Reverse Engineering between Technological Innovation and the Risk of Counterfeiting and Piracy: Conceptual Delimitations and Legal Implication

Bianca Cristina (Pop) Borgyos [1,*], Miorița Ungureanu [2], Raul Florentin Drența[3]

Abstract: *Reverse engineering occupies a dual position in the contemporary technological landscape. On one hand, it acts as a catalyst for innovation, facilitating interoperability, performance analysis, and the development of alternative solutions; on the other hand, it can be misused when applied for illicit purposes, such as counterfeiting and piracy. This article aims to clarify the conceptual boundaries between legitimate and illegal practices of reverse engineering through an analysis of the relevant literature and the applicable regulatory framework. The section on legal implications examines the tension between intellectual property rights and the need for technological progress, highlighting the challenges arising from the absence of uniform regulatory standards. The conclusions seek to formulate a balanced perspective that integrates both legal and ethical dimensions, providing guidelines for establishing a coherent framework in which reverse engineering can remain a driver of innovation without undermining intellectual property protection or market fairness.*

Keywords: *Counterfeiting, Intellectual property, Legal implications*, *Piracy, Reverse engineering, Technological innovation*

1 INTRODUCTION

In an era of technological globalization and accelerated commercial exchanges, reverse engineering has increasingly become a widely used tool, both for legitimate purposes—such as performance analysis, interoperability, or re-manufacturing—and for illicit purposes, including piracy and counterfeiting [21].

When it exceeds the legal boundaries of intellectual property, this practice entails economic and ethical disadvantages for entities engaged in innovation, constituting a barrier to both technological advancement and fair competition. In the United States, hundreds of billions of dollars are lost annually due to intellectual property theft. These enormous losses reflect the cumulative impact of practices such as unauthorized cloning, exploitation of licenses without authorization, and the reduction of research and development costs for infringers, enabling them to flood the market with competitively priced products. These losses can be analyzed from two interdependent perspectives:

- direct economic impact – loss of anticipated sales revenue, undermining of market share, deterioration of profitability, and the potential complete withdrawal from the market of affected innovative companies;
- long-term strategic impact – erosion of competitive advantage due to the need for additional investment in protective measures, adoption of more expensive technologies, or relocation of production for security purposes, all of which negatively affect the sustainability of business models [12].

Thus, in many cases, owners of industrial innovations have implemented protective measures against copying through reverse engineering. For example, in the field of computer science, there is a focus on safeguarding software against unauthorized modification (tamper-proofing), obfuscation (the deliberate hiding of code logic, structure, or meaning), and watermarking (the embedding of a signature or hidden information within a digital file) as complementary approaches designed to prevent piracy, reverse engineering, and unauthorized code alterations. Tamper-proofing must be robustly integrated into the application to withstand sophisticated attacks; obfuscation requires a balance between reducing code readability and maintaining functionality; and watermarking must be subtle enough to remain intact within the code while still being practically detectable. Collectively, these strategies provide a defense-in-depth, essential for effectively countering modern threats, where adversaries may operate both at the level of monitored code and through reverse engineering of the internal logic of digitally distributed programs [16].

Obfuscation techniques are employed in the field of software security to protect applications against reverse engineering, piracy, and unauthorized copying. They are particularly applied in industries where the source code or internal program logic constitutes a valuable asset, ranging from commercial applications and video games to critical systems in telecommunications, banking, or defense. The need for these methods arises from the fact that, once distributed, software can be analyzed and modified by malicious actors, leading to economic losses, compromise of intellectual property, and security risks. Hybrid obfuscation combines three complementary techniques: encryption of strings, including mathematical equations and repeated structures, to mask the meaning of the text; renaming of system language keywords into Unicode codes, complicating automated code comprehension; and transformation of identifiers into “junk” code, removing any clear semantic meaning and increasing the code’s informational density unnecessarily. In experimental testing, the reverse engineering process was compared on unprotected Java applications and applications protected with the mentioned technique. Evaluations were based on result correctness, syntax errors, program flow tests, and the names of identifiers, methods, and classes. The results indicate that, in the case of hybrid-obfuscated code, reverse engineering tools encountered significant difficulties: the generated code was almost unreadable,

and its performance was clearly degraded compared to the original version [1].

