

Cybersecurity in the Realm of Legal Philosophy: where mankind confronts cyberspace

ความมั่นคงปลอดภัยทางไซเบอร์ในขอบเขตของปรัชญากฎหมาย

Supichaya Soonthornthum
(สุพิชญา สุนทรธรรม)

LL. B Candidates

Faculty of Law, Chulalongkorn University, Phayathai Road, Pathumwan, Bangkok 10330

Corresponding author E-mail; 6340286734@student.chula.ac.th

นิสิตในหลักสูตรนิติศาสตรบัณฑิต

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กรุงเทพฯ 10330

Abstract

Amidst the ongoing advancement of technology in the digital era, it is inevitably known that cybercrime has often been conducted in the internet sphere to acquire targeted information through unauthorized methods. Cybersecurity is the mean to combat against this malicious access through cybercrime. Many wonder how far this cybersecurity can go without abusing its power and authority.

Some facets of cybersecurity may infringe on fundamental values such as equality, fairness, privacy, or freedom when overemphasized; however, taking cybersecurity for granted could undermine individuals' trust and confidence in many aspects of life. For instance, while cybersecurity is used as a tool to protect the data and privacy of individual, it also facilitates more access through private information by spontaneously giving those data to cybersecurity technicians as a pathway to identify malicious activities.

Accordingly, cybersecurity raises a plethora of ethical issues as to whether it can be conducted or not, assuming that the conduct itself violates the fundamental rights of engaged individuals, which respectively leads to another question as to which extent can cybersecurity be

implemented while balancing the benefits and the drawbacks to preserve those fundamental rights from being violated.

This article is thus written to envisage how cybersecurity shall be implemented and to guide the answers to the questions raised above by analyzing the issues through the lens of legal philosophy in the ambit of natural law school and positivism school of jurisprudence.

Keywords: cybersecurity; natural law school; positivism law school

บทคัดย่อ

ความปลอดภัยทางไซเบอร์ก่อให้เกิดประเด็นทางจริยธรรมหลากหลายประเด็น โดยเฉพาะประเด็นว่าด้วยความเหมาะสมในการดำเนินมาตรการดังกล่าว ด้วยเหตุที่มาตรการเช่นว่าย่อมนำไปสู่การจำกัดสิทธิพื้นฐานของปัจเจกชน อันนำไปสู่คำถามที่ตามมาว่าเราจะสร้างความสมดุลระหว่างการดำเนินมาตรการด้านความมั่นคงทางไซเบอร์กับสิทธิขั้นต้นเช่นใด บทความนี้มุ่งศึกษาและวิเคราะห์ประเด็นว่าด้วยการดำเนินมาตรการว่าด้วยความมั่นคงทางไซเบอร์บนพื้นฐานของทฤษฎีนิติปรัชญาสำนักกฎหมายธรรมชาติและสำนักกฎหมายบ้านเมือง

คำสำคัญ: ความมั่นคงปลอดภัยทางไซเบอร์; โรงเรียนสำหรับศึกษาเรื่องกฎหมายธรรมชาติ; โรงเรียนสำหรับศึกษาเรื่องกฎหมายพฤติกรรม

Introduction: The Two Distinct Jurisprudences

Legal Jurisprudence has been a subject that was one of the prominent interests of many thoughtful philosophers. When trying to understand the core concept of legal philosophy, it is thereby crucial to study the two main schools of legal thought: the school of natural law and the school of positivism. This article offers different perspectives of certain legal philosophers whose thoughts were based on different legal jurisprudences.

Firstly, one of the most distinguishing notions is the separability of law and morality deemed to be the core concept that positivists such as H.L.A. Hart raised as their main argument, while the natural law theorists, for example, Lon Fuller, consistently defended this statement. Although Hart and his fellow positivists centered their belief around the question of 'what the law is' as distinct from that of 'what the law ought to be', Hart accepted the minimum content theory of natural law as to morality. Still, by incorporating the minimum standard of morality into the legal system, Hart contended that they are only deciding what ought to be from within the framework of the legal system, so the legal system is free-floating.

