International Interest: Software Assessment for Security-Relevant Errors

A Primary Analysis with Respect to Copyright, Trade Secret and Patent Law

Thomas Hoeren and Stefan Pinelli

Based on the user's interest in the security of acquired software and its verification (I.), this paper examines whether and to what extent a careful analysis of software for security-relevant defects is permissible under copyright law (II.), trade secret law (III.) and patent law (IV.).

I. Initial Position

Frequently, the assessment of industrial software-based products is of considerable significance to its users. Considering the fact that the level of complexity of software is rising steadily, enabling developments that combine a wide variety of software, the processing of real-time data and the (partial or complete) guidance of the user, the granting of product quality in the form of security plays a particularly important role. The current discussions about cyber security, other IT security and data protection incidents demonstrate the relevance of safeguarding early knowledge about the properties and functions of software with regard to IT security. The following analysis deals with the copyright, patent and trade secret implications of software investigations. The evaluation of software investigations from a criminal law point of view is also not the subject of this article, although it should be pointed out that criminal consequences must be taken into account in individual cases.

The aim of software investigations can thus be to determine the extent to which the delivered software fulfils legal requirements, complies with the agreed specifications (properties and functions) of the buyer or customer and follows (non-binding) guidelines of authorities and other institutions. Investigations may cover a wide range of measures:

Monitoring and system monitoring intercepts communication from software to software or from software to hardware for the purpose of testing[1] and examines the program flow when various commands are entered without access to internal software structures (so-called *black box testing*[2]). In the course of assessments, *debuggers*,[3] line tracing tools, memory snapshots and *similar analysis tools are* used and *load and stress tests are* carried out. *Penetration testing*, in which the specialist in charge 'puts the security of IT systems to the test' then exposes any security weaknesses. Investigative measures may also include the *manipulation and extension of source code*, for example in the form of decompiled code and binary code. In addition, individual software components can be examined or the software can be analyzed by *decompilation. In* some cases the technical examination may also require the *circumvention of technical protective measures*.

Restrictions or prohibitions of such inspection measures could result particularly due to the provisions on the protection of computer programs (§§ 69a ff. UrhG). In addition, the Patent Law (PatG) and the Law on the Protection of Trade Secrets (GeschGehG), which implements the EU Directive 2016/943, could contain further restrictions. The specific connection of these protective systems must also be discussed.

II. Protection of Computer Programs According to §§ 69a et seq. UrhG

§§ 69a et seq. UrhG, which implement the EU Directive 2009/24/EC on the protection of computer programs, contain special provisions for computer programs.

1. Scope

§§ 69a ff. UrhG protect programs in any form, including design material, § 69a Abs. 1 UrhG. The underlying ideas and principles of computer programs are generally not covered (cf. Sec. 69a (2) sentence 2 UrhG) and protection always requires them to be the result of an intellectual creation of the author, Sec. 69a (3) UrhG.[4]

Computer programs, presumably including the programs to be assessed in practice, generally fulfil the requirements for protection and are thus subject to §§ 69a ff. UrhG.[5]

2. Measures requiring consent

§ 69c UrhG lists the right holder's exclusive rights. Here, the right to reproduce the computer program (Section 69c No. 1 UrhG) and the right to postprocess (Section 69c No. 2 UrhG) are particularly significant.

(a) Reproduction of the program

Pursuant to § 69c No. 1 UrhG, the right holder has the exclusive right to permanently or temporarily reproduce a computer program or parts of it, regardless of means and form. The term *'reproduction'* covers any action that makes program data visible to humans, whether by copying to another data carrier, printing or storing the source or program code.[6] Even if reproduction is necessary in connection with the execution of the computer program, such as in loading, displaying, running, transferring or storing, the consent of the right holder is required, § 69c No. 1 S. 2 UrhG. Furthermore, if loading a program into the main memory enables additional use by further copies of the program, this is already a duplication.[7]

The process of the assessments described above entails, among other things, the production of duplications of the computer program, although in the case of so-called embedded software solutions, duplication is not always mandatory. Limiting the investigations to comply with the program sequence does not avert this problem, since copies made in connection with the execution also require approval, § 69c No. 1 S. 2 UrhG.

