The legality of reverse engineering or how to legally decipher trade secrets

Carmen Tamara Ungureanu[1*], *Ștefan Răzvan* Tataru[1**]

[1] Faculty of Law, Alexandru Ioan Cuza University of Iasi, Romania

Abstract. Reverse engineering is the process of extracting secret information (trade secrets) by analysing an existing product. To determine whether reverse engineering falls within the limits of legality, the paper explores first the trade secrets (their meaning and forms, their regulation and legal protection). Then, the reverse engineering is brought under scrutiny, pointing out its main issues that of what reverse engineering consists of, what are the conditions that should be met in order to be considered legal, where it could be applied. The paper highlights the usefulness of reverse engineering in the traditional industry, software industry and as well as in the digital twins technology. In this endeavour, beyond the consulted legal literature, European and American caselaw is examined. Finally, the means of protection that trade secrets right holders have at their disposal against reverse engineering are revealed.

1 Introduction

Innovation and technological progress are subject to unrestricted access to the latest discoveries, scientific studies and processes or products. The absence of such information would make the work of a researcher difficult and lengthy. Gaining access to the latest technologies, so called 'state of the art' (meaning the level of development a particular field has reached at a particular point in time) [1], allows those who develop products or processes to innovate on an up-to-date scientific basis and save time and resources allocated to experiments or prototypes already tested and whose results have been made public and applied [2]. The same idea was expressed by the English scientist Isaac Newton who said 'If I have seen further, it is by standing on the shoulders of giants', confirming that the work and the scientific results obtained would not have been possible without the previous contribution made by the enlightened minds of the scientific community.

Those who fund the research and development of new products and technologies, do so with the purpose of recovering the investment and maximising the profit. The success of this objective lies in obtaining a monopoly on the market and protecting the innovation

* Corresponding author: carmen.ungureanu@uaic.ro
** Corresponding author: razvantataru@gmail.com

through the means considered appropriate to the given scientific field. Protection can be secured either by registering intellectual property rights (patent, brand, design or model) or by keeping confidential the information regarding the product's manufacture or the development of the technological process (trade secrets/know-how) [3]. Confidentiality is a safety precaution that blocks the access of unauthorized users to certain information, being at the same time a prohibition and an exception to the normal use of information. Protecting the interests of the parties implies the defence of commercial secrecy and implicitly the acceptance of confidentiality. According to the provisions of the International Standard on Information Security - ISO/IEC 27000:2018, confidentiality is 'the property according to which information is not made available or disclosed to unauthorized persons, entities or processes'.

The business environment at the national and international level has evolved into an extremely competitive one, and the development of products and technologies has become a continuous concern for all enterprises. Thus, as a Business Week headline from 1992 stated, '*Competitive advantage no longer belongs to the biggest or those blessed with abundant natural resources or the most capital. In the global economy, knowledge is king'.* Acquiring 'knowledge' is not easy for everyone, as it involves resources of all kinds (human, financial, and so on) [4]. The concept of Knowledge includes three elements: know-how, know-why and know-what. Knowledge represents an understanding of phenomena. In the context of technological systems, knowledge is an understanding of the principles that underlie their operation, the processes used to create them, and the uses that these technological systems serve. Once achieved, the information holders seek to protect it by preventing any interested party from obtaining it through illegal, non-competitive, or unethical means. In this context, we endeavour to shed light on what trade secrets are and how they can be legally acquired through reverse engineering activities.

2 Trade secrets

Reverse engineering is necessary and justified only in the situation where the information and technical principles incorporated in a product are not generally known or easily accessible, being kept secret by their holder and protected against disclosure. Hence, the concept of trade secrets and their legal protection are to be explored hereinafter.

2.1 Trade Secrets: Concept and Regulation

The term 'trade secret' [5] originates from the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). According to art. 39 of TRIPS, member states have the obligation to protect 'undisclosed information', in accordance with art. 10 bis of the 1883 Paris Convention for the Protection of Industrial Property. The TRIPS provisions do not use the notion of know-how or trade secrets, but of undisclosed information which are related to unfair competition.

The Romanian legislator takes over the provisions established in the TRIPS Agreement [art. 39 para. (2)] and defines the term of trade secret within the framework of art. 11 lit. d) from Law no. 11/1991 as 'the information that cumulatively meets the following requirements: 1. are secret in the sense that they are not, as a whole or as presented or articulated their elements, generally known or easily accessible to people in those circles that are usually dealing with the type of information in question; 2. have commercial value given by their secret nature; 3. have been the subject of reasonable measures, under the given circumstances, taken by the person who legally has control over the respective information, in order to keep it secret'.

More recently, the concept of commercial secrecy has been taken up within the provisions of Government Emergency Ordinance no. 25/2019 (hereinafter, G.E.O. 25/2019), which transposes into national legislation the Directive (EU) 2016/943 on the protection of know-how and undisclosed business information (trade secrets) against illegal acquisition, use and disclosure (hereinafter, Directive 2016/943). Although the directive defines the concept of trade secret in art. 2 point 1, these provisions are not taken over in G.E.O. 25/2019, which references to the definition included in Law no. 11/1991.

In the United States of America (USA), The Uniform Trade Secrets Act (UTSA) was adopted in 1979, with amendments from 1985, which is applied in almost all-American states [6]. The provisions of the UTSA are supplemented by guidance from the Unfair Competition Restatement of 1995, which defines a trade secret as 'any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others' [7].

2.2 Protection of trade secrets

The legal literature emphasises that protection of trade secrets means, in certain circumstances, protection against such conduct that is contrary to honest commercial practice [8]. Article 39 para. (2) of TRIPS, without defining the notion of undisclosed information, specifies the conditions that such information should satisfy as to be considered undisclosed and therefore protected. Thus, the natural and legal persons have the possibility of preventing information lawfully under their control from being disclosed to third parties, or acquired or used by others without their consent and in a manner contrary to honest commercial practices, under certain conditions that must be met cumulatively, so long as such information: '(a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) has commercial value because it is secret; and (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.' [9, 10]. Moreover, art. 39 para. (2) of TRIPS emphasizes that there is no absolute property right over undisclosed information. Unauthorized disclosure or use of information must be prevented only if such acts are contrary to honest commercial practices [11]. TRIPS defines "conduct contrary to honest commercial practices", stating that this includes at least practices such as breach of contract, breach of trust, and causing others to violate contractual provisions to which they are bound.

The Directive 2016/943 envisaged the adoption of uniform rules in the member states of the European Union (EU) to ensure the protection of know-how and undisclosed business information, as trade secrets, by establishing appropriate mechanisms of access to justice for the purpose of applying sanctions in the event of the illegal acquisition, use or disclosure of information constituting trade secrets. The Directive 2016/943 provides for a minimum harmonization, which results from art. 1 paragraph (1): 'Member States may, in compliance with the provisions of the TFEU, provide for more far-reaching protection against the unlawful acquisition, use or disclosure of trade secrets than that required by this Directive [...]'.

The Directive 2016/943 was a necessary piece of legislation in the context of a vast diversity of regulations on an EU member states level, since trade secrets did not benefit from protection in all states and where this protection existed, the norms were included in civil law, criminal law, labour law or in unfair competition legislation and intellectual property law [6].

