile victim, it is stated that he/she has the right to be accompanied by a trusted person, has the right to maintain the confidentiality of personal data, to request through the representative that the trial take place without the presence of the public.

The juvenile victim is questioned immediately by specialized persons and, when possible and appropriate, the conversation is recorded by audiovisual means. Audiovisual recording of a juvenile victim can be used as evidence in criminal proceedings and is evaluated together with other evidence. In cases where the juvenile victim is under 14 years old, the conversation takes place in environments suitable for him/her.

While the victim of the criminal offense can be the victim of sexual abuse or the victim of trafficking in human beings. In these cases, it is provided that in addition to general rights this category of victims of crime also has some additional rights such as: to be questioned without delay by a judicial police officer or prosecutor of the same sex; refuse to answer questions about the private sphere, which are clearly unrelated to the offense; seek to be heard through audiovisual means.

6. The ratio between the statements given during the preliminary investigation in relation to the evidence given at the hearing

The issue of the value ratio of the statements given during the preliminary investigations in relation to the evidence given before the court has been raised many times in practice. The Code of Criminal Procedure also provides for the rebuttal of testimony [545], where the rule is in order to rebut, in whole or in part, the contents of the testimony or when the witness refuses to testify, the parties may use the statements previously made by the witness before the prosecutor or judicial police and which are part of the prosecutor's file, but only after the witness has already testified on the facts and circumstances which are being rebutted. Such statements shall not constitute evidence in itself regarding the facts declared by it, but may only be taken into consideration by the court to determine the reliability of the person examined.

[545] Article 362 of the Code of Criminal Procedure

In *Luca v. Italy* the European Court of Human Rights (ECtHR) argues that[546]: "*... As the Court has stated on a number of occasions, it may prove necessary in certain circumstances to refer to depositions made during the investigative stage (in particular, where a witness refuses to repeat his deposition in public owing to fears for his safety, a not infrequent occurrence in trials concerning Mafia-type organizations).*

As such, admitting such depositions as evidence would not constitute a violation of Articles 6 & 1 and & 3 (d) of the Convention. However, in cases where an indictment and conviction rely solely or mainly on depositions made by a person whom the accused has not been able to question directly or indirectly, either during the investigation phase or during the trial, then the rights of defense are to the extent that it is incompatible with the guarantees provided for in Article 6. Following its jurisprudence in relation to similar cases, the Court emphasized that it was clear further that a question-and-answer session with the prosecution witnesses, in the sense of under the Convention, must necessarily take place in court. Although such evidence should normally be taken in court, some special circumstances such as those mentioned above may make it difficult, or even impossible, to repeat, in public court, statements made during the investigation stages. In such cases, Article 6 requires that only the accused should be given an appropriate opportunity and concretes to challenge the evidence in question even during the court hearing…"

The same reasoning is based on decision of the Criminal College of the High Court[547], where it is reasoned that: "*The Criminal College brings to attention the decision regarding the case "Breukhoven v. Czech Republic", no. 44438/06, dated July 21, 2011 when, the ECHR outlines clear jurisprudence, regarding the possibility and value of the use of acts, as well as the qualification of the accusations by the courts of fact.*"

According to the jurisprudence established by the court, all evidence must be taken in a public hearing, in the presence of the accused, in order to be able to challenge them. There are exceptions to this principle, but they should not violate the rights of the defense, which according to the general rule set out in paragraphs 1 and 3 (d) of Article 6 ECHR, require that the defendant be given an adequate and appropriate opportunity to present the objections of the case and to question the witness, either at the stage of statements or at a later stage. In particular, the rights of the defense are limited, to the extent that it is contrary to the requirements of Article 6 ECHR, if the sentence is based solely, or in a decisive manner, on the statements of a witness, of which the accused has not had the opportunity to be informed and oppose during the investigation or trial[548].

[546] See decision, of ECHR LUCA v. ITALY (application no. 33354/96 and decision date February 27, 2001)
[547] See decision no. 196, dated June 12, 2013 of the Criminal College of the High Court
[548] See decision of ECHR, AM v. Italy, no. 37019/97, § 25, ECHR 1999-IX

Following its position, the ECtHR: "*... concludes that the domestic courts based the applicant's conviction for trafficking only on the testimony of witnesses who did not appear in court and against whom neither the applicant nor his lawyer, they had not had the opportunity to ask them, at any other stage of the proceedings...".*

Considering the achievements of the ECtHR in the cited practice, with values of jurisprudence, the Albanian Criminal College finds in the trial sand achievements of Court of Appeals of Shkodër, the same shortcomings, not only in respecting the requirements of due process, but even in the misjudgment of the substantive law, conditioned by the violations committed. The court considers that the statements read in court contain only information about the situation in the pub and whether prostitution took place there, but not about specific elements of trafficking.

Taking evidence out of court, such as cases of taking evidence remotely by audiovisual means or in cases of taking the testimony of an anonymous witness, can raise problems in the context of violating due process. This is because Article 6 of the ECHR does not explicitly address the problem of the anonymous witness, it must be said that there is a bias in favor of this practice, which, although beneficial to justice, does not allow the defense to question the prosecution witnesses. In this case, a psychological fact, a serious risk to life for fear of retaliation and a legal record such as the principle of adversarial proceedings referred to in Article 6 paragraph 1 and especially Article 6 paragraph 3 of the ECHR are confronted.