Of the fact that inclusionary positivism allows a certain extent of morality into the legal system, Lon Fuller, a natural law theorist, contended that legal positivists are moralizing the nature of morality when, in fact, the moral input into the legal system is already there in positivism theory.¹ Natural law theorists added that when we see the attempt to internally reconcile all legal principles, it is seen as a value of fidelity to law, or the so-called value outside of the legal system to which that legal system necessarily refers.² The fidelity to law has been laid out as one of the chief issues as to how law and morality shall be distinguished from one another, otherwise, they are intermingled with each other.

“Law, as something deserving loyalty, must represent human achievement; it cannot be a simple fiat of power or a repetitive pattern discernible in the behaviour of state officials. The respect we owe to human laws must surely be something different from the respect we accord to the law of gravitation.”³

¹ Jeffrey Kaplan, 'Hart – Concept of Law – Ch5 (Primary and Secondary Rules)' (21 July 2020) <https://www.youtube.com/watch?v=Xg_9F2h89TE> accessed 22 April 2023.

² Ibid

³ Lon Fuller, *Positivism and Fidelity to Law: A Reply to Professor Hart* (71 Harv. L. Rev. 1958) 632

The excerpt from Fuller's work stated above is genuinely recognized by some of the positivists as well, for example, Hart officially criticized, in his work, on the Nazi regime⁴ and proposed the concept of an absolute monarch or *Rex*⁵ showing that he is also against the fiat of power, as a special prescriptive power, and advocates for the habit of obedience through *the Rex* system. Still, the concept of fidelity to law is differentiable between the notions of positivism and natural law school; therefore, it cannot be easily concluded as to which sides shall scholars agree on since it is one of the contents of controversial issues.

Accordingly, discussing this topic will not provide any more profitable solutions to the problem. However, it can be mentioned that fidelity to law is a facet of morality in legal positivism that positivists may not knowingly recognize throughout the legal system process. On the other hand, it is also arguably and widely discussed on the natural theorists' notion under their precious morality.

By far, the article will propose that we cannot examine the notion of cybersecurity by looking merely at one of the two distinct jurisprudences to the exclusion of the other since some aspects of both jurisprudences apply to the cybersecurity system. Some of these are derived from the natural law school, while it would be more suitable to examine some of the facets of cybersecurity through positivism.

Consequently, this article will explicate firstly the brief notion of a penumbra of law and the fidelity to law as the main debate between Hart and Fuller in Chapter 1, it will then elaborate on the debate between Hart and Dworkin, on the notion of rules and principles in the same chapter. Respectively in Chapter 2, the article will provide the readers with the concepts of legal indeterminacy and state of exception through the lens of cybersecurity. Lastly, the suggestion and recommendation on how cybersecurity can be best implemented from the perspectives of legal jurisprudences will be drawn out in the Conclusion.

1. Legal Elements, concerning Cybersecurity Laws, that constitute A Legal System.

As mentioned above, the two distinct jurisprudences have some fundamental differences in the viewpoint that underlie the whole debate between H.L.A. Hart and Lon Fuller. From within

⁴ Hart, *Positivism and the Separation of Law and Morals* (71 Harv. L. Rev. 1958) 615-21

⁵ Hart, *The Concept of Law* (2nd ed, Bulloch and Raz 1994) 52

the framework of positivism holding on the principle of separability of law and morality, there has been a question raised among the debate concerning the gray zone of interpretation, or the so-called penumbral situation. The question centers on an issue of law enforcement. Although the positivists claim that the legal system is a free-floating system and morality lies outside the realm of this system whose judges or the authorized officials are the ones who decide on the application of law, the natural law theorists raise a solid counterargument, which is that of interpretation issue.