According to the first point in the recitals of the Directive 2016/943, '[...] valuable know-how and business information, that is undisclosed and intended to remain

confidential, is referred to as a trade secret'. Next, point (2) of the recitals emphasizes that 'Businesses, irrespective of their size, value trade secrets as much as patents and other forms of intellectual property right. They use confidentiality as a business competitiveness and research innovation management tool, and in relation to a diverse range of information that extends beyond technological knowledge to commercial data such as information on customers and suppliers, business plans, and market research and strategies. [...] By protecting such a wide range of know-how and business information, whether as a complement or as an alternative to intellectual property rights, trade secrets allow creators and innovators to derive profit from their creation or innovation and, therefore, are particularly important for business competitiveness as well as for research and development, and innovation-related performance'.

The concept of trade secrets is also analysed at the point (14) of the recitals of the Directive 2016/943, where it is mentioned that: 'It is important to establish a homogenous definition of a trade secret without restricting the subject matter to be protected against misappropriation. Such definition should therefore be constructed so as to cover know-how, business information and technological information where there is both a legitimate interest in keeping them confidential and a legitimate expectation that such confidentiality will be preserved. Furthermore, such know-how or information should have a commercial value, whether actual or potential. Such know-how or information should be considered to have a commercial value, for example, where its unlawful acquisition, use or disclosure is likely to harm the interests of the person lawfully controlling it, in that it undermines that person's scientific and technical potential, business or financial interests, strategic positions or ability to compete. The definition of trade secret excludes trivial information and the experience and skills gained by employees in the normal course of their employment, and also excludes information, which is generally known among, or is readily accessible to, persons within the circles that normally deal with the kind of information in question'.

From the recitals of the Directive, we come to the point that a secret includes both the know-how and the undisclosed business information.

To be protected as trade secrets, according to art. 2 point 1 of the Directive, the information must cumulatively meet the following requirements:

a. 'To be secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question'. There are no international standards to clarify the meaning of being *generally known* or *readily accessible* to people within the normal business circles [6]. Some authors [12] have proposed that the moment when the last competitor finds out the secret, should be considered the point the secret information is generally known. Nevertheless, in this approach, knowing the secret does not seem advantageous to the information holder, who is almost everyone. Therefore, another method should be used namely that of the case-by-case analysis, bearing in mind that confidentiality agreements are concluded to maintain secrecy [6]. What it is meant by „readily accessible" is also not clear or explained. The term 'readily ascertainable', used in UTSA, similar to 'readily accessible', designates the situation in which 'information is readily ascertainable if it is available in trade journals, reference books, or published materials. Often, the nature of a product lends itself to being readily copied as soon as it is available on the market'. A more controversial hypothesis considers that the disclosure of the secret occurs by simply placing the product on the market [13, 6] – 'if the public is able to discover through reverse engineering the secret information embedded in a product once it is introduced on the market, the secret information embedded in it is no longer a secret and can no longer be protected'[14].

b. To have commercial value by being kept secret. The trade secrets have a commercial value arising from the confidential character of the information embedded within a product

or service, which represents a competitive advantage and has the ability to generate an economic benefit to the holder.

c. To have been the subject of reasonable measures, under the given circumstances, taken by the person lawfully in control of that information, to keep it secret. The holder of the trade secret should act in the way of protecting its own patrimony by implementing appropriate technical and organizational measures to preserve the confidential/secret character of the information.

2.3 A classification of trade secrets

If it is to be considered the types of information included in the broad concept of trade secrets, they could be divided into know-how and undisclosed business information (confidential information).

2.3.1 Know-how

The know-how is a form of intellectual property and represents a set of unpatented (patentable or non-patentable) and transferable technical knowledge that is used to manufacture a product or develop a process [15] [16] [17].

An essential characteristic of know-how is that its protection is achieved privately, i.e., through contracts concluded between business partners, unlike other forms of intellectual property such as patents, copyrights or trademarks, which are protected by rules developed in national and international legislation [18].

Another essential characteristic of know-how is that it does not have limited validity in time. It exists legally as long as the secrecy is kept. This is one of the reasons why companies prefer the use of know-how to the detriment of patents, which have time expiration. One of the best-kept commercial secrets (know-how) is the chemical formula of Coca-Cola, which has remained undisclosed for over 100 years. The Coca-Cola company preferred trade secrets over the patent, thus avoiding the entry of the formula into the public domain, which would have happened after the patent expired [18].

According to art. 1 lit. (if) of the Commission Regulation (EU) No 316/2014 of 21 March 2014 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of technology transfer agreements, the know-how is: 'a package of practical information, resulting from experience and testing, which is: (i) secret, that is to say, not generally known or easily accessible; (ii) substantial, that is to say, significant and useful for the production of the contract products, and (iii) identified, that is to say, described in a sufficiently comprehensive manner so as to make it possible to verify that it fulfils the criteria of secrecy and substantiality;''.

2.3.2 Undisclosed business information

Undisclosed business information or confidential information represents one of the most used and most valuable forms of intellectual property given the absence of any registration procedures or costs and the possibility to benefit from the protection and to 'exploit' the information indefinitely, under the condition of keeping the secret [3]. According to the doctrine, trade secrets are considered a category of goods which benefit from property protection rules, in accordance with art. 1 protocol 1 of the European Convention on Human Rights. [28] [66]

In the absence of a legal definition in the national legislation, we consider that 'confidential information' designates the non-public information, regarding an organization/an enterprise/a company, its activities or the operations in which it is involved,

and which have commercial value and are subject to protection measures against unauthorized access or public disclosure.

A definition of the concept of confidential information can be found in the content of the Confidentiality Contract Model developed by the International Chamber of Commerce in Paris, which represents 'any information [...] communicated by or on behalf of the Disclosing Party to the Receiving Party, including, but not limited to, any kind of business, commercial or technical information [...], except for information that is demonstrably non-confidential in nature' [19].

The scope of undisclosed business information is determined by each individual organization/enterprise/company, which establishes the precise categories of information considered confidential and the appropriate protection measures to keep them secret. Companies may consider confidential a wide range of information, including manufacturing technology processes, early-stage inventions, marketing or sales plans and strategies, market prospecting methods, distribution methods, supplier and/or customers databases, investment plans, research and development projects [3] [20].

Due to the similarities of the two concepts, know-how and undisclosed business information, their delimitation by the holder becomes, in practice, unfeasible. For this reason, it appears appropriate to use the notion of trade secrets, delimiting in this way the information used in business activities from other categories of information that must be kept confidential, such as classified or personal information.

The ways of legally acquiring a trade secret are provided in the art. 3 of the G.E.O. 25/2019. While in the art. 3 para. (1) a) the usual ways of creating trade secrets are laid down, more precisely through independent discovery / research-development, under para. (1) b) the methods of acquiring the secrets already incorporated within an existing product or object are presented. In this last scenario, the problem of so-called reverse-engineering arises.

3 Reverse engineering and trade secrets

In order to analyse the concept of reverse engineering, a few clarifications are necessary. First, the meaning of the engineering activity should be outlined, as to then could define the reverse engineering and show the conditions of keeping reverse engineering within the limits of legality. Afterwards, the application of reverse engineering in various industries are to be pointed out and, finally, the ways of protection against reverse engineering are to be revealed.