In electronics, protective techniques have been developed to conceal the functionality of integrated circuits. In this context, the TAO (Technique for Algorithmic Obfuscation) method aims to safeguard electronic circuits against reverse engineering attacks. Unlike other solutions applied only in the final stages of design, TAO operates at an early stage, at the level of algorithm description (in languages such as C). Essentially, the method deliberately modifies the code by introducing false branches, artificial dependencies, or masked constants, making the design difficult for an attacker to understand. Only the holder of the secret key can restore the design to its correct and functional form. The primary goal of TAO is to hinder the efforts of those attempting to illegally copy or analyze a hardware design. Because the modifications are applied directly at the algorithmic level, attackers cannot easily decipher the system's logic merely by examining the final circuit. However, this protection comes at a cost: obfuscated circuits may occupy more chip area and exhibit reduced speed. Even so, the method remains valuable, particularly for complex projects, where the benefits of security far outweigh these disadvantages [19].

A more rigorous conceptual and legal distinction is required between the legitimate practice of reverse engineering, as a tool for analysis and technological innovation, and illicit acts of copying or counterfeiting, which constitute the abusive use of industrial outputs without respecting intellectual property rights. From a legal perspective, it is essential to delineate a clear conceptual boundary between reverse engineering as a practice permitted under certain conditions and acts of copying or counterfeiting, which represent explicit violations of intellectual property protection regimes. From an ethical standpoint, it is necessary to differentiate between the use of reverse engineering as a legitimate method for learning and technological progress and its exploitation for illicit purposes, which undermines the integrity of the innovation process and the fairness of competitive relations. The importance of addressing this issue arises from the inherent ambiguity of the process: the same tool can generate transformative innovation when used for compatibility purposes, or it can lead to fraudulent copying when the goal is illegal trade or unauthorized technology exploitation. Analysis must encompass technical, legal, industrial, and ethical aspects, as well as the structural relationship with piracy and counterfeiting [7].

2 REVERSE ENGINEERING: CONCEPTUAL DELIMITATIONS

2.1 Scope of Reverse Engineering

Reverse engineering lies at the intersection of three fundamental domains:

- intellectual property law, which protects technical and creative expressions through copyrights, patents, and trade secrets.
- competition law, which encourages knowledge dissemination and competition through compatibility and technological alternatives. For example, [31] permits reverse engineering for interoperability, while [32] allows reverse engineering for legitimate purposes without restrictive contractual agreements, provided that the information is not used for unfair competition or direct replication;
- emerging technologies, particularly in the context of Artificial Intelligence and adaptive systems, where the distinction between legitimate analysis and imitation becomes increasingly blurred. AI models functioning as "black boxes" (i.e., not revealing how they make decisions or how they are constructed) are often accessed through online interfaces without providing direct information about the source code or training data. Nevertheless, by repeatedly querying such a model—sometimes thousands of times—it is possible to infer essential information about its operation: how it was constructed, the type of logic it uses, and the nature of the data it has learned from. This practice, technically referred to as "model extraction," may initially appear as a legitimate method of analysis. However, in many cases, it is used to recreate or clone the original model without the creator's permission. In such situations, the boundary between lawful research and fraudulent copying becomes extremely narrow. If the outcome is a competing product that mimics the behavior of the original, this constitutes a potential infringement of intellectual property rights [10].

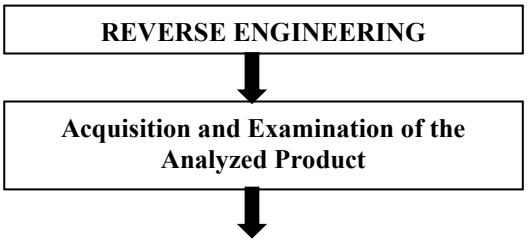
2.2 Methodological Approach in Reverse Engineering

Reverse engineering is a multidisciplinary technical-analytical practice that involves the systematic process of deconstructing an existing product, system, or technology to understand its functional components, internal architecture, manufacturing process, or operational logic [4].