In *Kostovski v. The Netherlands*[549], it is reasoned that: "*all the evidence must be produced in the presence of the accused at a public hearing with a view to adversarial argument. This does not mean, however, that in order to be used as evidence statements of witnesses should always be made at a public hearing in court ... As a rule, Article 6 requires that an accused should be given an adequate and proper opportunity to challenge and question a witness against him, either at the time the witness was making his statement or at some later stage of the proceedings.*"

It should be noted that the ECtHR does not in principle condemn testimony made by a person whose identity is secret. On the other hand, in practice it respects the spirit of due process: at one point or another, except in exceptional cases, the accused should be able to question the witness, specifically using the system that modifies voice and spirit.

In the case of *Ludi v. Switzerland*[550] the ECtHR addresses the problem of undercover agent, who constitute a special category of anonymous witnesses. The Court has concluded that there has been a violation of Article

[549]See decision of ECHR, Kostovski v. The Netherlands on November 20, 1989 (application no. 11)
[550] See decision of ECHR, Ludi v. Switzerland, on June 15, 1992 (application no. 238) the ECHR

6 ECHR, but does not in itself condemn the practice of infiltration. The judges convicted the Swiss authorities because in this case it had been possible for the confrontation to be organized in such a way as to preserve the anonymity of the police officers. However, in principle, infiltration and anonymity, consequently is not disputed.

In *Doorson v. The Netherlands*[551] the conditions for the use of anonymous testimony are clearly defined, confirming in principle a limit to it: there must be sufficient grounds to guarantee the anonymity of witnesses and during the examination of an anonymous witness the judge should intervene: the judge should develop an idea of the credibility of the witness; there must also be a significant extent on other evidence not derived from anonymous sources (application of confirmation theory).

In the case of *Van Mechelen v. The Netherlands*[552] police officers during the proceedings refuse to testify by visual contact. However, all measures were taken to ensure the authenticity of their testimony: The procedure followed for questioning them was that the investigating judge, the witness and a registrar were together in one room, and the defendants, their lawyers and the Advocate General in another. The defendants, the lawyers and the Advocate-General could hear all the questions asked to the witnesses and their replies through a sound link. The statements of the witnesses were repeated by the investigating judge to the registrar, who took them down. All 11 anonymous police officers were identified only by numbers (001, etc.). The Court reiterated that "*the use of anonymous witnesses should be resorted to only in exceptional circumstances with the Convention*". It added that the judge should intervene to verify the credibility of the witness. The defense should be able to present its doubts about witness statements, which means that it should be able to question them and establish its own judgment on their position. So, we can say that the Court requests that there be contact between the defense and the witnesses, which would allow the defense to observe the reactions of the witnesses to the questions posed, but in this case, there was no other conclusive evidence and the defense could not have questioned the witnesses in their presence, at a time when the proceedings did not sufficiently compensate for this obstacle.

The ECtHR even points out that these special witnesses, i.e., police officers, "*are obliged to obey the executive authorities and should be used as anonymous witnesses only in exceptional circumstances*". According to this decision, the possibility of hiding the identity of the witness from the defendant is not excluded.

Based on the jurisprudence of the European Court of Human Rights, it is an essential condition for a proper legal process of reviewing and taking

[551] See decision of ECHR, Doorson v. The Netherlands (on March 16, 1996)
[552]See decision of ECHR , Van Mechelen v. The Netherlands (on April 23, 1997)

evidence, which must be done in accordance with legal provisions. Taking evidence contrary to these predictions undermines the process. Equally important is the protection and questioning of witnesses, victims, to whom certain specific rules must be applied, especially when there are allegations that may endanger their health, their lives.

7. Conclusions

Allowing remote testimony even though it is provided as such by the Albanian Criminal Procedural Code should also guarantee the right of the defendant to defend and explain himself before the court. Moreover, one of the main principles of the criminal process is that of adversarial proceedings, i.e., where the defendant must be defended even by asking remotely, the witness or the victim of the criminal offense.

It follows from all the jurisprudence of the ECtHR that in order to accept evidence either remotely or anonymously, certain conditions must be met in advance. First, there must be sufficient reasons to guarantee the anonymity of the witness, for example because revenge must be avoided, or because there is a need to still hold the witness for prosecution or other investigations. In taking remote testimony, adversarial proceedings must be observed (decisions *Doorson, Ludi, Van Mechelen*).

Second, violations of the right to protection must be minimized, which means that the anonymous witness or the one who testifies remotely must be heard by an independent and impartial judge who knows his or her identity and who can give an assessment of the reasons justifying the concealment of identity and the reliability of the statements. The defense should be able to ask the witness directly, while it is not necessary for the defense to be able to personally observe the anonymous witness's reactions to his direct questions.

Third, the sentence should not be based solely or to a large extent (mainly) on anonymous statements or even only on evidence given remotely. The use of technological means for interrogation, the development of the judicial process in an audiovisual manner must be carried out by special means, which not only guarantee a regular legal process, but must enable the confidentiality of information and identity of the victim, witness, etc.