3.1 Reverse engineering: concept and regulation

To analyse the concept of reverse engineering, we should first define what the engineering activity is. Engineering means 'the creative application of scientific principles to design or develop structures, machines, devices or manufacturing processes or works' [21]. Thus, engineering involves a process that starts from the principles and ends with the final product. Reverse engineering goes in the opposite direction, being a process that starts with the known product and works backwards to find out the technical principle behind its construction. By reference to traditional manufacturing products and processes, this analysis can be performed by taking apart a machine and analysing its components. Modern methods include chemical analysis of components or electronic scanning of the shape of the product or its parts. Since the advent of computer technology, decompiling or disassembling software programs have become the most widely used methods of reverse engineering [10] [22].

In the specialized literature, there are also opinions that support the existence of an additional concept that of 'forward engineering' or 'advanced engineering', as a conventional process of moving from advanced ideas to their material implementation. This usually includes the preparation of engineering drawings from which models and then moulds are formed for the final stage of mass production [22]. In software development, forward engineering involves the development of a new product based on precisely established requirements that call for the use of advanced knowledge [23].

If initially reverse engineering processes demanded considerable effort on the part of a reverse engineer, nowadays they are facilitated by computer-aided design (CAD) to create three-dimensional virtual models of existing parts and subassemblies. A 3D scanner can create, as well, a CAD design by scanning an existing object [24]. Subsequently, 3D models can be processed with the help of computer-aided engineering (CAE) software programs and manufactured with the assistance of computer-aided manufacturing (CAM) software programs and 3D printers [25].

What does reverse engineering mean? Reverse engineering is the process the secret information is extracted by examining and analysing an existing product. In other words, the reverse engineer studies a product to discover and learn its design, construction, and mode of operation, which are not accessible to the public [8].

As to the regulation of reverse engineering, art. 39 of TRIPS regarding trade secrets, does not clarify the legal situation of reverse engineering. The TRIPS provision does not even explicitly refer to reverse engineering activities. However, it does not make the protection of undisclosed information subject to the impossibility of discovering it by following a reverse analysis, nor does it determine whether reverse engineering is always or only in some situations 'contrary to honest commercial practices' [10].

EU member state legislations take a different approach; for example, in German law reverse engineering is considered an unfair commercial practice [8] [6].

In the EU, it is not clear from the wording of the Directive 2016/943 whether reverse engineering is allowed or not, in what way and within what limits.

According to recital (16) of the Directive, 'in the interest of innovation and to foster competition, the provisions of this Directive should not create any exclusive right to know-how or information protected as trade secrets. Thus, the independent discovery of the same know-how or information should remain possible. Reverse engineering of a lawfully acquired product should be considered as a lawful means of acquiring information, except when otherwise contractually agreed. The freedom to enter into such contractual arrangements can, however, be limited by law'. It could be inferred that reverse engineering is legal under certain conditions. Considering the provisions of art. 4 para. (2) of the Directive, it seems that a case-by-case analysis should be applied as to assess whether the reverse engineering activity represents an anti-competitive behaviour and whether the trade secret was obtained unlawfully.

In the recital (17) of the Directive it is mentioned, as well, that 'In some industry sectors, where creators and innovators cannot benefit from exclusive rights and where innovation has traditionally relied upon trade secrets, products can nowadays be easily reverse-engineered once in the market. In such cases, those creators and innovators can be victims of practices such as parasitic copying or slavish imitations that free-ride on their reputation and innovation efforts'.

As a matter of fact, a reverse engineer could act as an *innovative analyst* or as *an imitative* one. In the first scenario, the reverse engineer tries to expand his own technological knowledge aiming at creating new, innovative products or at improving the existing ones. As *imitative analyst,* on the contrary, the engineer uses the reverse process to *copy* a product. In order to distinguish innovative reverse engineering activities based on legitimate acquisition of trade secrets and creation of a similar competing product from

imitative reverse engineering built on non-competitive practices such as servile copying and the creation of a low-cost identical product, a case-by-case method should be used. In USA, for instance, in *Bonito Boats v. Thunder Craft Boats*, the American Supreme Court held that '[I]mitation and refinement through imitation are both necessary to invention itself, and the very lifeblood of a competitive economy' [10].

According to art. 4 para. (3) of the European Directive, 'The use or disclosure of a trade secret shall be considered unlawful whenever carried out, without the consent of the trade secret holder, by a person who is found to meet any of the following conditions: (a) having acquired the trade secret unlawfully; (b) being in breach of a confidentiality agreement or any other duty not to disclose the trade secret; (c) being in breach of a contractual or any other duty to limit the use of the trade secret.'. The next paragraph specifies that 'The acquisition, use or disclosure of a trade secret shall also be considered unlawful whenever a person, at the time of the acquisition, use or disclosure, knew or ought, under the circumstances, to have known that the trade secret had been obtained directly or indirectly from another person who was using or disclosing the trade secret unlawfully within the meaning of paragraph 3.'.

In USA, the notion of reverse engineering was defined by the US Supreme Court in *Kewanee Oil v. Bicron Corporation* [26] as a form of information discovery, starting with a known product and analysing/working backwards to its origins to reveal the process that helped create, develop and manufacture it. If we are to admit the legality of reverse engineering, setting limits to trade secret protection, this is an essential step towards innovation [6].

Reverse engineering mainly concerns trade secrets, but it can also affect other intellectual property rights, such as those protected by patents or copyrights. Patents give inventors protection for twenty years and exclusive rights to make, use, and market the patented product, but only in exchange for public disclosure of significant technical details about their inventions. It seems that as long as the inventor is asked to disclose sufficient information about the invention and about how it is made, reverse engineering is not necessary and does not affect patent law. However, an infringement becomes possible when a 3D scanner is used for scanning an object, which is then printed with a 3D printer. The result is a copy of the original product protected by a patent [24].

In terms of copyright, which protects the expressed ideas but not the ideas themselves, reverse engineering is possible in the case of computer programs, as it was made clear in a case decided by the Court of Justice of the European Union (CJEU) [27]. In *SAS Institute v. World Programming Ltd* (C-406/10) on an infringement of copyright on computer programs and manuals relating to IT database system brought by SAS Institute the court stated that: '[…] neither the functionality of a computer program nor the programming language and the format of data files used in a computer program in order to exploit certain of its functions constitute a form of expression of that program […]. To accept that a functionality of a computer program can be protected as such (copyright) would amount to making it possible to monopolise ideas, to the detriment of technological progress and industrial development'.

In order to avoid reverse engineering, parties may enter agreements or include clauses that prohibit reverse engineering into computer programs [6].

Reverse engineering is not expressly mentioned in art. 10 TRIPS either relating to computer programs. In the USA reverse engineering is legal, both according to the caselaw of the Supreme Court of Justice [6] and to the Uniform Trade Secrets Act (UTSA). The US Supreme Court stated in Kewanee Oil v. Bicron Corp. that 'a trade secret law, however, does not offer protection against discovery by fair and honest means, such as by independent invention, accidental disclosure, or by so-called reverse engineering'.

At the international level, the World Intellectual Property Organization WIPO clarifies the controversy surrounding the activity of reverse engineering, considering it as a legal activity, in accordance with honest practices; information protected as trade secrets can be obtained lawfully by reverse engineering [27, 28] [30] [31].