Natural law theorists emphasize that the assertion of positivists treads more dubious ground since when the authorized figures decide where and how they apply the enacted provision or law, those figures shall inevitably apply the law. By applying the law, the problem will not arise if it can be comprehended by the mere direct application of the law; however, the problem will emerge if there is a gray zone in the application of the law which is when the law cannot be directly applied to the fact of a disputing case. Thus, the interpretation will occur as a tacit solution to the gray zone of law or the penumbral situation.

It is therefore recognized that by doing so, the stance of positivists is at risk when faced with natural law theorists' counterarguments. By exploring the interpretation issue, the implied question is raised as to whether the judges may decide 'what is' by analyzing 'what ought to be' which tacitly leads to the acknowledgement that they also take some morality aspect into their consideration when facing with the interpretation issue.

Hence, when trying to examine legal jurisprudences to understand the notion of cybersecurity, it is crucial not to take any of the legal schools of thought for granted since the mixed approach of studying legal jurisprudences is recommended.

After the above issue has been discussed, another debate that often respectively emerges is some of the aspects in the H.L.A. Hart and Dworkin Debate. According to this debate, Hart first introduces the concept that there shall be primary and secondary rules for some system of rules to be a legal system. These two types of rules, or 'the union of primary and secondary rules', may be regarded as 'the essence of a law.'⁶ It thus confers that a system that merely has primary rules is going to run into all kinds of defects.⁷

⁶ Hart, *The Concept of Law* (2nd ed, Bulloch and Raz 1994) 155

⁷ Jeffrey Kaplan, *supra* note 1

The first defect is called ‘uncertainty.’ It stems from the question of what the law is or what the rules are. Hart once mentioned that:

*“Hence if doubts arise as to what the rules are or as to the precise scope and some given rule, there will be no procedure for settling this doubt, either by reference to an authoritative text or to an official whose declarations on this point are authoritative.”*⁸

This depicts that only a small community closely attached to kinship, common sentiment, and belief, and placed in a peaceful environment, could consistently exist by such a regime of primary rules.⁹ On this problem, if there is a secondary rule said what counts as a rule and who decides what counts as a rule which is a Rule of Recognition¹⁰, then the dispute will be settled. These secondary rules in the ambit of cybersecurity are, for example, EU International Cyberspace Law and Policy, and the purposive orders deciding what counts as rules from the National Cyber Security Agency (NCSA) of Thailand.

The second defect is called ‘staticness.’ The static nature of law happens due to its unchanging nature or slowly changing nature. As Hart stated:

*“The only mode and change in the rules known to such a society will be the slow process of growth, whereby courses of conduct once thought optimal becomes first habitual or usual, and then obligatory, and the converse process of decay when deviations once severely dealt with is first tolerated and then pass unnoticed.”*¹¹

Hart contends that if society merely has primary rules, then the rules can only change through a mutual agreement and a slow time-consuming process.¹² These slow changes emerge when there is firstly a course of conduct that was thought optimal, but not required, then that kind of behaviour was thought to be a better kind of behavior. In other words, it is perceived as a better way to behave and eventually becomes habitual or common practice. This process takes

⁸ Hart, *The Concept of Law* (2nd ed, Bulloch and Raz 1994) 92

⁹ Ibid.

¹⁰ J. Austin, *The Province of Jurisprudence Determined* (H.L.A. Hart ed. 1954) 92; Michael Payne, *Hart’s Concept of A Legal System* (18 William & Mary Law Review 1976) 289

¹¹ Hart, *supra* note 8

¹² Jeffrey Kaplan, *supra* note 1

place for a long process of time to be a course of conduct that is obligatory.¹³ Hence, if any courses of conduct are to be publicly viewed as obligations in a legal system, there have to be enough people who think of those conducts as obligatory which takes an enduring period to do so.¹⁴ Likewise, the same pattern goes for getting rid of the old rules whose mechanism is known as a converse process of decay.¹⁵