Unlike classical "top-down" development, which progresses from concept to product, reverse engineering follows a "bottom-up" approach, reconstructing the underlying idea, logical model, or operational algorithm starting from the finished product [6].

This approach can be applied across multiple domains—hardware, software, mechanical, electronic, pharmaceutical, or biological products—and can serve a wide range of objectives, from compatibility analysis, reconstruction of lost documentation, ensuring interoperability, security auditing, and redesign for optimization, to unauthorized imitation of protected technologies [13].

The main stages of the reverse engineering process are illustrated in the fig. 1



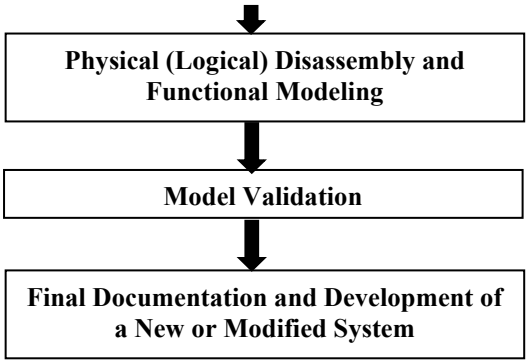


Fig. 1 Main Stages of Reverse Engineering
Source: own elaboration

The acquisition of the product, representing the first step in reverse engineering, involves the legal procurement of the target product. This may include purchasing the physical device, legally extracting the binary code that enables computers to store, process, and communicate information, or obtaining authorized access to the executable code that allows the computer to actually run a program. It is essential that this process complies with intellectual property legislation. During this step, a preliminary audit of the product is also conducted, assessing its physical condition, verifying the integrity of its components, and evaluating its suitability for subsequent physical analysis. In the case of software, this involves checking the binary format, compatibility with analysis tools, and the availability of documentation [2].

The specific activities are:

- acquisition of the product or software: purchase, valid licensing, or public access [14]. "*Reverse engineering has always been a legal means of obtaining trade secrets embedded in mass-marketed products, but only if the product was legally acquired*" [20];
- preliminary non-invasive observation: before any disassembly or decapsulation, document visible characteristics such as labels, markings, software version, and physical interfaces;
- creation of the initial technical record: inventory of visible components, versions, interfaces, and observable behaviors;
- identification of useful reference points for future analysis: determining locations where advanced methods can be applied [8];
- establishing the purpose of the activity: determining whether the process will serve interoperability, security, documentation, or unauthorized replication [27].

Physical or Logical Disassembly and Functional Modeling represents the second step in reverse engineering. When the object of reverse engineering is a mechanical product, such as a mechanical body or an industrial component, a systematic method of physical disassembly is applied. This involves [18]:

- component removal while respecting the operational sequence and avoiding damage: components are disassembled screw by screw, element by element, documenting the arrangement for subsequent reassembly or CAD (Computer-Aided Design) modeling;
- precise measurements of each part: dimensions, shapes, thicknesses, and materials. Tools such as calipers, micrometers, 3D scanning, or tomography are used to capture exact geometries;
- creation of a CAD model based on measurements and images, aiming to obtain an accurate and detailed digital representation of the product;
- analysis of functional dependencies: some components cannot be removed without extracting others. A precedence matrix is employed to optimize the disassembly sequence (minimizing time, risks, and complications). The precedence matrix is a tabular representation indicating the order or dependencies between activities or steps. Each row and column represent an activity and the elements of the matrix show whether one activity must be completed before another. This matrix assists in: identifying the correct sequence of activities to respect all dependencies; detecting the critical path by determining which activities must start and finish in a specific order to avoid delays or project compromise; and understanding precedence relationships among components. This step ensures a thorough understanding of the product's structure and logic, laying the groundwork for redesign, optimization, or interoperability.