ESSAY

Towards a criminal statute of the internet and multimedia: criticalities and perspectives of a system in constant evolution*

Mattia Romano Ph.D. Cand.[553]

Abstract: *Starting from the end of the last century, criminal legislation has had to progressively adapt to technological and media evolution. Thus the need arose to draft rules aimed at cyber-security and to face the advent of cyber-crime. Whenever the legislator has deemed it necessary, it has introduced new types of crime that did not exist before the time of digitization. Over time, however, it has become necessary for the legislator to make the cases already introduced or those newly introduced more and more specific. Certainly, a catalyst of this innovation of the criminal system was the strong change due to the opening of the internet public which triggered a necessary legislative change aimed at fighting cyber attacks on the network and, more generally, all so-called cyber crimes. Moreover, the cybernetic reality seems to have completely overcome the traditional spatial and temporal categories, in so doing it is necessary to find a new lexicon for the formulation of the cases. Over the years, the doctrine has worked hard to put in place purely dogmatic activities, aimed at researching and developing the theoretical principles of legal institutions related to "cybercrime". However, at present, there is no internationally recognized definition of "computer crime" or "computer related crime" or "cyber-crime". We must therefore consider the future of such a sensitive and important subject.*

* This article is the result of a re-elaboration of the intervention given by the author at the International scientific conference held on April 8, 2022.

553 Mattia Romano, Ph.D.Cand. in criminbal law, University eCampus (Italy).

To understand how important is to create an internet statute and web crime, it is necessary to analyse the evolution of the fragmented and usually inorganic criminal legislation on the Internet and the needing of protection of the users of the multimedia world.

The role of the law is, in fact, to standardize and regulate human phenomena.

As a result of that, law needs to be upgraded day by day following the evolution of the communication methods.

We have all seen how technology has improved during the mid-twentieth century and how the world has changed with it.

We can all understand now the importance and the weight of this new technological era.

Therefore, these phenomena has created a need for a precise and well balanced legislation especially because nowadays this enormous quantity of knowledge and information is currently available for everybody using a simple pocket device.

To sum up, we are basically trying to keep up with this unstoppable technological and multimedia progress by attempting to regulate this new "digital society", trying to create a "legislation 2.0", capable of regulating the new communicative phenomena that characterize the advent of the new millennium.

And among the various branches of the law that have been faced with changes there is certainly criminal law.

Through criminal law, in fact, we have tried to raise some borders in order to limit the illegitimate behaviours created by this spring of new communication technology.

Since 1993 Italy has been trying to legislate this new phenomena with the Law 547, that has amended the penal code and the criminal procedure code in order to sanction computer crimes[1].

[1] The first Italian legislation on telematic crimes was introduced by law 547 of 1993, with the related amendments to the criminal code and the code of criminal procedure. Added to these are the amendments made by Law 48/2008 on the Ratification and execution of the Council of Europe Convention on Cybercrime, made in Budapest on November 23, 2001.

As a matter of fact, nowadays computer data is extremely important but at the same time extremely dangerous:

- from one side we are now able to use this new technology as a fighting crime method, in order to take down terrorist networks by intercepting online communications, through this new technological exploits such as a Trojan virus;
- from the other side, the criminal use of technology may lead to a violation of our fundamental rights and, sometimes, our personal security.

It is therefore the duty of criminal law to protect us from hacker attacks, from the illegal use of our own data whether stored regularly or seized by means of Trojans or from all other trickeries that may come from the web or the media.

As a result of the evolution of the use of technology, criminal law has attempted to punish illicit behaviours, already rooted in society, and the advent of entirely new forms of crime.

In short, we can simply call it: cybercrime.

As an example of how this technological improvement has alterated and widen the possibility of committing crimes we can think about bullying that has become cyberbullying; we can think about the ease of distribution of child pornography; and we also have to consider the need for a greater protection of data and sensitive information that needs to be developed, thus giving rise to the so-called cybersecurity;

However, according to many, the cyber law of our internal system still appears today in an excessively embryonic phase of evolution.

In fact, it is unable to support the criminal legislator in the correct classification of some human behaviours characterized by a strong social impact.

But the problem is that we are currently using laws that are not keeping up with the growth of this phenomena called cyberspace.

Cyberspace represents a "non-place" where information can be transferred, reaching a very large number of individuals simultaneously.

We can clearly understand that there is a huge qualitative and quantitative gap compared to the most obsolete communication methods.

We have completely changed how we have to handle information nowadays: the web grants us access through an endless stream of information.

But if this stream goes through the hands of people that have become experts of the web, this so-called hackers, this can lead to an unfair and wrongful use of this data: so our sensitive information can be in danger.

In conclusion, it is clearly necessary that we have a need of a constant update to the criminal legislation and, sooner rather than later we need to create an exhaustive single text: a “criminal statute of the internet and multimedia”.

Once concluded this necessary premise, let's move on to the analysis of the concrete difficulties found by the legislator in the drafting of the incriminating rules on cyber crime.

I want to analyse only one of the multiple problems involving this branch of law.

I think that this example may be useful to give an idea of the extreme complexity of drafting laws in this peculiar matter.

The discipline of the crime of unauthorized access to a computer system, in Italian “accesso abusivo a sistema informatico”, pursuant to article 615-ter of the Italian Criminal Code, concerns the hypothesis in which a hacker illegally accesses another computer system.