At least in the case of measures such as monitoring, system monitoring, black box tests and load and stress tests, reproductions are usually required. The use of other analysis tools also regularly results in duplicates. Concerning the analysis of a single program part, it seems useful to extract and duplicate this part beforehand.

(b) Program amendment

Pursuant to § 69c No. 2 UrhG, the right holder continues to have the exclusive right to translate, edit, arrange and otherwise modify a computer program and to reproduce the results. Even the act of post-processing requires approval, not the publication of the result.[8] The purpose of this provision is to protect the expertise of the right holder.[9] The term 'modification' is to be understood widely and covers all changes to the program.[10] This requires an intervention in the program material. As an example, § 69c No. 2 UrhG mentions forms of reworking.[11] The term 'translation' refers to the transfer of the program into another programming language.[12]

The translation category includes, for example, the retranslation of object code into source code.[13] The cases of manipulation, change and extension of the source code[14] as well as penetration tests involve an intervention in the program substance and therefore constitute a case of editing.

The cases of monitoring, system monitoring, black box tests as well as load and stress tests, memory dumps and line scanning, on the other hand, involve almost no interference with the program material, and thus do not constitute any form of editing in the sense of § 69c No. 2 UrhG. Depending on the specific method used, the use of debuggers requires an analysis of the individual case.

3. Consent

As laid out above, carrying out the listed audit procedures requires the consent of the respective right holder. In the absence of an expressed consent, an *implied consent* (or granting of rights of use) is sufficient to meet the requirements with regard to the protection of computer programs. It depends on the circumstances of the individual case whether or not an implied granting of rights is given. In particular, it may only apply if it is customary practice in the sector and has previously been contractual practice between the parties. Moreover, the purpose of the contract must be doubtlessly established.[15]

The determination of implied consent requires a careful contemplation of the individual case. Although investigative measures are common in the industry, contracts between software suppliers and software purchasers usually claim to be complete due to their extensive regulations regarding rights of use, ruling out additional implied consents. In case of doubt, the acceptance of an implied granting of rights of use beyond expressly agreed subjects contradicts the intention of the parties. Least of all, this results from the principle of purpose transfer, which also applies to computer programs, §§ 69a para. 4, 31 para. 5 UrhG.[16] It states that in case of doubt, a granting of rights shall not exceed the purpose of the contract.[17]

This standard rule for interpretation remains unchanged by the fact that a large part of the agreements on rights of use is regularly governed by general terms and conditions. It is highly controversial whether the principle of transfer of purpose constitutes a *mere rule of interpretation* or a *content standard* with the additional content that contractual deviations from the legal scope and content of the rights of use are only permissible under special conditions.[18] However, this only affects cases where agreements go beyond the purpose of the contract or general terms and conditions are subject to content check.[19] Since there is a broad consensus about the function of the purpose transfer principle as an interpretation rule, there is usually little room for implied consent in the case of unregulated types of use in a sufficiently differentiated contractual arrangement because, in case of doubt, the rights should remain with the author.[20] Therefore, the consent of a right holder usually has to be given expressly and cannot be inferred in an implied form.

4. Intended use according to § 69d (1) UrhG

Despite the fact that legally permissible inspection measures generally require consent, they would be even lawful without it if a special exception pursuant to §§ 69d, 69e UrhG is applicable.