3.2 Reverse engineering legality conditions. Applicability of reverse engineering in industry

In the common law, the first condition that should be fulfilled for the reverse engineering to be legal is the *ownership* of the product that is "disassembled". Ownership must have been lawfully acquired. In the case of *Mars UK Ltd v. Teknowledge Ltd*, a British court stated in 2000 that "what the owner has is the full right of ownership. With that goes an entitlement 'to dismantle the machine to find out how it works and tell anyone he pleases" [6].

In the EU the condition demanded is not the ownership, but the legal *possession* of the product. Alternatively, the object/product, subject to a reverse engineering, should have been made available to the public. The Directive 2016/943 establishes in art. 3 paragraph (1) (b) these conditions stating that the observation, study, disassembly or testing should be carried out on a product or an object that has been made available to the public or on a product/ object that is lawfully in the possession of the person who acquired the information and to whom no legally valid contractual obligation to limit the acquisition of the trade secret applies. This leads to the idea of licensing agreements, such as software licenses.

As we mentioned previously, the reverse engineering process can be applied to any product or process, presenting different particularities depending on the field of activity / industrial sector to which the object subject to reverse engineering belongs. In the specialized literature, reference is often made to three main areas: the manufacturing industry (traditional), the semiconductor industry (production of microchips) and the software industry. From our point of view, the manufacturing industry includes the semiconductor one, the technical peculiarities that the latter encompasses not justifying the creation of a distinct category. However, a new field is gaining momentum, which includes elements from the traditional industry, the data economy and the software industry: the use of reverse engineering for the creation of digital twins (which will be shortly analysed). Another particular domain is evolving, as well: 3D bioprinting technology, nanotechnology and tissue engineering technology. It combines cutting-edge machinery, electronic circuitry, software, materials, and processes (which will not be addressed in this paper) [32].

3.2.1 Reverse engineering in manufacturing industry

Traditional products and manufacturing processes can be reverse engineered starting from simple, common products such as boats or children's toys to complex military, pharmaceutical or automotive products.

The motivation of reverse engineering processes can vary. James Pooley, university professor and international expert in the field of trade secrets, identifies six reasons behind reverse engineering: acquiring new information for a better understanding and use of a product; modification or reparation of a product; provision of an associated service; development of a compatible product; clone creation; improvement of the product [2]. In the industrial production sector, the economic goal of reverse engineering is the development of a similar competitive product or an improved object. Reverse engineering undertaken for the purpose of repairing a purchased product may well affect the manufacturer's aftermarket (eg. for parts or service), but this will generally have less

economic effect on the manufacturer than it would have a new reverse engineered competing product [2]. However, the process of developing similar competing products is time-consuming, difficult and expensive, so that an innovator should not fear the reverse engineering; he/she has actually a significant period of time to enjoy market exclusivity, sufficient for the recovery of product research and development expenses [2].

If reverse engineering is carried out for the purpose of developing a new, improved product, banning it would hinder innovation. The economic effects can be at least partially positive, including the situations when reverse engineering serves only to providing information for servile copying, because such copying tends to break up monopolies and reduce market prices.

3.2.2 Reverse engineering in the software industry

In the software industry, reverse engineering is a common practice used to understand how each module of the software program works and how it interacts with other systems [33]. Unlike industrial manufacturing products and processes, software programs are information-rich and incorporate a lot of know-how, which explains the efforts to restrict reverse engineering in this area.

The most common tools for reverse engineering computer programs are disassemblers, debuggers, and decompilers [34]. Decompilation is a form of reverse engineering that involves translating object code into a human-readable form, largely through trial and error. Part of the decompilation process can be computer assisted; there are, for example, disassemblers that will translate object code into an intermediate form of assembly language that is more decipherable for skilled readers, namely source code [35] [36].

Some authors consider that a 'software engineer that has to reverse engineer a computer program for education and interoperability purposes, will always be protected by the ECJ and has not to worry any legal action by the software owner', even if the software engineer does not have any permission from the owner. Moreover, a reverse engineer will not infringe any rights if he/she wishes to re-engineer the software, taking into account only the 'principles' or 'ideas' of the original [33].

In a different opinion [37, 2] decompilation and disassembly should be illegal from the point of view of copyright and trade secret law. A reverse engineering cannot be completed without unauthorized copies of the program, and this violation makes decompilation and disassembly to be an improper means of obtaining trade secrets. In the US, courts have allowed software to be copied during decompilation or disassembly if necessary to achieve fair purposes, such as interoperability between software programs or between a program and a hardware platform.

The European rule is similar in that it is purpose-based, with decompilation permitted when and if it is done to achieve interoperability [10]. In the software industry, the provisions of Directive no. 2009/24/CE on the legal protection of computer programs apply. According to art. 1 paragraph (2) and (3) the protection is provided to any form of expression of a computer program. The ideas and principles underlying an element of any computer program, including those underlying its interfaces, are not protected by copyright. A computer program is protected if it is original, in the sense that it is an intellectual creation of the author.

As art. 6 of Directive no. 2009/24/CE reads reverse engineering in the form of decompilation is allowed for the reproduction of the object code, if the aim is to ensure interoperability. Thus, the reproduction of the object code and its decompilation is permitted without the authorization of the holder when it is indispensable for obtaining the information necessary to achieve the interoperability of a software program created independently of other programs [36] and subject to the following conditions: '(a) those

acts are performed by the licensee or by another person having a right to use a copy of a program, or on their behalf by a person authorised to do so; (b) the information necessary to achieve interoperability has not previously been readily available to the persons referred to in point (a); and (c) those acts are confined to the parts of the original program which are necessary in order to achieve interoperability'. According to art. 6 para. 2 lit. c), the information thus obtained cannot be used for 'development, production or marketing of a computer program substantially similar in its expression, or for any other act which infringes copyright'.

Art. 5 para. (3) provides for another form of allowed reverse engineering: '(3) The person having a right to use a copy of a computer program shall be entitled, without the authorisation of the rightsholder, to observe, study or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program if he does so while performing any of the acts of loading, displaying, running, transmitting or storing the program which he is entitled to do'.

Decompiling, making a copy and analysing, studying or testing the operation of the program in order to identify ideas and principles cannot be restricted by contractual clauses. Such agreements would be null and void (art. 8, para. 2) [36]. Recently, the CJEU ruled in the case *Top System SA v. Belgian State* (C-13/20) that a 'lawful purchaser of a computer program who wishes to decompile that program in order to correct errors affecting the operation thereof is not required to satisfy the requirements laid down in art. 6 of Directive 2009/24/EC. However, that purchaser is entitled to carry out such a decompilation only to the extent necessary to affect that correction and in compliance, where appropriate, with the conditions laid down in the contract with the holder of the copyright in that program' [38].

The reverse engineering is legal according to the Directive 2016/943, unless the one who acquired the information is subject to any legally valid contractual obligation that prohibits reverse engineering. Recital 16 of the directive stated that 'Reverse engineering of a lawfully acquired product should be considered as a lawful means of acquiring information, except when otherwise contractually agreed. The freedom to enter into such contractual arrangements can, however, be limited by law', leaving it to the discretion of the EU member states to limit the party autonomy. The Romanian legislator did not deal with this issue in G.E.O. 25/2019 transposing the directive.