This discipline refers to the structure of the case of the violation of domicile ruled by art. 614 of the Italian Criminal Code, showing a terminology that does not appear to be adequate for the type of conduct to be sanctioned.

In particular, the legislator has used the expression “introdursi”, in English "to infiltrate".

It is the same expression used by the legislator in the text of art. 614 of the Italian Criminal Code to punish who physically goes into a home, or into a building.

So this does not seems to be proper as it refers to a "non-place" such as cyberspace and, more generally, the computer world.

As already mentioned, in fact, cybernetic reality has completely overcome the traditional spatial categories, thus rendering the term "introduction" anachronistic and inadequate.

So, it's clear that the legislator in 1993 has appropriately decided to introduce art. 615-ter but, at the same time, it's evident his inexperience and his "distance" from the idea of this so-called crime 2.0.

And the inexperience of the legislator explains the consequent not particularly suitable use of terminology for the new context.

In conclusion, to recall the title of the conference, one of the most important legal challenges in the digital era is the implementation of law drafting techniques and identification of an appropriate lexicon to rule this particular matter.

The problems related to the spread of technology are certainly not limited to the mere need to identify new legislative techniques.

For example, it is always necessary to identify new methods of ascertaining the criminal conduct committed by means of IT tools and to guarantee the highest reliability of the investigative results.

The challenges are therefore varied and the jurist must constantly keep up with the times.

Some notes on interpretative problems in bankruptcy crimes. Comparative aspects of the Albanian and Italian discipline

The question of the declaration of bankruptcy by the civil court in relation to the pre-bankruptcy crimes

Prof. Assoc. Dr. Ersi Bozheku

1. Introduction: criminal offenses in the field of economy in general.

Criminal offenses can be divided into several groups based on the legal goods (objects) they protect. In this context, we can identify several macro-groups whose purpose is to protect certain segments of goods or legal interests.

This is how we can generally identify the criminal offenses that have the individual as the object of protection. Among these crimes, we can identify several subgroups such as crimes against life (such as murder), those against health (wounds), against individual freedom (kidnapping), etc. Among the many macrogroups that can be found in the criminal code, criminal offenses against property and the economy are included.

It is about those acts that discipline the punishment of those facts that damage or endanger property, private or collective, or the economy. These offenses include a wide variety of criminal offenses: from theft or fraud to fiscal evasion or criminal offenses in the field of bankruptcy. What essentially unites these acts is the fact that their goal is to protect society and individuals from criminal offenses that have an impact on the economic framework.

2. General assessments on criminal offenses in the field of bankruptcies.

The topic of criminal offenses in the field of bankruptcy is one of the most complicated in the panorama of criminal law all over the world. Their correct application requires a good knowledge and an interpretative coordination between the provisions provided in the criminal code, those of the law on commercial companies and the articles provided by the law on bankruptcies.

From their origin, which has its roots in Medieval law ([1]), until today, the penal provisions in the field of bankruptcies aim to rebuke and punish economic initiatives by entrepreneurs or commercial companies which carry a higher risk than the physiological one of the commercial initiatives, or cases where these risks have been intentionally or negligently disregarded.

In cases where the activities of the entrepreneur or the management subjects of a legal entity have been totally contrary to the objectives of the legal entity or have been able to violate the guarantees of its creditors, the instrument of the bankruptcy law is no longer efficient.

Then in addition to this, the legislator (in every country of the world) defines a number of criminal provisions which aim to punish in this plan the entities, natural persons (such as administrators, general directors, etc.) who have brought the legal entity into a state of bankruptcy.

It is reasonable to determine immediately, that the criminal provisions in the field of bankruptcies constitute an *extrema ratio.* They are provided by the legislator in relation to those facts for which the provisions present in the legal system in the field of the law of obligations, the law of commercial companies and the law of bankruptcy are not suitable. In order to respond to certain behaviors that have a high level of violation of the legal good of credit (good that this is only a habit of the legal good of the property), the Albanian legislator has provided certain provisions within the criminal code and specifically articles 193, 194, 195 and 196 of the Criminal Code. ([1]).

In Italy, bankruptcy offenses were originally contemplated within the Bankruptcy Law (Royal Decree March 16, 1942, n. 267), later rewritten by Legislative Decree 9 January 2006, n. 5 (Organic reform of the discipline of insolvency procedures), even if the novel did not affect the criminal provisions referred to in Title VI, dedicated, precisely, also to bankruptcy crimes. The main distinction within bankruptcy was between simple

bankruptcy (Articles 217 and 224, Bankruptcy Law) and fraudulent bankruptcy (Articles 216 and 223, Bankruptcy Law), relating to a different intensity of objective and subjective gravity.

The discipline of bankruptcy crimes has been reshaped following the recent publication of Legislative Decree 12 January 2019, n. 14, containing the "Code of business crisis and insolvency in implementation of the law of 19 October 2017, n. 155 ", with the aim, as stated in the press release published on the Government website, to organically reform the discipline of bankruptcy procedures, with the main purpose of allowing an early diagnosis of the state of difficulty of the companies and safeguarding the entrepreneurship of those who face a business failure due to particular contingencies.