According to § 69d (1) UrhG, the acts referred to in § 69c No. 1, 2 UrhG do not require consent unless a (valid) contractual provision[21] to that effect has been made and they are necessary for the intended use of the computer program, including the correction of errors, by anyone authorised to use a copy of the program. The purpose of this provision is to achieve an proper balance between the interests of the legitimate user and those of the right holder.[22] Hence, in this case the legislator considers the interest of the right holder in intended use of the program superior to the interests of the right holder.[23]

(a) Legitimacy

§ 69d UrhG privileges any person who has been granted a corresponding right of use by the right holder. This applies to everyone who has concluded an effective license agreement, not just buyers. As a rule,[24] the exemption results from the lawful acquisition or purchase of the software (purchase contract or contract for work and services) or the authorisation to use the software in test operation.

(b) Intended use

The challenge in the copyright protection of software is the constitutive legal element of intended use. The decisive element in the exemption provision is the standard of intended use. According to the prevailing opinion in case law and literature, it is based on the purpose of the transfer and other contractual circumstances.[25] In addition, the conflicting interests of the parties must be weighed against each other and brought to a fair balance.

Active Software Analysis: The contractual agreement transferring the right to use the software will either be a software purchase contract (for standard software only) or a software development contract[26] which is categorised as a contract for work and services.[27] In the case of software provided for a limited period of time, contracts regularly take the form of a rental agreement. The inspection of software usually serves

the purpose of defect inspection. If the inspected software fails to meet the statutory legal requirements or the specific (lawful) specifications of the buyer, it is defective within the meaning of § 633 BGB or § 434 BGB, depending on the type of contract.[28] This gives rise to the question whether active checking for software errors also constitutes intended use within the meaning of § 69d (1) UrhG.
So far, literature has apparently been silent on the matter.

In the opinion of the authors, measures that are necessary for troubleshooting may constitute intended use in individual cases. § 69d (1) UrhG expressly grants the entitled party the right to correct errors. Within the scope of error correction, a significant intervention in the program substance always takes place. The exclusive search for errors, which interferes into the program in a considerably weaker kind than a correction, must therefore be *a fortiori* admissible.[29] In the event of a defect, the software user is entitled to warranty rights according to § 437 BGB or § 634 BGB as buyer or orderer; a right to inspect for defects can therefore be justified on the basis of the underlying contract. In the case of a commercial purchase of software, § 377 HGB (German Commercial Code), whose applicability has been confirmed by the German Federal Court of Justice,[30] even establishes a duty for the commercial buyer to immediately examine the object of purchase. Moreover, within the framework of contracts for work and services, for commercial and private orderers alike, acceptance despite knowledge of a defect leads to a limitation of warranty rights, § 640 (3) BGB. Thus, a certain obligation to inspect for defects also exists in the presence of contracts for work and services. However, it is unreasonable to charge the buyer with the burden of having to wait until a defect is discovered by other means; particularly since he would thereby be exposed to the risk of limitation of his claims. Accordingly, contracts for work or purchase of software already establish the right to active testing for freedom from defects. In principle, this argumentation can be transferred to rental agreements, since from the user's point of view there is also a need to examine the rental object for defects after all.

Which investigative measures are specifically permissible must be determined by means of reconciliation of the opposing interests of the contracting parties. This includes taking into account the possible liability risks or reputational damage for the benefit of the buyer. In cases where the use of the software is specified further, individual considerations should be made according to its use. These can, for example, take the use of software in sensitive semi-automated or fully automated areas as well as its danger to legal assets such as property, life and limbs into consideration. However, the interests of the software purchasers are countered by the interest of the software supplier in the protection of his expertise. Depending on the interests in the individual case, the protection of the supplier or the buyer, purchaser or lessee may predominate.