In the US, restricting the right to reverse engineering by contract is controversial. In the 1988 case of *Vault Corporation v. Quaid Software Limited*, prohibition of reverse engineering was declared unenforceable [6]. In 2005, in another case, it was considered valid and effective (the case of Davidson & Associates v. Jung [39]) - where the court considered that: 'In Vault, plaintiffs challenged the Louisiana Software License Enforcement Act, which permitted a software producer to impose contractual terms upon software purchasers provided that the terms were set forth in a license agreement comporting with the statute. [...] Unlike in Vault, the state law at issue here neither conflicts with the interoperability exception under 17 U.S.C. § 1201(f) nor restricts rights given under federal law. Appellants contractually accepted restrictions on their ability to reverse engineer by their agreement to the terms of the TOU and EULA. [...] By signing the TOUs and EULAs, Appellants expressly relinquished their rights to reverse engineer [6]'. Subsequently, the case law of the American courts' records equally different and controversial rulings.

Restricting the right to conclude contracts, which imposes an obligation not to reverse engineer, would aim to promote innovation and ensure progress with effects also on a healthy commercial competition. Allowing contractual 'not to do' obligations can lead to unfair competition, giving the trade secret holder the possibility to impose market conditions, including price-related criteria (which would affect consumers, as well), ensuring its dominant position on the market, and the impossibility of innovation.

An example could be the case *Microsoft v. European Commission* (T-201/04) [40], decided in 2007, whereby Microsoft was required to provide access to the information, documents and 'source code' of relevant Microsoft products under violation of art. 102 TFEU for dominant market position (as it refused to provide the interoperability information and authorize its use).

The most relevant US software reverse engineering case is *Sega Enterprises Ltd. v. Accolade Inc*. [41]. In this case, Accolade, an American computer game company, disassembled Sega's software programs in order to obtain the information necessary to make its games compatible with the Sega Genesis platform. Accolade was subsequently able to market independently developed games in direct competition with those produced by Sega and by licensed third-party developers. Sega sued Accolade claiming copyright infringement by copying and disassembling the object code. The Ninth Circuit court did not consider the commercial purpose of Accolade's copying, as it was done 'solely to discover the functional requirements for compatibility with the Genesis platform — aspects of Sega's programs that are not protected by copyright'. Reverse engineering was, in fact, the only way Accolade was able to gain access to this information. Even if Accolade had copied the object code of the software programs developed by Sega in the process of reverse engineering, the court did not consider this aspect relevant, as it constituted an intermediate stage in the development of Accolade's software. Although the court found that the Accolade games adversely affected the Sega game market, it found that the copyright on the Genesis console was not affected. The court did not legitimize all reverse engineering activities on the object code of the software developed by Sega, but only those that have been undertaken for the purpose of ensuring interoperability and only if they 'provide the only means of access to those elements of the code that are not are protected by copyright' [2] [42].

The US Court of Appeals for the Ninth Circuit reaffirmed this reasoning in *Sony Computer Entertainment Inc. v. Connectix Corp*. [43], in which Connectix disassembled Sony's object code in order to ensure the interoperability of other hardware devices with games developed exclusively for the Sony Playstation platform. In this case, Connectix developed emulation software (Virtual Game Station) that allowed games developed exclusively for the Sony Playstation platform to run on other devices. The Court of Appeal ruled in favour of Connectix, holding that there is no relevant difference between decompiling for interoperability purposes for the development of competing platforms and developing a virtual platform for game interoperability.

The analysis of the reverse engineering purpose in the *Sega v. Accolade* and *Sony v. Connectix* cases demonstrates that reverse engineering in the software industry has other motivations than those in the manufacturing industry, namely, ensuring the interoperability of one software program with another or with a hardware system. Reverse engineering for software programs is far too difficult and resource consuming to be cost-effective and to be used for the purpose of developing a similar competing product [2].

3.2.3 Reverse engineering, digital twins and Metaverse

Technology has opened up immeasurable possibilities for reverse engineering. By using real-world models, with the contribution of the data industry, the AI (Artificial Intelligence) and the software industry, digital twins can be created.

What is a digital twin? Although it would seem that the digital "twin" is the virtual replica of a physical object, in fact, digital twin means more than that. While the digital replica, which a reverse engineer could make with a 3D scanner, does not receive data from the original [44], the digital twin or the virtual 'twin' of an object, process or even a service, allows data analysis and its monitoring through simulation in virtual space [45]. In

other words, the digital twin is the mirror image of its real-world counterpart [46], which it is interdependent with; the real-world object/process/service can be adapted, improved according to the feedback generated by its digital twin, which is 'fed' real-time 'sensory data' from the real world, recreating the environment and conditions of the actual object/process/service [46].

Digital Twin Technology is often confused with CAD (Computer-Aided Design). What distinguishes it from this is that CAD technology only provides the digital image/representation of the real-world object, while digital twin technology aims to create an interdependence between the virtual and the real representation [47].

What a digital twin could be used for? There are various domains where digital twins would be useful: in ensuring the good functioning of a driverless vehicle (autonomous car) [47], in the agri-food sector (in the food processing industry) [44], in medicine, in the manufacturing industry, in the distribution chain, etc. [48]. Finally, digital twins are present in the Metaverse[3].

Digital replicas have already been run, for instance in the virtual reality Second Life (a platform that has been offering Metaverse-specific experiences since its inception in 2003 until now), where General Motors, Nissan and other vehicle manufacturers have opened dealerships since 2005 [49]. Ferrari is present in the game Fortnite since 2021 [50]. Car manufacturers create digital twins for models to be launched in the real-world market, and afterwards, the 'twins' 'learn' from each other, contributing to the improvement of their performances, as is done for example by the Renault group [51], Hyundai [52] and others, and not least Tesla Motors [53]. However, these professionals do not need reverse engineering to create digital twins, as they have at their disposal all the data/information that is the basis of their products, from the real world or the virtual world, protected by intellectual property mechanisms.

Could a digital twin be created by reverse engineering? Advances in technology make the answer affirmative. Reverse engineering is a booming activity supported and powered by technology. Trade secrets, whatever form they take, can be deciphered.

There are platforms that offer reverse engineering services, one example being CadCrowd [54], registered in Canada, which offers freelance services provided by licensed and qualified engineers. On the opening page of the platform, the legality of the services offered is mentioned: 'Items, products, or programs that are purchased by an entity from a competitor can be reverse engineered legally as long as any patented or protected material is not used in a new product. This is often done to figure out just how a new product or program operates so that the information discovered can be used as the basis for improvement' [54]. In the adhesion contract imposed by the platform (Terms of Service) [55] at point 4(a) it is stipulated that 'Any Designs submitted, input, or uploaded by a Service Buyer will be owned by the Service Buyer or its licensors. Cad Crowd claims no rights in such Designs;'. Therefore, the condition of ownership of the object to be 'disassembled', or the condition of possession of the object under a license agreement is necessary to be fulfilled for the legality of the reverse engineering services. In addition, the new reverse-engineered "product" must not contain patented or otherwise protected information.