As a result of this regulatory intervention, the discipline of bankruptcy and other bankruptcy crimes is brought back into Title IX of the new Code, dedicated to "Criminal provisions" (Articles 322-347), without this entailing any repeal of the legislation contained within the bankruptcy law, as well as the criminal provisions on bankruptcy.

In Italy, bankruptcy can be proper or improper, depending on whether the fact of simple or fraudulent bankruptcy is committed by a bankrupt individual entrepreneur or by a person other than the subject subject to judicial liquidation, such as, for example, an administrator, a general manager, a statutory auditor or liquidator of a trading company. In the context of its own bankruptcy, the acts committed by the partners with unlimited liability must also be brought back, as can be seen from art. 328, according to which the decree declaring the bankruptcy of a general partnership, limited partnership and limited partnership for shares, also produces the bankruptcy of unlimitedly liable partners.

Both the facts of simple bankruptcy and fraudulent bankruptcy can be committed on assets or on books or accounting records. In the first cases we speak of asset bankruptcy (or bankruptcy in the strict sense), while in the latter case we speak of documentary bankruptcy.

3. Announcement of the bankruptcy procedure in the structure of criminal offenses in the field of bankruptcy.

A key moment for the understanding and interpretation of bankruptcy criminal offenses is related to the identification of bankruptcy, which, as we mentioned in the Albanian legislation, must be understood at the moment of announcing the bankruptcy procedure. Only if we have a bankruptcy in the formal plan (so declared by the court), then they can examine whether or not it is the result of a criminal offense. In other words, the determination of the status of "bankruptcy", using the terminology of the Albanian code, constitutes the essence for the determination or not of criminal offenses of bankruptcy, as it constitutes an objective legal condition that must be fulfilled in order to proceed to the examination of criminal offenses in this area.

So, the question arises, what is the role of bankruptcy (more correctly, the decision to declare bankruptcy proceedings) in the framework of the structure of criminal offenses in the field of bankruptcy?

Regarding the pre-bankruptcy criminal offenses, when the court announces the opening of bankruptcy proceedings by decision, the objective condition for their application is automatically fulfilled (Articles 193 and 194 of the Criminal Code). Regarding these crimes, the announcement of the bankruptcy procedure takes the role of a condition that must be fulfilled for the examination and punishment of the facts in the plan of pre-bankruptcy provisions.

Regarding post-bankruptcy criminal offenses, the announcement of the bankruptcy procedure constitutes an essential element for their realization (Articles 195 and 196 of the Criminal Code). Therefore, in connection with these acts, the announcement of the bankruptcy procedure constitutes an essential element in the framework of the structure of these acts. For reasons of publishing space, we will not deal with the analysis of post-bankruptcy criminal provisions. We will return to them in a second moment, which will have as a specific focus the analysis of articles 195 and 196 of the Crimanl Code.

In Italy, one issue, which has always been debated in doctrine and jurisprudence, is that relating to the role assumed by the bankruptcy ruling from the civil judge in the context of the crime of pre-bankruptcy.

Nulla quaestio, with regard to the post-bankruptcy case: in relation to the latter, in fact, it is agreed that the sentence in question assumes the role of a prerequisite for the crime "having to precede the typical conduct, and being a source of legal effects: first of all, the dispossession of the assets of

the entrepreneur and his submission to a series of obligations towards the bodies responsible for the procedure".

The vexata quaestio revolves around the phrase "if it is declared bankrupt", contained within the articles 216 and 217 of the Italian Bankruptcy Law.

4. Announcing the bankruptcy procedure as an objective condition for reprimanding and punishing pre-bankruptcy criminal offenses in Albania.

From a broader analysis of the structure of criminal offenses in general, it emerges that not all the elements defined by a legal provision are essential elements of the criminal offense. The latter, as is well known, are only those facts or behavior determined by the legislator within the legal provision, the realization of which leads to the realization of the criminal offense since the concrete fact realized is identical to the abstract one defined by the provision. The world doctrine of the last hundred years has shown that if they are missing, there is no criminal offense. Their realization or not depends on the author of the fact. If a subject shoots a pistol and takes the life of an individual, he has knowingly committed the crime of murder. His behavior, i.e. the realized fact, is a solution of the author who chooses between two possibilities, committing the crime and maintaining a correct behavior, and acts in its realization. At the moment that the typical fact described by the provision is realized, we have the commission of the criminal offense. So, the elements of the core of the criminal offense, or its essential elements, apart from the fact that they must be present for its confirmation, are nothing but behavior that the subject carries out in the context of a criminal offense.

However, there are many criminal offenses which carry in their core an element which cannot be considered an integral part of the core of the typical behavior required by the provision. We are talking about those crimes where their various elements do not describe behavior related to the action or inaction of the author, but facts that do not depend on the author of the criminal offense.

In these types of provisions, only when the condition provided by the legislator is fulfilled, then the criminal offense can be considered

fulfilled. Otherwise, behavior that conforms to the criminal provision cannot bring about its affirmation as long as the condition is not fulfilled.

Conditions are elements that are outside the core of the criminal offense, understood as the typical fact (action or inaction, causal link and consequence) that the legislator requires for the affirmation of a criminal offense. Conditions are an objective element, where **their realization does not depend on the author of the fact** but on other external elements that are not under his control.