In the case of hardware components, reverse engineering begins with the layer-by-layer disassembly of the device. Techniques such as decapsulation, industrial tomography imaging, or scanning electron microscopy are used to examine each level of the integrated circuit. This process enables the detailed reconstruction of netlists (files that describe the components of an electronic circuit and the connections between them, essentially a textual representation showing which components—such as resistors, transistors, and capacitors—are used and how they are interconnected through nodes, also called nets) and the circuit topology (the logical structure of connections between elements of a circuit, independent of physical placement, indicating which component is connected to which and through which nodes), which is useful for functional analysis or the detection of potential vulnerabilities [24].

For software, methods such as disassembly (converting binary code into assembly language, i.e., a very low-level programming language used to write programs that interact directly with a computer's hardware), decompilation (reconstructing the logical structure into a high-level programming language), and static binary analysis (examining an executable file without running it, to understand what the code does and how it is structured) or dynamic analysis (examining the behavior of a program while it runs to observe its actual operation) are employed. These processes enable engineers to understand the operation of the application even when the original source code is not available [23].

Functional Mapping is the systematic process of analyzing a product to identify, describe, and represent all of its constituent functions. This constitutes a

fundamental step in reverse engineering, as it enables the reconstruction of the original design intent based on empirical observations and performance testing of the examined object. The objective is to determine how each component contributes to the fulfillment of the product's overall functionalities. The process begins with segmenting the product into modules or subsystems, followed by the assignment of specific functions to each segment in relation to the product's overall purpose. This approach allows for thorough documentation of each part, facilitating analysis and potential redesign [11].

In the case of hardware components, functional mapping involves a careful decomposition of the system into its physical assemblies: motherboards, integrated circuits, processors, sensors, or power supplies. Each of these elements is analyzed to determine its specific role within the system, such as which signal it receives, what transformation it applies, and which signal it outputs. This analysis is typically conducted in parallel with the examination of the PCB (Printed Circuit Board) layout, meaning a detailed inspection of how electronic components are arranged and interconnected on the circuit board [3].

Model Validation represents the third step in reverse engineering. After completing the reverse engineering process and obtaining a functional model (mechanical, hardware, or software), the next step is the validation of the model, i.e., verifying its fidelity and functionality in comparison to the original product. This is typically performed through simulated testing, which may include numerical simulations, finite element modeling (dividing a complex object or system into smaller, simpler finite elements connected via nodes; the physical problem is solved locally within each microelement, and the solutions are then combined to obtain the overall behavior of the system), performance analyses (evaluating the behavior of an object or system under real-world conditions without physically constructing the product from scratch), or virtual prototypes (digital representations of a product or system created in design software, such as CAD). The purpose of validation is to determine whether the recreated model reproduces the same physical, logical, or functional behavior as the original device under similar usage conditions. Validation methods include: dynamic simulations (to verify time-dependent behavior, such as resistance to stress or mechanical wear); output data comparison (assessing whether the reproduced model generates identical responses to identical stimuli, e.g., flow rate, pressure, force); CAD-to-reality comparative analyses (using 3D scanning and geometric correlation with the reconstructed CAD model); rapid digital modeling and physical testing (in cases where virtual simulation is insufficient, 3D printing or producing a physical prototype may be employed) [29].

Final Documentation and Development of a New or Modified System represents the last step in reverse engineering. After validating the functional model, rigorous and detailed documentation is required to create a replicable model, conduct technical audits, or provide legal justification in the event of intellectual property disputes. This combined process (comprehensive documentation, physical reconstruction, and reproduction) ensures not only technical accuracy but also legal robustness of the reconstructed product, striking a balance between innovation and respect for intellectual property rights. This stage should include: description of the testing objectives (e.g., desired flow rate, operational cycles, environmental conditions); model configuration (CAD data, parameters, boundary conditions, defined materials); simulation results and comparison with empirical data; identified errors and any adjustments made; comparative graphs and diagrams (flow rates, pressures, efficiency); recommendations for model replication and proposals for optimization [28].