The possibility of obtaining a digital twin through reverse engineering emerges equally from the tools available on the market. For example, the Artec 3D platform (Artec Europe

[3] The notion of Metaverse was first used by the American writer Neal Stephenson in his book *Snow Crash*, published in 1992, where the Metaverse is a 3D virtual reality. Currently, Metaverse illustrates the same concept, of a virtual reality, built on the infrastructure of the Internet, in which blockchain technologies, virtual currencies and NFTs (non-fungible tokens) are used. In this regard, see [66].

SRL) [56], specialized in the sale of 3D technology (scanners and scanning software), offers the necessary equipment for this. Andrei Vakulenko (Chief Business Development Officer at Artec 3D), said that '[…] 3D scanning lets you conduct precise inspections of the real-world versions of these digital twins in mere minutes, thus ensuring intelligent analyses of manufacturing variances and product performance' [57].

Digital twins of collectable cars or of unique models are created. For example, The Bridgade [58], a design studio based in New York, creates digital twins of rare cars (using reverse engineering equipment), which can be accessed using tokens on platforms such as Opensea [59]. A Mercedes model is to be offered for sale on the Opensea platform, with a link to a 3D configurator [60].

As virtual realities develop, to offer users experiences comparable to those in the real world or even more spectacular, digital twins will occupy an important place. Reverse engineering will provide the 'supply' of 'twins' where real-world model owners are unwilling or unable to participate in the Metaverse marketplace.

3.3 Protection against reverse engineering

To reduce the risk of losing trade secrets, their holders could employ different methods of protection against reverse engineering activities, among which: licensing agreements; confidentiality agreements; increasing brand awareness (of the innovative product) and implementing other measures to attract and keep customers; using trade secret protection systems that make reverse engineering difficult.

Licensing agreements are an easy way to reduce the threat of reverse engineering. The holder of the trade secrets can grant licenses, thereby controlling the entry of new competitors into the market. By granting a license, the licensor is able to recover its research and development expenses through licensing revenues and prevent the licensee from selling the product at prices that would have a destructive effect on the market [61]. Licensing agreements create the premise of obtaining the same secret information and economic advantages as in the case of reverse engineering, but without the allocation of financial, human and time resources to carry out the entire reverse engineering process [2]. Also, as long as reverse engineering is permitted by law, trade secret holders will be willing to offer licenses on favourable terms to drive the opportunity cost against reverse engineering. In economics, *opportunity cost* means „the cost of a benefit that must be forgone to pursue an alternative" or, in other words, potential gains missed by choosing one option over another [62].

Confidentiality agreements could be chosen, as well, as means of protecting trade secrets, in every stage of the business relations. Even reverse engineers may be required to enter into confidentiality agreements with the enterprise/natural or legal person to whom they provide reverse engineering services. For example, the freelancing platform CadCrowd imposes confidentiality rules on engineers through the adhesion contract available on the platform (Terms of Service). In Appendix 1 to the Terms of Service it is stated that: 'Restrictions. The Service Provider understands that the Information is owned by the Service Buyer or its licensors, and is confidential to the Service Buyer or its licensors, and shall not be used or disclosed, except in accordance with the terms of this Appendix. To ensure protection of the Information, Service Provider will: 1. maintain the Information in strict confidence; 2. not copy or use the Information or any part thereof in any way, except as required for the purposes set out in Section 4; 3. not disclose the Information or any part thereof directly or indirectly to any other party without in each instance having first obtained the prior express written consent of the Service Buyer; 4. not alter, modify, disassemble, reverse engineer, or decompile the Information or any part

thereof in any way except as required for the purposes set out in Section 4; 5. protect the Information against unauthorized disclosure' [55].

An indirect path to contrabalance reverse engineering could be the increasing of brand awareness by carrying out marketing campaigns. In this way, the innovative product would keep its market share and would be easily distinguishable from any other similar product introduced later on the market. For instance, the promotion of the Coca-Cola brand, a product that also incorporates trade secrets (the manufacturing recipe), determined notoriety at the international level, even if several competing similar products entered the market.

Last but not least, the trade secret holder can implement protection measures against reverse engineering starting from the design and manufacturing stage of the product. Thus, the trade secret holder may use sealing systems or construction materials that break down in the disassembly process and make reverse engineering difficult, if not impossible. The manufacturer or developer can use different techniques in this context, such as: encapsulation of hardware components to make non-destructive disassembly almost impossible; mislabelling or marking components to mislead a potential reverse engineer; adding some 'locks' on the product components or within the software program [2].

In addition to the measures taken by the manufacturers themselves a few state legislators have enacted regulations that punish the illegal use of trade secrets and the anti-competitive practices of using information obtained through reverse engineering to make slavish imitations. In the US, since the 1970s, several states have adopted regulations prohibiting the creation of moulds as a way of reverse engineering some products already on the market [63]. Through these rules, US states forbade the use of a mould to manufacture identical products in direct competition with the moulded product [2].

In Romania, in the same vein, the Law no. 344/2005 regarding some measures to ensure compliance with intellectual property rights in customs clearance operations states in art. 3 paragraph (2) the fact that moulds are assimilated to goods that infringe an intellectual property right, provided that their use infringes the right holder. According to art. 4 para. (5) from Directive 2016/943, 'the production, offering or placing on the market of infringing goods, or the importation, export or storage of infringing goods for those purposes, shall also be considered an unlawful use of a trade secret where the person carrying out such activities knew, or ought, under the circumstances, to have known that the trade secret was used unlawfully within the meaning of paragraph 3'. By 'infringing goods' should be understood, according to art. 2 point 4 of Directive 2016/943, goods, the design, characteristics, functioning, production process or marketing of which significantly benefits from trade secrets unlawfully acquired, used or disclosed.

At EU level, trade secret holders are entitled to apply to the competent court for the enforcement of measures, procedures and remedies provided by law to prevent, restrain, or obtain redress for, the unlawful acquisition, use or disclosure of their trade secrets.

Unlike patents, where the information becomes part of the prior *state of the art*, trade secrets are not made public and therefore do not provide 'defensive' protection to the holder. In the absence of this type of protection, for example, if a manufacturing process of a product has been protected as a trade secret, any person can obtain a patent for the same technological process as long as he independently developed / discovered the information [29].

The World Intellectual Property Organization (WIPO) states that 'a trade secret owner, however, cannot stop others from using the same technical or commercial information, if they acquired or developed such information independently by themselves through their own R&D, reverse engineering or marketing analysis, etc' [29].

Recently, norms belonging to an international organization have been adopted with reference to reverse engineering. Thus, the FIA (Fédération Internationale de l'Automobile), revised the technical regulations for Formula 1 from 2021, prohibiting the

use of reverse engineering regarding the design of rival competitors [64]. In the new regulation, reverse engineering is not permitted: 'No competitor may design its Listed Team Components (LTC) based on reverse engineering of another competitor's LTC. For the purpose of this Article, 'reverse engineering' shall mean: 1. The use of photographs or images, combined with software that converts them to point clouds, curves, surfaces, or allows CAD geometry to be overlaid onto or extracted from the photograph or image. 2. The use of stereophotogrammetry, 3D cameras or any 3D stereoscopic techniques. 3. Any form of contact or non-contact surface scanning. 4. Any technique that projects points or curves on a surface so as to facilitate the reverse-engineering process. Listed Team Components are defined by the regulations as components whose design, manufacture and intellectual property is owned and/or controlled by a single Competitor or its agents on an exclusive basis. On occasions where there is deemed to be significant similarities between listed components on different team cars, the FIA has the right to investigate the matter asking a team to prove that their design was independently created' [65].