Emblematic in this context are the pre-bankruptcy criminal offenses, which have as their object the examination and punishment of behaviors carried out before the announcement of the opening of the bankruptcy procedures of the legal entity. The object of examination of pre-bankruptcy criminal offenses (Articles 193 and 194 of the Criminal Code) is the impact of the behavior of entities with management skills of the legal entity on its economic capabilities. If these behaviors, that we will deal with later, must be of a pathological nature (not legal, on these aspects see the following pages), have resulted in an irreversible economic disability which was later recognized by a court decision, we are facing a situation of provoked bankruptcy. If the behavior of the entities with the most management skills has influenced the deepening of the economic crisis of the legal entity by contributing to the creation of a situation of irreversible economic incapacity, we will face the criminal offense Article 193 of the Criminal Code. Just as we will have the criminal offense of concealing the state of bankruptcy (Article 194 of the Criminal Code) when the entity with managerial capacity of a legal entity enters the latter into economic-commercial relations with third entities, when it is in a situation of irreversible economic incapacity.

In all these cases, the behavior of the active entity in relation to the economic situation of the legal entity is subject to review. The decision to announce the bankruptcy procedure is not part of this binomial, but simply a legal moment that, when it recognizes a state of economic incapacity of the legal entity, realizes an objective condition for the consideration of the criminal offenses in question.

As can be easily understood, the bankruptcy procedure does not constitute an essential element of these acts. The opening of the bankruptcy procedure depends not on the active subject of the criminal offenses provided for in this framework, but on a decision of the bankruptcy court.

The active entity has no possibility to determine whether or not bankruptcy. This is a formal moment that is formally pronounced by the competent court which by means of a formal act, the decision to open the procedure, recognizes and affirms in the legal plan a situation of economic incapacity of a subject.

The perpetrator of criminal offenses in the field of bankruptcy (we are talking about pre-bankruptcy offenses) can realize facts that reduce the economic capabilities of the legal entity (wrong investments, excessive personal expenses, embezzlement of funds, etc.) leading it to economic crisis; however, the opening of bankruptcy proceedings, as a formal act, does not depend on it but on the court.

From a conceptual point of view, bankruptcy (more correctly in our legislation the terminology decision to open bankruptcy proceedings should be used) constitutes an objective condition of punishment; therefore, in order to carry out a criminal offense and to punish its active subject, this element must first be fulfilled: the court formally pronounces the decision to open bankruptcy proceedings. Without formal bankruptcy (that is, without a declaration of the opening of bankruptcy proceedings), there is no criminal offense despite the fact that there is a misuse of the company's assets by entities with management skills within it. For these reasons in the world doctrine, bankruptcy is defined as an objective condition of criminality that is outside the core of the basic elements of pre-bankruptcy criminal offenses ([1]).

Consequently, as long as the legal person is not declared financially incompetent by means of a decision that decides the opening of the bankruptcy procedure, the illegal acts within it that affect its property cannot be examined criminally in the plan of criminal provisions in the field of bankruptcies (Articles 193 and 194 of the Criminal Code). And this is because there is no fulfillment of the condition, the court decision decreeing the opening of the bankruptcy procedure, i.e. of that objective fact that does not depend on the author of the criminal offense, without the fulfillment of which the criminal offense cannot be examined criminally.

Only after the economic-financial situation of the legal entity has been formally declared, i.e. after its inability to guarantee the right to credit to its creditors has been declared by a court decision (where the tax burden of the State is also included) with the opening decision of the bankruptcy procedure, pre-bankruptcy criminal offenses can be examined ([1]).

Let's take an example: the construction company Z is full of debts with the banks, it does not pay taxes or salaries. Its property was misused by the administrator who took a large part of it for himself and his family. As long as the company has not been declared unable to repay debts by a court decision, i.e. bankruptcy proceedings have not been opened, there can be no talk of bankruptcy criminal offenses such as induced bankruptcy (Article 193 of the Criminal Code). After the declaration of its economic incapacity by court decision, the said criminal offense arises against the administrator for the mismanagement of the assets of the company when it was operational. The same conclusion also applies to cases where the legal entity enters into an economic-commercial relationship with a third party when it is objectively in a state of irreversible economic incapacity, but a court decision announcing the opening of bankruptcy proceedings has not yet intervened. The criminal offense provided for by Article 194 of the Criminal Code it cannot be considered completed as long as the decision to open the bankruptcy procedure is not made.

The declaration of bankruptcy by court decision (more precisely, based on our legislation on the opening of bankruptcy proceedings, since from that moment the entity is formally declared incapable of fulfilling its obligations towards creditors), constitutes the condition for the affirmation, examination and punishment of the act's criminal pre-bankruptcy. From that moment these can be called accomplished. From that moment, the conduct and the facts realized by the governing bodies of the legal entity in the plan of pre-bankruptcy criminal offenses can be taken into consideration. ([1]).

So, from the opening by court decision of the bankruptcy procedure, the facts realized by them during the activity of the legal entity can be analyzed to see if they intentionally or not led to a state of irreversible economic crisis. Thus, from the declaration of bankruptcy, after the condition required by articles 193 or 194 of the Criminal Code has been met, the actions or facts realized by the apical bodies of the legal entity during the period when it exercised its economic activity can be evaluated. If, later during the investigation, it turns out that these behaviors carried out during the period when the legal entity was in a sufficient economic condition have influenced the birth or deepening of an irreversible economic crisis within it, which culminates in the court's decision to open bankruptcy procedure,

the entities that have carried out those behaviors or facts will be criminally liable for the offense provided for by Article 193 of the Criminal Code.