It is thus inevitably crucial to have another distinct pattern of rules which is the secondary rules about how to change the rules. That distinct pattern is called “a rule of change” which is considered as a kind of the power-conferring rules.¹⁶ The secondary rules in this context are agreements between state parties, other binding instruments, and the general principles of law. Other binding instruments can be, for instance, UNGA Resolution 53/70 and UNGA Resolution 68/98. For the latter UNGA Resolution, it has been stated in paragraph 21 that States shall make efforts to address the security of ICTs to go hand-in-hand with respect for human rights and fundamental freedoms outlined in the Universal Declaration of Human Rights and other international instruments.¹⁷ It is thus an obligatory duty for each State to abide by this binding instrument unless there is no other novel instrument that overrules the old paradigm for state practices.

Lastly, the third defect is concerned with 'inefficiency,' in determining if the rules are violated. As Hart explicated in his work:

*“Disputes as to whether an admitted rule has or has not been violated will always occur and will, in any but the smallest societies, continue interminably, if there is no agency specifically empowered to ascertain, finally and authoritatively, the fact of violation.”*¹⁸

Legal scholars have agreed about what the rules are, and there is no need to change them as they are fixed for a moment. However, once there is an accusation of someone's wrongdoing

¹³ Mehrdad Payandeh, *The Concept of International Law in the Jurisprudence of H.L.A. Hart* (21 The European Journal of International Law, EJIL 2011) 983

¹⁴ Jeffrey Kaplan, *supra* note 1

¹⁵ Ibid.

¹⁶ Hart, *The Concept of Law* (2nd ed, Bulloch and Raz 1994) 96

¹⁷ UNGA Resolution 68/98, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/68/98, 2013) para 21.

¹⁸ Hart, *The Concept of Law* (2nd ed, Bulloch and Raz 1994) 93

and that individual defend oneself, there will be no way to settle an incessant dispute if the community is only regulated by the mere primary rules. Thus, any disputing problems will not be ultimately resolved unless there are a bunch of secondary rules or the rule of adjudication in a constructed system. The Rule of Adjudication can be structured through institutions of police, judges, and juries and can be mechanized through the process of gathering evidence and the channel of different trials. Examples of the rule of adjudication in the cybersecurity facet are Thailand Cybersecurity Act 2019, article 61 to article 69. Specifically considered, article 61 of this law is written purposively to confer the power of an authorized organization named the National Cyber Security Agency (NCSA) on collecting both the testimonial and physical evidence when there is any imminent threat or cybercrime that reaches the highest threshold of gravitation.¹⁹

So far, Hart elaborated on his widely recognized concept of primary and secondary rules which are parts of the foundation of a legal system. Another facet of a legal system that is typically raised among legal scholars is Dworkin's notion of principles as a tool to supplement the system to cover some legal gaps.

Rules are the obligations toward any behaviour which applied in an all-or-nothing fashion²⁰, meaning that if an individual's behaviour is against a rule, it will be interpreted as delict. On the other hand, with Dworkin's notion of principle accepted, it will be easier to understand the legal system as a whole since some problems arising from the hard cases cannot be tackled unless there are rules incorporated with principles.²¹ A perplexity may happen to the legal system without principles because the rules are defeated by people's behaviour or other considering factors. The principle is, however, different from rules when they are applied in cases. The difference lies in the fact that the principle applies to any disputing cases albeit outweighed by other considerations or surrounding factors.²² It is, from the perspectives written in this article, of crucial aspect for legal scholars to note that legal elements constituting a complete legal system shall be comprised of both rules and principles.

¹⁹ Thailand Cybersecurity Act 2019, s 61(1).

²⁰ James Donato, *Dworkin and Subjectivity in Legal Interpretation* (40 Stanford Law Review 1517) 1987-88

²¹ Elise G. Nalbandian, *Notes on Ronald Dworkin's Theory of Law* (3(2) Mizan Law Review 2009) 375; See also Riggs v. Palmer (1899).