However, the FIA does not completely prohibit reverse engineering, but only that which looks at the design of rival competitors. Creating digital replicas of rival cars with improved performance, even digital twins, does not seem to be off limits.

According to the opinion of some authors [31], 'Information and knowledge diffusion (and free competition) are the rule and intellectual property protection is the exception'. Because of this rule, all intellectual property protection regulations are limited in various ways. Trade secret regulation is no exception. In fact, since the protection is not conditional on a disclosure or *quid pro quo*, the holder's rights are more limited.

4 Conclusions

Protecting the valuable information to a business by designating it as a trade secret is a necessity on the today's ultra-competitive global market. Businesses need a protected, confidential environment with a view to developing new products and generating business strategies. By means of trade secrets, the developer of a product has the ability to insulate all information from disclosure, irrespective of the product stage (from the research and development phases until the application for a patent protection, if wanted so); or the developer could keep protecting the information as trade secrets, if the threat of reverse engineering is mild.

An effective protection of an innovative product can only be achieved in a strategic way, by combining available and complementary intellectual property protection methods, through technical and organizational data security measures within and out of the organization. According with this line of reasoning the product and its manufacturing process could be protected both by an invention patent and by means of trade secrets, the latter as to the information that is not required to be disclosed in the patent application, but which is relevant to the success of the product and the effectiveness of the manufacturing process. These protection methods can be supplemented, where possible and appropriate, by registering other intellectual protection rights (trademark, design and utility model).

Given the particularities of trade secrets and their value within businesses/companies/organizations, it seems that they can be viewed as genuine intellectual property rights. However, the activity of reverse engineering as a means of legally acquiring trade secrets should be included in the field of competition law, its main impact being felt in the competition on the market, whether the market is traditional or virtual (located in Metaverse).

To sum up the reverse engineering represents an easy, adaptable and indispensable tool for 'deciphering' trade secrets and at the same time an incentive for innovation, generating

competition on the market and indirectly, competitive prices and the desire to improve the existing products.

References

1. D. Barford, *Intellectual Property and Patent Information*, World Intellectual Property Organization, URL: https://www.wipo.int/export/sites/www/tisc/en/ppt/Philippines/state_of_the_art_search.pdf, accessed 12.10.2022 (2011)
2. P. Samuelson, S. Scotchmer, The Yale Law Journal, **111(7)**, 1662 (2002)
3. Ș.R. Tataru, Analele Științifice UAIC, SSJ, **Tomul I(LXVI)**, 261-277 (2020)
4. R. Garud, Advances in Strategic Management, **14**, 83-85 (1997)
5. R. Dincă, Protecția secretului comercial în dreptul privat (Universul Juridic, București, 2009)
6. G. Surblyte, Enhancing TRIPS: Trade Secrets and Reverse Engineering, 731 in H. Ullrich, R. M. Hilty, M. Lamping, TRIPS plus 20 From Trade Rules to Market Principles (Springer, 2016)
7. American Law Institute, *Restatement of the Law 3rd, Unfair Competition*, URL: https://wipolex-res.wipo.int/edocs/lexdocs/laws/en/us/us216en.pdf, accessed 12.10.2022 (1995)
8. D. Arcidiacono, European Papers, **1(3)**, 1076, DOI:10.15166/2499-8249/83 (2016)
9. C.T. Ungureanu, Dreptul comerțului internațional. Contracte de comerț international (Hamangiu, București, 2014).
10. Ohly, Reverse Engineering: Unfair Competition or Catalyst for Innovation? in W. A. Pyrmont, Patents and Technological Progress in a Globalized World, MPI Studies on Intellectual Property, Competition and Tax Law Vol. 6, DOI:10.1007/978-3-540-88743-0_37 (Heidelberg: Springer, Berlin, 2009)
11. O.-M. Florescu, Economie teoretică și aplicată, **6(501)**, 67 (2006)
12. N. P. de Carvalho, The TRIPS Regime of Antitrust and Undisclosed Information (Kluwer Law International, Haga, 2008)
13. S. H. Leong, *World Intellectual Property Organization*. URL: https://www.wipo.int/edocs/mdocs/sme/en/wipo_smes_uln_13/wipo_smes_uln_13_o_leong.pdf, accessed 12.10.2022 (2013)
14. S.H.S. Leong, presentation titled 'In Confidence' - Putting in Place a Trade Secret Protection Program from the Training of the Trainers Program on Effective Intellectual Property Asset Management by Small and Medium Sized Enterprises (SMEs), organized by the World Intellectual Property Organization (WIPO), Mongolia, Ulaanbaatar, October 8-10, 2013
15. I. Macovei, Tratat de drept al comerțului internațional (Hamangiu, București, 2014)
16. C.T. Ungureanu, Dreptul comerțului internațional (Hamangiu, București, 2018)
17. J. Reichman, Vanderbilt Law Review, **42(3)**, 656 (1989)
18. W. F. Fox, International Commercial Agreements and Electronic Commerce (5th ed.) (Kluwer Law International 2013)
19. International Chamber of Commerce, ICC Model Confidentiality Agreement, ICC Services Publications Department, Paris, URL: https://epdf.pub/icc-model-confidentiality-agreement.html, accessed 12.10.2022 (2006)