An example of reverse engineering involves a traditional furniture workshop in Bosnia and Herzegovina that received old furniture pieces without any technical documentation. Clients requested the exact reproduction of damaged or outdated pieces. To enable the relaunch of production for these models without CAD files, reverse engineering was necessary, involving 3D scanning, CAD modeling, and digital manufacturing. The process consisted of:

- 3D scanning: original prototypes were scanned using a portable laser scanner, capturing a precise point cloud, including complex shapes (approximately 1 hour per object);
- processing and CAD modeling: raw PCD (Point Cloud Data) was converted into an STL mesh. A mesh is a network of triangles or polygons that collectively form the 3D surface of an object. Essentially, it is represented by points called vertices connected to form triangles (or other simple shapes). The ensemble of these triangles provides an approximation of the object's surface. STL (STereoLithography) is a file format that contains only the geometric shape of the object, without color, textures, or other attributes, used to store 3D models based on these meshes. The data were then imported into a CAD environment, where the shape was reconstructed parametrically. Missing details and geometric tolerance corrections were added;
- dimensional analysis: the CAD model was compared with the ideal model through metrological analysis, and geometric deviations within tolerances (<0.5 mm) were evaluated using specialized software;
- prototyping and production: the model was 3D printed and used as a mold for casting or CNC (Computer Numerical Control) machining - an automated manufacturing process in which a computer controls tool movement to cut, mill, drill, or shape parts from metal, plastic, or wood with high precision. For decorative furniture pieces, 3D printing enabled rapid reproduction of complex parts;
- project outcomes:

a) restored pieces identical to the originals, ready for production;

b) CAD models for adapting and expanding the product line;

c) standardized reverse engineering procedure for the workshop: scan → model → analysis → product [15].

In the context of generic drug development, pharmaceutical companies aim to recreate the formulations of original products (RLD – Reference Listed Drug) when they become generic. Through reverse engineering, RLD tablets are analyzed to determine their qualitative and quantitative composition, solid-state structure, and manufacturing technology, with the objective of producing a clinically equivalent, effective, and safe generic formulation [5].

3 LEGAL IMPLICATIONS

In modern industry, trade secrets (including know-how, formulas, and manufacturing processes) constitute a competitive advantage. When a product undergoes reverse engineering, there is a risk that protected information may be disclosed without authorization, threatening the company's economic value. Directive (EU) 2016/943 and similar U.S. regulations (Uniform Trade Secrets Act) provide the legal framework for protecting such information against unlawful or abusive acquisition [26].

An example of the impact of reverse engineering on intellectual property is Decision 110 Tai-Shang-3193 of the Supreme Court of Taiwan, July 2021: a former employee of a Taiwanese company producing double-sided UV forming machines took CAD files and PDF documents used within the company to reproduce similar machinery through his own business. The plaintiff company argued that these constituted protected trade secrets. The defendant contended that, for an engineer with access to the machine, only the physical measurements of the equipment mattered, and that the CAD files contained information easily reproducible through disassembly; therefore, they were not secret. The first-instance court ruled that the reverse engineering defense was not established, as even by dismantling the original machine to take measurements, complete information about the CAD file could not be easily obtained. The second-instance court held that the reverse engineering defense was valid, reasoning that values nearly identical to the real component dimensions could be obtained simply by disassembling the physical machine into parts and taking measurements using three-dimensional measurement technologies. The Supreme Court overturned the second-instance decision, stating that it had overlooked the legal premises of reverse engineering, the significant cost involved, and the difficulty of actual implementation, which do not negate the confidential nature of the files. Conclusions: reverse engineering does not exempt CAD files or precise documentation from confidentiality protection; if reverse engineering requires significant investment (costs, expertise, errors), the information is still considered a secret; dissemination through unauthorized means (e.g., acquiring the files) can constitute impermissible use, even under the guise of reverse engineering [25].