²² Jeffrey Kaplan, *supra* note 1

2. When Legal Indeterminacy Provokes the State of Emergency of Cyberspace.

After the notions of two distinct jurisprudences are discussed, it can be construed that legal scholars may examine the two distinct jurisprudences by utilizing a mixed approach to resolve issues in question as to the realm of cyberspace.

Regarding “the problem of penumbra”, the problem of legal indeterminacy concurrently occurs amidst this grey zone of interpretation. This problem, raised by Hans Kelsen, in his work, *The Reine Rechtslehre*, points out the relative indeterminacy of every law-applying act.²³ The notion of indeterminacy from Kelsen’s perspective is described in the sense of the lack of a determination or the decision of the lower authority.²⁴ Put briefly, in a legal system that is, of nature, dynamic, the validity of lower-level norm is not completely determined by its higher-level counterpart. In other words, the validity of the higher rule is a necessary, but not sufficient condition of the lower rule’s validity.²⁵ It can be comprehended that a lower rule must be issued without indeterminacy through an act of decision or determination of the lower authority in compliance with the higher rule to emerge validly into existence.²⁶ It is, however, crucial to acknowledge that the higher-level norms cannot inclusively govern the lower-level norms although there is a hierarchy of law.²⁷

Thus, the law is, in this sense, inconclusive when it does not examine a specific solution for each case. If an activity that is carried out either by officers (the lower authority) or by judges (the authority applying the law) is not regulated and determined by a higher rule, it will fall into the sphere of a discretionary activity.²⁸ When deciding on “hard cases”, the judges shall thereby

²³ Kelsen, *Reine Rechtslehre* (2nd edn, 1960) cited in Claudio Luzzati, *Discretion and “Indeterminacy” in Kelsen’s Theory of Legal Interpretation* (n.d.) 1; Kelsen, *Introduction to the Problems of Legal Theory: A Translation of the First Edition of the Reine Rechtslehre or Pure Theory of Law* (Oxford University Press 1997) 65-67, 78

²⁴ Kelsen, *Introduction to the Problems of Legal Theory: A Translation of the First Edition of the Reine Rechtslehre or Pure Theory of Law* (Oxford University Press 1997) 78-79

²⁵ Claudio Luzzati, *Discretion and “Indeterminacy” in Kelsen’s Theory of Legal Interpretation* (n.d.) 5

²⁶ Ibid.

²⁷ Kelsen, *General Theory of Law and State* (The 20th Century Legal Philosophy Series, Vol. I. Harvard University Press, 1945) 161-162; Kelsen, *Introduction to the Problems of Legal Theory: A Translation of the First Edition of the Reine Rechtslehre or Pure Theory of Law* (Oxford University Press 1997) 78

²⁸ Claudio Luzzati, *supra* note 23

exercise their discretion to resolve the disputing cases.²⁹ Hence, the core concept of legislating and interpreting the law is concerned with discretion.

Legal indeterminacy can happen in every law-applying act, for instance, Thailand Cybersecurity Act 2019 since each law may not be complete in itself, and it is ineradicably indeterminate. To illustrate, Thailand Cybersecurity Act 2019, article 60 may depict an indeterminacy on how NCSA shall determine the gravity of cyber threats, leading to their use of discretion. Hence, the aforementioned discretion is in dire need of the adjudication of cyberspace relating to cases as the article has already discussed in the topic of the Rule of Adjudication. It is thereafter crucial to point out that when an indeterminacy in the cybersecurity law occurs, it is similar to other law-applying acts in the sense that it requires the decision or discretionary determination of the authority, which shall comply with the higher-level norms. This is widely recognized as Kelsen's so-called *Stufenbaulehre* or the theory of legal hierarchy³⁰.

A judicial decision, for example, is implicitly seen as the enactment of a specific norm that confers power from the statute to which it applies.³¹ The enactment of the statute is, in turn, accepted and authorized by the constitutional norms seeking to frame the proper procedure for legislation process. The limitations for a creation of general legal norms may also be laid out through the so-called constitutional norms.³² Hence, from the Kelsenian perspective, scholars hold a belief that the activity of legislators shall be subject to constitutional review to be in the check-and-balance system. This notion of Kelsen is invoked amidst the unusual and disrupted situation of *Prassenschlag*.