In light of these considerations, it must be assumed that all testing measures serving to detect security-relevant software errors are intended uses within the meaning of § 69d (1) UrhG. A decompilation, however, can in no case constitute intended use, since the special provision of § 69e UrhG may not be circumvented.[31]

5. Observation, examination and investigation pursuant to § 69d (3) UrhG

Pursuant to § 69d (3) UrhG, the lawful user of a program may, without the consent of the right holder, observe, examine or test the functioning of the program in order to determine the underlying ideas and principles of a program element if this occurs by loading, displaying, running, transferring or storing the program, ie within the framework of normal program execution. This exception is limited to the purpose of identifying the ideas and principles; further reproductions and adaptations are not covered.[32]

The provision does not cover interventions to the content of the program substance.[33] The source code is also not a permissible object of identification or examination.[34]

§ 69d (3) UrhG covers common analysis measures such as monitoring, system monitoring, black box tests,[35] load and stress tests, memory dump[36] and line tracking.[37] The permissibility of the use of debuggers depends on the type of debugger and the interventions it causes in the program substance.[38] Decompilation, on the other hand, is not permitted under Section 69 (3) UrhG.[39]

6. Permissible decompilation according to § 69e UrhG

§ 69e UrhG regulates the special case of decompilation; it establishes its admissibility without consent for the

purpose of creating *interoperability* with other programs. The purpose is regulated comprehensively; further purposes are not covered.[40]

If the primary purpose of the investigation is to ensure compliance with legal standards or contractual specifications, another purpose is pursued. Decompilation in this context is not covered by § 69e UrhG.

7. Circumvention of technical protective measures

The legal admissibility of investigative measures to circumvent technical protective measures is determined by § 69f (1) and (2) UrhG. Pursuant to § 69a (5) UrhG, § 95a UrhG does not apply to computer programs.[41]

Pursuant to § 69f (2) UrhG, the right holder is entitled to destroy all means which are solely intended to facilitate the unauthorised removal or circumvention of technical program protection mechanisms. This essentially leads to the conclusion that, in contrast to § 95a UrhG, the use of means should not be recorded as such.[42]

In some cases, however, the *so-called indirect protection of protective measures is* assumed. According to this, § 69c UrhG is infringed if the use of the means constitutes an act requiring consent.[43] The reproduction and reworking of the program is of particular importance. However, the use of the work may again be justified by §§ 69d, 69e UrhG.[44]

Technical program protection mechanisms are understood to include dongles, copy protection mechanisms, password queries, program blocks, time blocks, etc.[45] § 69f (2) UrhG already covers measures that only facilitate circumvention. However, they must be intended for circumvention purposes only – means which are also intended for lawful use are not covered.[46]

III. Protection of Trade Secrets According to GeschGehG

The implementation of the EU Trade Secrets Directive[47] has changed the previous provisions of §§ 17 et seq. UWG and has led to a much more differentiated system of protection for trade secrets. The corresponding draft of the *Federal Government* for a law for the protection of business secrets (hereinafter referred to as GeschGehG was modified in the Bundestag and entered into force at the end of April.[48]

1. Trade secret

According to § 2 No. 1 GeschGehG, trade secrets are information which is neither generally known nor readily accessible and therefore of economic value, either in its entirety or in the precise arrangement and composition of its components, to persons in the circles which normally deal with this type of information. In addition, the information must be subject to appropriate confidentiality measures by its lawful holder with respect to the circumstances. The burden of proof for these protection measures lies with the holder of the trade secret.[49] The definition itself is the subject of numerous legal disputes which cannot be resolved within the scope of this paper.[50]

However, one can assume that in individual cases the software to be inspected, the source code itself or individual parts may contain or represent trade secrets in this sense. The information must not be easily accessible, which is determined by the persons who usually come in contact with such information (*professionals*). Such facts, which can be ascertained by an average expert, therefore fall outside the scope of the GeschGehG.[51] However, reverse engineering measures do not make information easily accessible, as otherwise § 3 (1) no. 2 GeschGehG would be deprived of its regulatory content.

In the following, due to the current difficulties of a legally secure handling of the definition, it is assumed that trade secrets will be disclosed or at least used in investigations.