International legislation does not prohibit reverse engineering per se, but it requires that information obtained through such practices be assessed within the context of fair commercial practices. Individuals and legal entities thus have the ability to prevent the disclosure, acquisition, or use of information lawfully under their control by third parties, without their consent, in a manner contrary to honest commercial practices, provided that the information:

- is secret in the sense that it is not generally known or readily accessible, either as a whole or in the precise configuration and assembly of its components, to persons who normally deal with the type of information in question;
- has commercial value because it is secret;
- has been subject to reasonable measures, under the given circumstances, by the person lawfully controlling the information to maintain its secrecy. A contrary manner to honest commercial practices includes, at a minimum, practices such as breach of contract, breach of trust, and inducement to breach, and encompasses the acquisition of undisclosed information from third parties who knew or were grossly negligent in not knowing that such practices were involved in the acquisition [33].

Moreover, any act of competition contrary to honest industrial or commercial practices constitutes an act of unfair competition, specifically prohibiting the following:

- any acts likely to create confusion by any means with the business, products, or industrial or commercial activities of a competitor;
- false statements made in the course of trade that may discredit the business, products, or industrial or commercial activities of a competitor;
- indications or statements whose use in the course of trade is likely to mislead the public regarding the nature, manufacturing process, characteristics, fitness for purpose, or quantity of the products [22].

For the protection of trade secrets, preventive measures may be taken, such as: companies must implement strict policies of controlled internal access, with confidentiality agreements and the separation of reverse engineering teams from research teams; technical documentation must be clearly marked, with access restricted; anti–reverse engineering contractual clauses must be drafted with temporal and geographical limits, so as to be legally valid and compliant with antitrust legislation [9].

Reverse engineering proves to be a metaphor of the current technological era, a two-sided process in which creativity and vulnerability intertwine in a complex choreography of industrial progress. Looking beyond the purely technical dimension, reverse engineering is the expression of a world in which the boundaries between imitation and innovation are becoming increasingly porous, while legal frameworks, no matter how sophisticated, sometimes lag behind the dynamic realities of the digital economy and applied engineering. Against this backdrop, tension arises between the freedom of technological analysis—essential for interoperability, competition, and improvement, on the one hand, and the need for effective legal protection of innovation, which should not be open to exploitation through mechanical reconstruction, on the

other. This tension is not merely theoretical; it manifests itself in industrial litigation, in strategies for securing know-how, and in the ways governments adapt their intellectual property policies in the face of increasingly sophisticated risks of counterfeiting and piracy.

A simple prohibition or authorization of reverse engineering is not sufficient. What is required is a contextual, differentiated approach that takes into account the specificities of each field. It is evident that reverse engineering should not be regarded solely as a threat, but rather as an indicator of the existence—or absence—of an adaptable legal infrastructure capable of correctly regulating the balance between openness and protection. The Japanese model, for example, has developed a form of indirect protection of know-how, relying not only on the trade secrets regime but also on corporate ethics norms and technological certification standards [30].

On the other hand, in Nigeria, the legislative framework faces the opposite challenge: the absence of a clear delineation of the legitimacy of reverse engineering simultaneously creates opportunities for local entrepreneurs and risks of counterfeiting proliferation, particularly in the field of medical devices [17].

4. CONCLUSIONS

Reverse engineering can be a legitimate tool for innovation, but it becomes problematic when used to obtain trade secrets without authorization. From a legal standpoint, this necessitates the clarification and harmonization of the intellectual property rights framework so that legitimate practices are protected while abuses are sanctioned. From an ethical perspective, it is essential to ensure that reverse engineering does not undermine fair competition or the respect for the creative work of innovators. Intellectual property rights provide protection, but only if trade secret holders implement rigorous procedures of control, documentation, and contractual limitations. Modern legislation should aim to establish a balance by permitting reverse engineering under fair conditions, while ensuring strict control over information distribution and incorporating well-balanced contractual safeguards.