Though Kelsen's argument received several commendations, his plea for the embarkment of creating a proper constitutional court in Weimar Germany also gained strong opposition from Carl Schmitt through his 1931 monograph *Der Hüter der Verfassung* or The Guardian of the Constitution. In short, Schmitt neither supported Kelsen's constitutional adjudication nor parliamentary sovereignty. In the aspect of the opposition to constitutional adjudication, Schmitt contended that constitutional adjudication exceeds the legitimate purview of the court.³³ His

²⁹ Juan Alberto del Real Alcalá, *The Controversies about Legal Indeterminacy and the Thesis of the 'Norm as a Framework' in Kelsen* (European Journal of Legal Studies, 2013) 177

³⁰ This is a theory that Kelsen adopted from his pupil Adolf Julius Merkel; Compare Kelsen, *Reine Rechtslehre* (1934), 55–75

³¹ Lars Vinx, *The Guardian of the Constitution* (2015) 7

³² Ibid. 8

³³ Lars Vinx, *The Guardian of the Constitution* (2015) 9; Schmitt (1931a), 12–48; See also Schmitt (1967).

argument is focused on the fact that a judicial tribunal typically encounters contestable and controversial disputes, or hard cases in the Dworkinian sense. Meanwhile, constitutional provisions are often too ambiguous and open-textured to allow for unanimous or specifically correct decisions. Consequently, the court would be forced to take political decisions which are no longer justifiable as the application of determinate legal norms,³⁴ and would thus violate the separation of powers.

Another aspect of Schmitt's opposition toward parliamentary sovereignty is based on the claim that modern parliament, where the limitations of the state's interference with the society and economy often disappeared, is in no way capable of maintaining political decisions in the name of people as a whole.³⁵ The state tends to be controlled by parliamentary majorities that capriciously act for private gains. Thus, parliament cannot be designated as a guardian of the constitution. In this way, when there are any cyber threats and the state must employ the cybersecurity act that may infringe embedded human rights, it can be construed that neither the existence of the parliament nor of the judicial tribunals is justifiable in coping with a legal indeterminacy.

Accordingly, the issue in question is concerned with what will be a reasonable answer that confers power to the state concerning the problems arising in cyberspace. Fortunately, there is another notion expounded by Schmitt in his work named *The Guardian of the Constitution* that may, to some extent, resolve and give an answer to the problem in question. This concept is founded on Schmitt's belief that the president's power of dictatorship conferred by article 48 paragraph two of the Weimar Constitution is legitimate and that by launching an emergency decree, the president showed himself to be the true guardian of the constitution.³⁶ Schmitt gave the reason behind his notion of sovereign dictatorship that the application of all law, including constitutional law, is in dire need of a condition of normalcy. If the law is threatened, it can only be secured by extra-legal rules launched by dictators or executive organizations. From Schmitt's perspective, the sovereign is he who decides on the state of exception.³⁷ In other words, when

³⁴ Lars Vinx, *The Guardian of the Constitution* (2015) 9

³⁵ Schmitt (1931a), 73–91; See also Schmitt (1938), 65–77.

³⁶ Schmitt (1931a), 132–59

³⁷ Carl Schmitt, *Political Theology: Four Chapters on the Concept of Sovereignty* (University of Chicago Press, 2005), trans. George Schwab, 5.

an emergency convulses accepted orders in normalcy, the sovereign steps in to decide on any dispute and deploy extra-legal acts.

Conclusion: Mixed Approaches of Jurisprudences in the Realm of Cybersecurity.