20. Kumar, P. Mohanty, R. Nandakumar, Journal of Intellectual Property Rights (JIPR), **11(6)**, 397-408, DOI: 0971-7544 (2006)
21. United States Engineers Council for Professional Development, Britannica.com, URL: https://www.britannica.com/technology/engineering, accessed 12.10.2022 (2022)
22. S. Guernsey, *Competition, Non-Patented Innovation, and Firm Value*, DOI: 10.2139/ssrn.3074622 (2019)
23. *Difference between Forward Engineering and Reverse Engineering*, URL: https://www.geeksforgeeks.org/difference-between-forward-engineering-and-reverse-engineering/, accessed 12.10.2022
24. M. Weinberg, *When 3D Printing and the Law Get Together, Will Crazy Things Happen?* 15 in Van den Berg, B, Van der Hof, S., Kosta, E. (Editors), 3D Printing Legal, Philosophical and Economic Dimensions, DOI: 10.1007/978-94-6265-096-1 (Springer, ebook, 2016)
25. Michigan State University, *What is the Difference between CAD, CAE and CAM?*, Michigan State University, URL: https://online.egr.msu.edu/articles/cad-vs-cae-vs-cam-what-is-the-difference/, accessed 12.10.2022 (2021)
26. USA Supreme Court, 416 U.S. 470, *Kewanee Oil Company v. Bicron Corporation et al.* (1974)
27. Court of Justice of the European Union, C-406/10, *SAS Institute v. World Programming Ltd*
28. G. Faludi, *Balancing The Relevant Legitimate Interests In The Legal Protection Of Trade Secrets In Hungarian Law*, WIPO Symposium on Trade Secrets and Innovation, Geneva, Switzerland, URL: https://www.wipo.int/edocs/mdocs/mdocs/en/wipo_ip_inn_ge_22/wipo_ip_inn_ge_22_p4.pdf, accessed 12.10.2022 (2022)
29. World Intellectual Property Organization - Trade Secrets section, World Intellectual Property Organization, URL: https://www.wipo.int/tradesecrets/en/tradesecrets_faqs.html, accessed 12.10.2022
30. J. Watal, *Balancing Legitimate Interest in the Trade Secret System under the WTO TRIPS Agreement*, WIPO Symposium on Trade Secrets and Innovation, Geneva, Switzerland, URL: https://www.wipo.int/edocs/mdocs/mdocs/en/wipo_ip_inn_ge_22/wipo_ip_inn_ge_22_p3.pdf, accessed 12.10.2022 (2022)
31. K.S. Sandeen, *Balancing Legitimate Interests in the Trade Secret System*. WIPO Symposium on Trade Secrets and Innovation, Geneva, Switzerland, URL: https://www.wipo.int/edocs/mdocs/mdocs/en/wipo_ip_inn_ge_22/wipo_ip_inn_ge_22_p5.pdf, accessed 12.10.2022 (2022)
32. E.D. Ferrill, K. Rajan, *3D Bioprinting, Nanotechnology, and Intellectual Property*, 505-523 in L.G. Zhang, J.P. Fisher, K.W. Leong, (Editors), 3D Bioprinting and Nanotechnology in Tissue Engineering and Regenerative Medicine, Second edition (Elsevier, 2022)
33. P. Ciancarini, D. Russo, A. Sillitti, G. Succi, *Reverse Engineering: a European IPR perspective*, SAC'16: Proceedings of the 31st Annual ACM Symposium on Applied Computing. DOI: 10.1145/2851613.2851790 (2016)
34. URL:https://hack.technoherder.com/reverse-engineering/, accessed 12.10.2022
35. D. Varadarajan, Iowa Law Review, **103**, 1596 (2018)
36. U.-M. Mylly, ICC, **52**, 1323, DOI: 10.1007/s40319-021-01120-3 (2021)

37. R. Grogan, *Decompilation and Disassembly: Undoing Software Protection*, Computer Law (1984)
38. Court of Justice of the European Union, C-13/20, *Top System SA v. Belgian State* (2021)
39. Davidson & Associates, doing business as Blizzard Entertainment Inc; [...] v. Tim Jung, URL: https://h2o.law.harvard.edu/collages/45578, accessed 12.10.2022
40. Court of First Instance (Grand Chamber), T-201/04, *Microsoft Corp. v. Commission of the European Communities* (2007)
41. United States Court of Appeals, *Sega Enterprises Ltd. v. Accolade Inc.* (Ninth Circuit 1992, URL: https://h2o.law.harvard.edu/cases/4486, accessed 12.10.2022
42. K. Love, Technology & Intellectual Property Law, **4(1)** (1993)
43. U.S. Ninth Circuit Court of Appeals, Sony *Computer Entertainment Inc. v. Connectix Corporation*, 203 F.3d 596 (2000)
44. Koulourisa, N. Misailidis, D. Petrides, Food and Bioproducts Processing, **(126)**, 317-333 (2021)
45. M. Alba, *Finally Digital Twins get their own consortium*, URL: https://www.gafcon.com/engineering-com-digital-twins-get-their-own-consortium/, accessed 12.10.2022 (2020)
46. G. Bhatti, H. Mohan, R.R. Singh, Renewable and Sustainable Energy Reviews, **141** (2021)
47. F. Tao, F. Sui, A. Liu, Q. Qi, M. Zhang, *Digital twin-driven product design framework*, International Journal of Production Research, DOI: 10.1080/00207543.2018.1443229 (2018)
48. P. Augustine, Advances in Computers, **117(1)**, DOI: 10.1016/bs.adcom.2019.10.008 (2020)
49. *Bridging the real and the virtual for the automotive aftermarket*, URL: https://peel-3d.com/blogs/news/bridging-the-real-and-the-virtual, accessed 12.10.2022
50. *Test Drive The Ferrari 296 Gtb In Fortnite*, URL: https://www.epicgames.com/fortnite/en-US/news/test-drive-the-ferrari-296-gtb-in-fortnite, accessed 12.10.2022 (2021)
51. *Vehicle Digital Twin: when physical and digital models unite*, URL: https://www.renaultgroup.com/en/news-on-air/news/vehicle-digital-twin-when-physical-and-digital-models-unite/, accessed 12.10.2022 (2022)
52. *Hyundai Motor to adopt digital twin in latest move of virtual technology use Digital twin technology set to be introduced at HMGICS, allowing the automaker to create a digital replica of a real car for simulation not only in virtual space but also in the physical world*, URL: https://www.kedglobal.com/tech/newsView/ked202107050009, accessed 12.10.2022 (2021)
53. D. Piromalis, A. Kantaros, *Digital Twins in the Automotive Industry: The Road toward Physical-Digital Convergence,* Applied System Innovation, URL: https://www.mdpi.com/2571-5577/5/4/65(2022), accessed 27.08.2022
54. URL: https://www.cadcrowd.com/hire/reverse-engineering, accessed 12.10.2022
55. URL: https://www.cadcrowd.com/page/termsofservice, accessed 12.10.2022
56. Terms of Use, URL: https://www.artec3d.com/terms-use, accessed 12.10.2022

57. T. Kevan, *Introducing the New Reverse Engineering*, URL: https://www.digitalengineering247.com/article/introducing-the-new-reverse-engineering/design, accessed 12.10.2022
58. URL: https://brigade.tv/about/, accessed 12.10.2022
59. URL: https://opensea.io/, accessed 12.10.2022
60. *Bridging the real and the virtual for the automotive aftermarket*, URL: https://peel-3d.com/blogs/news/bridging-the-real-and-the-virtual, accessed 12.10.2022 (2022)
61. J.H. Reichman, *Legal Hybrids Between the Patent and Copyright Paradigms*, Columbia Law Review, 2441, URL: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1075&context=faculty_scholarship, accessed 12.10.2022 (1994)
62. B. Haghpour, E. Sahabeh, H. Halvari, International Journal of Consumer Studies, **46**, 1942–1959 (2022)
63. D.W. Carstens, Harvard Journal of Law & Technology, **3(Spring)**, 174-175 (1990)
64. *Reverse engineering clampdown and super licence revisions approved by FIA*, URL:https://www.formula1.com/en/latest/article.reverse-engineering-clampdown-and-super-licence-revisions-approved-by-fia.4S2ZYwi3X37jsnkJNlOxxW.html, accessed 12.10.2022
65. *Formula 1 Bans 3D Scanning and Reverse Engineering*, URL: https://metrology.news/formulae-1-bans-3d-scanning-and-reverse-engineering/, accessed 12.10.2022 (2020)
66. T.F. Aplin, *Right to Property and Trade Secrets* in C. Geiger, Research Handbook on Human Rights and Intellectual Property, 421-422, Edward Elgar
67. M.D. Murray, *Trademarks, NFTs, and the Law of the Metaverse*, DOI: http://dx.doi.org/10.2139/ssrn.4160233 (2022)