2. Scope of protection

Pursuant to § 4 GeschGehG, a trade secret may not be obtained by unauthorised access to appropriation or reproduction of documents, objects, materials, substances or electronic files which are subject to the lawful control of the owner of the trade secret and which contain the trade secret or from which it may be derived, § 4 (1) no. 1 GeschGehG. If the right holder gave his consent, the acquisition is not unauthorised within the meaning of this provision.

Furthermore, a trade secret may not be acquired by any other conduct which, under the respective circumstances, does not comply with the principle

of good faith, taking into account honest market practices, § 4 (1) no. 2 GeschGehG. This fact is ill-defined and can hardly be discussed without recourse to rhetorical practice.[52] In any case, such acts which are already permissible under §§ 69a et seq. UrhG (see II.4.-7. above) shall not be regarded as acts of infringement. Moreover, it is not yet possible to make a legally certain subsumption of the customary nature of the intended investigative measures on the market.

3. 3rd barrier for reverse engineering

According to § 3 (1) no. 2 GeschGehG the acquisition of trade secrets by observing, investigating, dismantling or testing a product or object is permitted. The product or object must either be publicly available (lit. a) or be in the lawful possession of the person taking the corresponding measures (lit. b):

- *Publicly available (lit. a):* The former applies if the software is freely available on the market, so that permission according to lit. a is given and measures according to No. 2 are generally permissible.
- *Legitimate possession (lit. b):* This applies if the supplier produces the software specifically for the purchaser and does not offer it on the free market. In this case of lawful possession, the freedom of inspection may however be limited by contract, § 3 (1) no. 2 lit. b GeschGehG.

In practice, suppliers individualise standard products and tailor them to the needs of the customer. In this case, although the classification among the alternative elements of No. 2 is indistinct, the result is irrelevant, since in each case the action fulfills the provision and is hence permissible.

This means that possible investigative actions are partially admissible with regard to the protection of secrets. Within the scope of monitoring, system monitoring, line monitoring and memory swapping, the program is only executed in an observing way. Artificial commands are entered for black box tests as well as load and stress tests, so these are to be assigned to testing in the above sense. The same applies to the use of debuggers. The decompilation of software can be classified as deconstruction.

While under previous regulation it was forbidden to use a trade secret obtained through reverse engineering,[53] the same is permitted under today's laws presuming that the trade secret was lawfully obtained. The prohibition to use trade secrets in § 4 Abs. 2 GeschGehG only applies to cases in which the secret was obtained illegally (according to Abs. 1, see 2. above) or where a non-disclosure agreement was breached. According to that the manipulation and extension of source code that either constitutes or contains a trade secret is only permitted if the source code has been lawfully obtained.

IV. Protection of Software under Patent Law

Software in general is not qualified as object of protection under German patent law. Thus, the same does not preclude the herein examined measures.[54]

Software cannot achieve protection by patent as such. However if the computer program contains a technical feature that goes beyond what is necessary to interact with the hardware it may attain such protection.[55] It is predominantly seen as decisive to whether a program can achieve protection as a so-called computer-implemented invention or not, that the software takes over an additional technical function that goes beyond the pure control of the hardware.[56]

If a computer program fulfills this requirement, a product patent will be granted. According to § 9 (2) No. 1 PatG product patents restrain third persons from manufacturing, offering for sale, marketing or using the product, importing or possessing it for the aforementioned purposes.

However, since the patent owner (supplier) consented to circulating the software copy,[57] the patent right is exhausted. Due to the application of the first sale doctrine in patent law as well, the patent owner cannot prohibit the use of the respective object.[58]

Moreover, according to § 11 No. 2 PatG the protection by patent is limited. Measures that pursue experimental purposes relating to the subject matter of the invention are forbidden. However, if only existing information is to be confirmed, the taken measure is not prohibited by German patent law.[59]

V. Conclusion

The protection systems described herein do not suspend each other. The holder of the respective rights can enforce them independently. Thus, computer programs can enjoy simultaneous protection of several of these systems.[60] In particular, the reverse engineering limitation under the GeschGehG cannot

be transferred to the other protection systems. The explanatory memorandum to the draft law at the time expressly excludes this application.[61] In addition, each protection system also contains an elaborated limitation system, which must not be circumvented by the transmission of external limitations.[62] Recital 38 of the Confidentiality Directive states that the Directive does not preclude the application of other relevant legislation, including copyright rules.