REFERENCES

[1] A. Al-Hakimi, A. B. Md Sultan, A. Ghani, N. Mohd Ali, N. I. Admodisastro (2020). Hybrid Obfuscation Technique to Protect Source Code from Prohibited Software Reverse Engineering, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9211395.

[2] H. Amini (2017). Process of Technology Transfer and Reverse, International Journal of Engineering Trends and Technology, vol. 45, nr. 2, pp. 76-79.

[3] N. Asadizanjani, S. Shahbazmohamadi, M. Tehranipoor, D. Forte (2015). Non-destructive PCB Reverse Engineering Using X-ray Micro Computed Tomography, in International Symposium on Test and Failure Analysis, Oregon.

[4] E. J. Chikofsky, J. H. Cross (1990). Reverse engineering and design recovery: a taxonomy, IEEE Software, vol. 7, nr. 1, pp. 13-17.

[5] D. Choudhary, P. Suryanarayana, T. Gupta, D. Kalyane (2024). Elucidation of processing parameters for the reverse engineering of tablets, RSC Pharmaceutics, vol. 1, nr. 2, pp. 333-343.

[6] S. Ducasse, D. Pollet (2009). Software Architecture Reconstruction: A Process-Oriented Taxonomy, IEEE Transactions on Software Engineering, vol. 35, nr. 4, pp. 573-591.

[7] M. Fyrbiak, S. Strauß, C. Kison, S. Wallat, M. Elson, N. Rummel, C. Paar (2019). Hardware Reverse Engineering: Overview and Open Challenges, https://arxiv.org/abs/1910.01518.

[8] B. Hass (2021). Hardware Reverse Engineering Student Workbook, CyberTruck Challenge.

[9] M. R. Halligan (2024). Trade secret misappropriation claim turns on proof of improper means, Reuters.

[10] S. K. Jha (2025). Legality of Reverse Engineering: Impact on Trade Secrets Intellectual Property, International Research Journal, vol. 12, nr. 1, pp. 561-565.

[11] S. B. Jørgensen, M. Lind, N. Jensen (2019). Functional Modeling View on Product and Process Engineering in Design and Operations, Industrial and Engineering Chemistry Research, vol. 58, nr. 26, pp. 11129-11148.

[12] S. Klix et al. (2023). Stealing Maggie's Secrets - On the Challenges of IP Theft Through FPGA Reverse Engineering, https://arxiv.org/abs/2312.06195.

[13] O. Komolafe, I. T. Adejugbe, T. I. Olorunsola, J. A. Olowonubi, O. Oluwole, J. O. Aigbovbiosa, O. A. Oyegunwa (2024). Reverse Engineering: Techniques, Applications, Challenges, Opportunities, International Research Journal of Modernization in Engineering Technology and Science, vol. 6, nr. 8, pp. 399-410.

[14] J. Liang, R. Pang, C. Li, T. Wang (2023). Model Extraction Attacks Revisited, https://arxiv.org/abs/2312.05386.

[15] A. Muminovic, L. Gierz, H. Rebihić, J. Smajic (2024). Enhancing Furniture Manufacturing with 3D Scanning, Applied Sciences, vol. 14, nr. 4112, pp. 1-18.

[16] G. Naumovich, N. D. Memon (2003). Cover feature - Preventing piracy, reverse engineering, and tampering, Computer, vol. 36, nr. 7, pp. 64-71.

[17] M. I. Obianuju Nwogu (2014). The Challenges of the Nigerian Copyright Commission (NCC) in the Fight Against Copyright Piracy in Nigeria, Global Journal of Politics and Law Research, vol. 2, nr. 5, pp. 22-34.

[18] D. K. Pal, B. Ravi, L. Barghava, U. Chandrasekhar (2006). Computer-Aided Reverse Engineering for Rapid Replacement Parts: A Case Study, Defence Science Journal, vol. 56, nr. 2, pp. 1-14.

[19] C. Pilato, F. Regazzoni (2018). TAO: Techniques for Algorithm-Level Obfuscation, https://re.public.polimi.it/bitstream/11311/1066138/2/obfuscation.pdf.