Let's take an example: in 2018, company A spends about 2 million euros for purchases that were not included in the framework of its activity and which go in favor of the administrator or one of his relatives. From that moment it goes into an economic crisis (they don't forget to pay the creditors) which is irreversible. In 2021, company A, after the request to open bankruptcy proceedings by one of its creditors, is declared in bankruptcy proceedings.

Until 2021, there will be no realization of the criminal offense provided for by Article 193 of the Criminal Code (provoked bankruptcy), even though the fact in 2018 has put the company in a state of economic incapacity. Only in 2021, upon the announcement of the opening of the bankruptcy procedure, does the criminal offense in question arise. From that moment, the facts realized by the top entities of the company up to the date of the announcement of the bankruptcy procedure can be started and examined. If, during the investigation and trial, it turns out that these have led to an irreversible economic crisis, recognized and formally announced by the bankruptcy court, we will affirm the responsibility of the authors.
The same conclusion applies to cases where the legal entity enters into economic-commercial relations with a third party when objectively it is in a state of irreversible economic incapacity, but a court decision announcing the opening of bankruptcy proceedings has not yet intervened.

In conclusion, the announcement of the decision to open the procedure constitutes an objective condition for the examination and punishment of bankruptcy criminal offenses. Although the facts realized by the managers of a legal entity may be harmful to its assets and contradict the interests of creditors as they violate their guarantees, criminal proceedings cannot be taken against the perpetrators if the condition in question is not fulfilled. The facts of the managers of the legal entity that have brought about the misuse of its property take criminal forms, that is, they take on the power of harming (or offending) the legal good protected by the criminal-bankruptcy provisions, which rests on the right of credit of the creditors whose guarantees they should not decrease, when we have a court decision that formally declares the opening of the bankruptcy procedure. Until that moment, the facts in question do not have a degree of offense to the legal good, since the realization of the formal condition (court

decision) is missing. As long as there is no announcement of the opening of the bankruptcy procedure, the illegal actions of the administrators of the company cannot receive criminal value in the implementation plan of the criminal bankruptcy provisions ([1]).

5. The debate on the relevance of the bankruptcy declaration from the civil court to the whole of fraudulent patrimonial bankruptcy crimes in Italy.

In Italy, traditional doctrine favors a qualification of the bankruptcy sentence form the civil judge in terms of extrinsic punishment condition pursuant to Article 44 of the Criminal Code, since "the judicial consecration of the state of insolvency does not contribute to defining or increasing the offense of the crime, representing, so to speak, a requirement that, by the will of the legislator, remains confined to the margins of the case of pre-bankruptcy without the need to be invested on the etiological and psychological level by any connection with respect to the conduct set out in Articles 216 and 217 of the Italian Civil Code. Residing in reasons of political and criminal expediency, the choice of subordinating the entrepreneur's punishment to the filing of bankruptcy".

Traditional jurisprudence appears differently.

In particular, with the historic Mezzo judgment of 1958, the United Sections affirm that "the declaration of bankruptcy from the civil Tribunal, while constituting an essential element for the punishment of bankruptcy crimes, differs conceptually from the objective conditions of actual punishment because, while these presuppose a crime that is already structurally perfect, from an objective and subjective point of view, instead it actually constitutes a condition for the existence of the crime, in relation to those commissive and omissive facts prior to its pronouncement, and this because it pertains so strictly to the 'legal integration of the criminal case, to be qualified the facts themselves, which outside the bankruptcy, would be criminally irrelevant, as facts of bankruptcy ".

More recently, it is stated that the bankruptcy sentence represents "an indispensable element for attributing the qualification of crimes to otherwise lawful or criminally indifferent conduct"; consequently, the disposition acts committed by the entrepreneur and the other acts

enumerated by art. 216 l. bankruptcy. as a hypothesis of bankruptcy, they assume a criminal relevance only through the pronouncement of the bankruptcy sentence.

Furthermore, it should be emphasized that, although the declaration of bankruptcy is a constitutive element of the case in point, it does not constitute an event of the crime and, therefore, does not necessarily have to be connected by a psychological link to the agent; equally irrelevant is the etiological link between "the conduct that took place with the implementation of a dispositive act - which affects the equity consistency of a commercial enterprise - and bankruptcy".

6. The announcement of the bankruptcy procedure as a formal condition in the structure of pre-bankruptcy acts in Albania: economic incapacity as an essential element of these acts.

Starting from the premise that the announcement of the bankruptcy procedure constitutes an objective condition for the punishability of pre-bankruptcy criminal offenses, as it recognizes and affirms on the formal-legal level a situation of economic incapacity of an entity, for example a commercial company, it cannot to be the object of the psychological element of the criminal offense. So, the fact of the realization or not of bankruptcy does not enter the sphere of will (purpose). The active subject of the criminal offenses provided for by articles 193 and 194 of the Criminal Code cannot foresee or want bankruptcy. It does not depend on him, but on a formal court act. It would be absurd to think that the will can embrace the concept of opening bankruptcy proceedings which is a formal (court) act.