It turns out that a large number of examination measures which serve to detect security-relevant software errors are intended uses in the sense of § 69d Para. 1 UrhG. This evaluation of copyright must be transferred to the new Law on the Protection of Trade Secrets and the Patent Law, which, however, is likely to be very difficult under the differentiated provisions of the first. Therefore, we will have to wait for further legal developments in order to establish a uniform system of intellectual property protection with regard to the prerequisites and limits of software examination.

Thomas Hoeren, Institute for Information, Telecommunication and Media Law, University of Münster

Stefan Pinelli, Attorney at law, Volkswagen AG, Wolfsburg

Notes

1 *Pinions*, WRP 2018, 795 (796).
2 Detailed information on the different black box methods: *Schmidt* in Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2nd edition 2016, § 1 Rn. 300 ff.
3 *Schmidt* in Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2nd edition 2016, § 1 marginal 72.
4 For protection requirements related to encryption algorithms see *Triebe*, WRP 2018, 795 (796).
5 *Czychowski* in Fromm/Nordemann, Copyright, 12th ed. 2018, § 69a marginal 18; *Raubenheimer*, CR 1996, 69 (69).
6 *Grützmacher* in Wandtke/Bullinger, UrhR, 4th ed. 2014, § 69c marginal 4; *Redeker*, IT-Recht, 6th ed. 2017, marginal 45.
7 BGH, Urt. v. 3.2.2011 - I ZR 129/08, WRP 2011, 480 (482) - UsedSoft.
8 *Dreier* in Dreier/Schulze, Copyright Act, 6th ed. 2018, § 69c marginal 14; *Grützmacher* in Wandtke/Bullinger, Copyright Act, 4th ed. 2014, § 69c marginal 17.
9 *Grützmacher* in Wandtke/Bullinger, UrhR, 4th ed. 2014, § 69c marginal 17.
10 *Dreier* in Dreier/Schulze, UrhG, 6th ed. 2018, § 69c marginal 15; *Redeker*, IT-Recht, 6th ed. 2017, marginal 61.
11 LG Hamburg, Ert. v. 3.5.2016 - 408 O 46/16, CR 2016, 782 (783); *Dreier* in Dreier/Schulze, UrhG, 6th ed. 2018, § 69c marginal 16.
12 *Grützmacher* in Wandtke/Bullinger, UrhR, 4th ed. 2014, § 69c marginal 18.
13 *Dreier* in Dreier/Schulze, Copyright Act, 6th ed. 2018, § 69c marginal 16; *Grützmacher* in Wandtke/Bullinger, Copyright Act, 4th ed. 2014, § 69c marginal 18.
14 Supplementation of the source code as a classical form of processing, *Czychowski* in Fromm/Nordemann, Copyright, 12th ed. 2018, § 69c Rn. 21.
15 Higher Regional Court Frankfurt a.M., Urt. v. 29.10.2013 - 11 U 47/13, MMR 2014, 661 (662).
16 *Dreier* in Dreier/Schulze, Copyright Act, 6th ed. 2018, § 69a marginal 34.
17 *Wiebe* in Spindler/Schuster, Electronic Media Act, 3rd ed. 2015, § 31 UrhG Rn. 12.