As it is understood, when problems of cybercrime arise and require a cybersecurity law to counter those problems in question, the judges or the judicial tribunals have to decide the verdicts of any disputing cases by using their discretion. In that situation, which is widely recognized as the problem of penumbra, legal indeterminacy concurrently occurs. This leads to the answer to justify the validity of the cybersecurity act that may infringe on individuals' rights through the notion of the state of exception or emergency. It can be subsequently noticed that extralegal rules in cybersecurity arise when it appears to be much more cybercrime committed in the emergent state, and the aftermath of those exceptions persists through the state of normalcy.³⁸ Since all the issues according to cybersecurity amidst the modernized era of globalization can be tackled by the underlying concept of each jurisprudence, it can be affirmatively concluded that cybersecurity law is not in conflict with legal philosophy by looking through the lens of mixed approaches of jurisprudences, whether it is the natural law school of jurisprudence or the positivism.

An analytical conclusion that can be given as an instance is concerned with the concept of self-defense in cyberspace. A legitimate act of defense must be able to stop an imminent unjust attack. If an implemented technique of cyber-defence cannot terminate an imminent unjust attack, then it cannot be defensive but may, rather, be considered offensive³⁹ which cannot be considered self-defence. The core concepts instilled in this widely accepted definition of self-defence in cyberspace are the notions of necessity and imminence which are depicted in article 25 of draft articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), with commentaries from the International Law Commission (ILC). This denotes the incorporative application of article 38(1)(a) of the ICJ Statute, regarding as an international convention, and article 38(1)(d) of the ICJ Statute, regarding as subsidiary means for the determination of the rules

³⁸ Thongchai Winichakul, 'Rule by Legal Exceptions: RbLE' (11 March 2023) <<https://www.facebook.com/Thammasatlaw/>> accessed 26 April 2023.

³⁹ Denning and Strawser (2017) cited in Markus Christen et al., *The Ethics of Cybersecurity* (21 Springer 2020) 321

of law. This integrated application of law implicitly represents an example where rules are incorporated with principles in the realm of cyberspace.

Another instance according to the cybersecurity facet is the question as to whether illegal breaches from cybersecurity service providers can be profited from. This question arises from the case of an Italian antivirus company named *Hacking Team*⁴⁰ which provided offensive technology for cybersecurity this leads to an issue as to whether this company can analyze the source code gained from their technology to improve their tools since it is considered an infringement of the trade secret.

This issue cannot be determined by a clear legal regulation and an ethical choice has to be made. A principle that shall be applied to the case is the principle laid out that 'no man may profit from his wrongs.' However, the principle can lose out to other considerations as it has been earlier stated. It can be subsequently construed that this principle does not imply that the law 'never' permits a man to profit from a wrong he commits. It is thus plausible to conclude that the company may still profit from its offensive technology through this legal reasoning, regardless of the result of the court verdict.

Lastly, the recommendation to be proposed is concerned with Fuller's notion of the inner morality of law which expresses a view that a legal obligation to obey law only arises in response to, or anticipation of, a corresponding effort on the part of the lawgiver. Therefore, this idea of reciprocity to secure fidelity to the law implies that a lawgiver must enter into a relationship of reciprocity with the people who shall be obligated by the law. If the enacted law is failed to meet the eight principles of inner morality of law, it does not simply result in a bad law but rather falls into the ambit of something that shall not be called a legal system at all.⁴¹ If this bond of reciprocity is finally and completely ruptured, 'nothing is left to ground the citizen's duty to obey the lawgiver's rules'⁴²

In summary, to state that cybersecurity law is not in conflict with the notions of legal philosophy, internal law and policy governing the conduct of cybersecurity shall be aligned with the inner morality of law and legal framework of each nation, considering the concept of legal

⁴⁰ Satter R, 'Italian Prosecutors Seek to Shelve Hacking Team Breach Case' (*Phys.org*, 12 December 2017) accessed 28 May 2023.

⁴¹ Kristen Rundle, *Fuller's Internal Morality of Law* (2016) 500

⁴² Fuller, *The Morality of Law* (1969) 40

indeterminacy and discretion. It is also important to note that the problems of cyberspace can be regulated by extra-legal rules as well.