In some writings we have evidenced within the Italian doctrine, as in the conceptual plan (and this reasoning applies to all legislations throughout the world) the object of the psychological element in the framework of criminal offenses in the field of bankruptcies cannot be a formal act of an authority, but, in coherence with the basic principles of criminal law, a fact. Only the facts that are committed or can be committed by the author and their consequences in terms of fact, and not the legal ones that simply recognize and declare a factual situation, can be the object of the psychological element ([1]).

The essential fact in the field of bankruptcy is the economic inability of the legal entity to pay its obligations to creditors. These situations are concrete facts, while their recognition by the court with the decision announcing the opening of the procedure is nothing but an act of recognition of a concrete situation. Realization of this formal act by the court fulfills the condition for the affirmation, examination and punishment of criminal offenses in the bankruptcy field. However, it is the economic disability that derives from the illegal behavior of the active subject of these criminal acts ([1]).

The constituent elements of the criminal offenses in question must be analyzed in relation to the consequences they have brought to the economic and financial situation of the legal person and more specifically whether they have influenced the creation of an irreversible crisis or aggravated a previous crisis situation by bringing about a situation his disability, later recognized by the court with the decision to declare the bankruptcy procedure.

More precisely, the criminal court must analyze whether the acts or facts carried out by the management entities of a commercial company (on which there has been a decision to declare bankruptcy proceedings) have led it to a state of economic incapacity. The latter must be the subject of judicial evidence both in relation to the moment of its occurrence and in the causal plan in relation to the actions or inactions carried out by the active entity. If these have influenced the birth of the economic crisis, causing a state of irreversible economic disability, or have contributed to the deepening of a previous economic crisis, influencing the material plan in its deepening, then we can talk about the criminal offenses of provided by articles 193 and 194 of the Criminal Code (pre-bankruptcy criminal offense). Thus, the economic disability of the legal entity is the consequence of the criminal offense and must be subject to assessment by the criminal court. ([1]). In other words, the court must evaluate whether the economic crisis a) is irreversible; b) whether it was created as a result of a misadministration, characterized by the implementation of intentional acts by its leaders, which has had consequences the significant reduction of the financial capacity of the legal entity, leading it to a state of irreversible economic disability.

Of course, the impact of this conclusion is also clear in terms of the psychological element of the criminal offense ([1]).

The object of intent on the part of the active subject in Article 193 of the Criminal Code seems to be the fact that he realizes, which must be foreseen and required by him, as well as the impact that this behavior has on the economic situation of the legal entity. More specifically, the active entity must or can imagine the consequences that the realization of a fact can have on the economic situation of the legal entity that it manages.

7. The bankruptcy declaration form the civil court in the dynamics of the crimes of fraudulent bankruptcy in in the recent jurisprudence of the Italian Suprem Court.

In Italy, only recently the Supreme Court, in adherence to the prevailing doctrine, comes to define the declaration of bankruptcy as a condition of punishment.

In particular, within the Santoro ruling, it is stated that "the declaration of bankruptcy does not in any way aggravate the offense that creditors suffer as a result of the conduct of the entrepreneur". Therefore, this declaration "as an event unrelated to the typical offense and the agent's sphere of will, represents an extrinsic condition of punishment [...], which restricts the area of the criminally offense, imposing the penal sanction only in those cases in which to the conduct of the debtor, which is in itself offensive to the interests of creditors, is followed by the declaration of bankruptcy ". However, it should be noted that the same ruling recalls the conclusions already reached in the Passarelli judgment of 2016 with which Sections joined "while not qualifying the declaration of bankruptcy as an objective condition of punishment, this role has unequivocally assigned to it (subsequent event and stranger to whom the punishment is subordinate) ".

Following the Santoro ruling, the jurisprudence appears divided. Some rulings, for example, have expressly adhered to the line inaugurated by the sentence de qua. In other cases, on the other hand, there was a revirement of the judge of legitimacy who, adhering to the traditional orientation, established that "in the matter of bankruptcy, the declaration of bankruptcy is a constitutive element of the crime and not an objective condition of punishment; therefore, the offense is completed in all its

constitutive elements only in the event that the subject, who has also previously committed theft of company assets, is declared bankrupt".

In any case, the "wavering" trend we have witnessed in recent years does not allow us to consider the contrast between doctrine and jurisprudence to be completely overcome.

Hence the need for legislative intervention on the subject, which can attribute "a coherent and constitutionally solid dogmatic position to the bankruptcy sentence.

8. Conclusions.

The purpose of this intervention was aimed at highlighting some profiles of homogeneity and diversity with regard to the regulation of fraudulent bankruptcy in Italy and Albania. Despite the proximity between the two countries, the two legal systems for bankruptcy are very far apart. This depends not only on the different formulation of the norms but also on the different degree of cultural development of the doctrine and jurisprudence in the two countries. In view of this, however, various points of contact between the relevant provisions cannot be reported; the bankruptcy civil judgment in Italy or the opening of the bankruptcy civil judgment in Albania constitute an objective condition of punishment in both legal systems. However, if such a datum is undisputed in Albania, at least according to the analysis proposed by the relative doctrine, this cannot be said in Italy where the debate on the subject is still very heated and I still do not find a univocal position within the jurisprudence of the Supreme Court.