18 Zum Ganz *Schulze* in Dreier/Schulze, Copyright Act, 6th ed. 2018, § 31 Rn. 114 ff. m.w.N.; *Wiebe* in Spindler/Schuster, Electronic Media Act, 3rd ed. 2015, § 31 UrhG Rn. 12.
19 *Schulze* in Dreier/Schulze, Copyright Act, 6th ed. 2018, § 31 marginal 114.
20 *Schulze* in Dreier/Schulze, Copyright Act, 6th ed. 2018, § 31 marginal 114.
21 For the limits of such agreements see *Grützmacher* in Wandtke/Bullinger, UrhR, 4th ed. 2014, § 69d para. 33 et seq.
22 See *Grützmacher* in Wandtke/Bullinger, UrhR, 4th ed. 2014, § 69d marginal 1, 3rd ed.
23 *Dreier* in Dreier/Schulze, Copyright Act, 6th ed. 2018, § 69d marginal 5.
24 *Witte/Auer-Reinsdorff* in Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2nd edition 2016, § 5 marginal 211; *Dreier* in Dreier/Schulze, Urheberrechtsgesetz, 6th edition 2018, § 69d marginal 6.
25 OLG Düsseldorf, Urt. v. 29.5.2001 - 20 U 166/00, CR 2002, 95 (96 f.); *Wiebe* in Spindler/Schuster, Elektronisches Mediengesetz, 3rd ed. 2015, § 69d UrhG marginal 11; *Grützmacher* in Wandtke/Bullinger, UrhR, 4th ed. 2014, § 69d marginal 7.
26 Higher Regional Court Frankfurt a.M., Urt. v. 17.8.2017 - 5 U 152/16, MMR 2018, 100 (101).
27 *Czychowski* in Fromm/Nordemann, Copyright, 12th ed. 2018, § 69c marginal 39.
28 Cf. OLG Cologne, reference decision of 20.12.2017 - 18 U 112/17, NJW-RR 2018, 373.
29 At least one processing of the program is necessary for error correction, *Grützmacher* in Wandtke/Bullinger, UrhR, 4th ed. 2014, § 69d marginal 17.
30 BGH, Urt. v. 12.12.1999 - VIII ZR 299/98, NJW 2000, 1415 (1415).
31 *Dreier* in Dreier/Schulze, UrhG, 6th edition 2018, § 69d marginal 10.
32 *Wiebe* in Spindler/Schuster, Electronic Media Act, 3rd ed. 2015, § 69d UrhG marginal 28; *Grützmacher* in Wandtke/Bullinger, UrhR, 4th ed. 2014, § 69d marginal 64.
33 *Czychowski* in Fromm/Nordemann, Copyright, 12th ed. 2018, § 69d marginal 28; *Grützmacher* in Wandtke/Bullinger, Copyright, 4th ed. 2014, § 69d marginal 63.
34 *Pinion*, WRP 2018, 795 (799).
35 *Czychowski* in Fromm/Nordemann, Copyright, 12th ed. 2018, § 69d marginal 29.
36 *Kaboth/Spies* in BeckOK, Copyright, 23 Ed. 15.1.2019, § 69d Rn. 15.
37 *Wiebe* in Spindler/Schuster, Electronic Media Act, 3rd ed. 2015, § 69d UrhG Rn. 28 m.w.N.
38 So also *Triebe*, WRP 2018, 795 (798); for the admissibility of the error search *Kaboth/Spies* in BeckOK, Urheberrecht, 23. Ed. 15.1.2019, § 69d marginal 15; *Grützmacher* in Wandtke/Bullinger, UrhR, 4th edition 2014, § 69d marginal 63.

39 *Czychowski* in Fromm/Nordemann, Copyright, 12th ed. 2018, § 69d marginal 28; *Kaboth/Spies* in BeckOK, Copyright, 23rd ed. 15.1.2019, § 69d marginal 15; *Wiebe* in Spindler/Schuster, Electronic Media Act, 3rd ed. 2015, § 69d UrhG marginal 28.