[20] P. Samuelson (2002). Reverse Engineering Under Siege, Communications of the ACM, vol. 45, nr. 10, pp. 15-20.
[21] P. Samuelson, S. Scotchmer (2002). The Law and Economics of Reverse Engineering, The Yale Law Journal, vol. 111, nr. 7, pp. 1575-1663.
[22] M. Senftleben (2024). Article 10bis of the Paris Convention as the common denominator for protection against unfair competition in national and regional contexts, Journal of Intellectual Property Law & Practice, vol. 19, nr. 2, pp. 81-89.
[23] M. Stamp, T. Cipresso (2010). An introduction to software reverse engineering, in Handbook of Information and Communication Security, New York, Springer, pp. 654-690.
[24] I. Stănășel, F. Blaga, T. Buidoș, D. Crăciun (2018). Reverse Engineering and CAD-CAM Approach for Manufacturing of Spare Parts. Case Study, in MATEC Web of Conferences, France.
[25] J. Tsai, Y. Chiang, L. Hsu (2022). Analysis of Trade Secrets Cases in Taiwan: Whether the "Reverse Engineering" Defense Affects the Determination of Secrecy, Lexology.
[26] C. T. Ungureanu, Ș. R. Tătaru (2023). The legality of reverse engineering or how to legally decipher trade secrets, in International Conference Legal Perspectives on the Internet. COPEJI 6.0. The Right to the Confluence of Two Universes: Where to?, SHS Web Conf.
[27] D. Votipka, S. M. Rabin, K. Micinski, J. S. Foster, M. L. Mazurek (2019). An Observational Investigation of Reverse Engineers' Processes, https://arxiv.org/abs/1912.00317.
[28] N. Walkinshaw, J. Derrick, Q. Guo (2009). Iterative Refinement of Reverse-Engineered Models by Model-Based Testing, in Formal Methods. FM 2009. Lecture Notes in Computer Science, Berlin, Springer, pp. 305-320.
[29] C. Yin, A. Mckay (2018). Model verification & validation strategies and methods: an application case study, in The 8th International Symposium on Computational Intelligence and Industrial Applications, Tengzhou.
[30] *** Ministry of Economy, Trade and Industry Japan (2022). White Paper on Intellectual Property Strategy, https://www.meti.go.jp/policy/intellectual_assets/intellectual_property_wp2022.pdf
[31] *** European Parliament and the Council of the European Union, Directive 2009/24/EC on the Legal Protection of Computer Programs, Article 6, https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32009L0024.
[32] *** European Parliament and the Council of the European Union, Directive (EU) 2016/943 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure, Recital 16, https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016L0943.
[33] *** WIPO (2017). WIPO Database, https://www.wipo.int/wipolex/en/treaties/details/231.

Authors addresses

[1]Bianca Cristina (Pop) Borgyos, drd., Tehnical University of Cluj Napoca, European University of Technology, European Union, Memorandumului street no. 28, Cluj-Napoca, Romania, e-mail bibocris@yahoo.com

[2]Ungureanu Miorița, dr. habil., Department of Engineering and Technology Management, Faculty of Engineering, Technical University of Cluj Napoca, North University Center of Baia Mare, European University of Technology, European Union 62A V. Babes St., RO-430083, Baia Mare Romania, miorita.ungureanu@imtech.utcluj.ro

[3]Raul Florentin Drența, dr., Department of Engineering and Technology Management, Faculty of Engineering, Technical University of Cluj Napoca, North University Center of Baia Mare, European University of Technology, European Union 62A V. Babes St., RO-430083, Baia Mare Romania, raul.drenta@imtech.utcluj.ro

Contact person

** Bianca Cristina (Pop) Borgyos, drd., Tehnical University of Cluj Napoca, European University of Technology, European Union, Memorandumului street no. 28, Cluj-Napoca, Romania, e-mail bibocris@yahoo.com*