40 *Czychowski* in Fromm/Nordemann, Copyright, 12th ed. 2018, § 69e marginal 1, 8 f.; *Grützmacher* in Wandtke/Bullinger, Copyright, 4th ed. 2014, § 69e marginal 7.

41 *Czychowski* in Fromm/Nordemann, Copyright, 12th ed. 2018, § 69f para. 15.

42 Similar to *Grützmacher* in Wandtke/Bullinger, UrhR, 4th ed. 2014, § 69f Rn. 13.

43 See *Kreutzer*, CR 2006, 804 (806).

44 *Kreutzer*, CR 2006, 804 (806 ff.).

45 *Kaboth/Spies* in BeckOK, Copyright, 23. Ed. 15.1.2019, § 69f Rn. 9.

46 Cf. LG Munich I, judgment v. 13.3.2008 - 7 O 16829/07, MMR 2008, 839 (841); *Kaboth/Spies* in BeckOK, Copyright, 23. Ed. 15.1.2019, § 69f para. 10; referring to the main purpose of the means of circumvention, *Czychowski* in Fromm/Nordemann, Copyright, 12. ed. 2018, § 69f para. 11.

47 Directive (EU) 2016/943 on the protection of commercially sensitive information (business secrets) against unlawful acquisition, use or disclosure. Available at https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L0943&from=DE, last retrieved 1.3.2019.

48 BGBl I 2019, 466 valid from 26.4.2019; The government draft is available at https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_GeschGehG.pdf;jsessionid=38047E8EF10338EF53661CFC7627E69F.2_cid324?__blob=publicationFile&v=1, last accessed 1.5.2019.

49 *Grohmann*, GRUR-Prax 2019, 27 (29); *Hiéramente/Golzio*, CCZ 2018, 262 (263); *Hoeren/Münker*, WRP 2018, 150 (152); *Von Busekist/Racky*, ZRP 2018, 135 (137).

50 See *Müllmann*, ZRP 2019, 25 (26); *Partsch*, Stellungnahme zum GeschGehG, available at https://www.transparency.de/fileadmin/Redaktion/Aktuelles/Stellungnahmen/2018/18-12-11_Stellungnahme_Umsetzung_der_EU-Richtlinie_zu_GeschGehG.pdf, last downloaded 12.3.2019.

51 See *Hoeren/Münker*, WRP 2018, 150 (151); see *Kalbfus*, GRUR 2016, 1009 (1010).

52 *Hoeren/Münker*, WRP 2018, 150 (152).

53 *Köhler* in Köhler/Bornkamm/Feddersen, UWG, 37th ed. 2019, previous sections 17–19 marginal 47; *Trebeck/Schulte-Wissermann*, NZA 2018, 1175 (1179).

54 Another exciting question is what effect US patents have on software. A discussion would go beyond the scope of the essay. The same applies to the question of how the investigation obligations in the context of the DSGVO and KRITIS should be viewed from the point of view of information security.

55 *Bacher* in Benkard, PatG, 11th edition 2015, § 1 marginal 105.

56 *Baldus* in Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2nd edition 2016, § 5 marginal 112; *Osterrieth*, Patentrecht, marginal 377.

57 Exemplary BGH, Urt. v. 26.9.1996 - X ZR 72/94, GRUR 1997, 116 - Prospectus holder; *flocks* in Benkard, PatG, 11th edition 2015, § 9 marginal 16.

58 *Schweyer*, The Legal Evaluation of Reverse Engineering in Germany and the USA, p. 317.

59 *Flocks* in Benkard, PatG, 11th edition 2015, § 11 marginal 6.

60 *Pinions*, WRP 2018, 795 (796).

61 RegE p. 24, available at https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_GeschGehG.pdf?__blob=publicationFile&v=1, last retrieved 12.3.2019.

62 See *Kaboth/Spies* in BeckOK, Copyright, 23. Ed. 15.1.2019, § 69c marginal 1; see also *Triebe*, WRP 2018, 795 (804).