ETHICAL HACKERS UNDER THE INFORMATION TECHNOLOGY ACT: THE CYBER TERRORISM CONUNDRUM AND 'PROTECTED' SYSTEMS

Vivek Krishnani [*]

Recurrent cyber offences, particularly due to the introduction of the Aadhaar scheme by the Unique Identification Authority of India (UIDAI), have made conspicuous the loopholes in the infamous Information Technology Act, 2000. Having said that, what is laudable is the acknowledgement of the flaws by the legislature and its willingness to make amendments to the legislation.

In this Essay, the author claims that certain penal provisions governing "systems restricted for reasons of security of the State", even after significant amendments, are unsuitable for the purpose that underlies them. To realise the intent of the legislature, another amendment to the Information Technology Act is not only prudent but also necessary. Accordingly, this Essay argues in favour of narrowing down these provisions to exclude from their ambit those persons to whom liability was never intended to be attributed.

To expound this argument, the author cites, as an illustration, a hypothetical incident of a lapse in the security framework of the UIDAI. In the latter half, deriving inspiration from the other provisions of the IT Act itself and from internationally accepted definitions of the concerned offences, revisions that could better assist in fulfilling the purpose of the provisions have been proposed.

[*] Vivek Krishnani is a 3rd year BA. LL.B. (Hons.) student at the National Law University, Jodhpur. He may be contacted at vivekkrishnani19@gmail.com. The author would like to thank Mr. Jaideep Reddy for his suggestion of authorising ethical hacking, among other extremely valuable inputs.

CONTENTS

INTRODUCTION

"*Crime is crime because it consists in wrongdoing which directly and in serious degree threatens the security or well-being of society, and because it is not safe to leave it redressable only by compensation of the party injured.*"[1]

Upon a perusal of these lines, one could understand the severity of an act that constitutes crime: *"wrongdoing which directly threatens the society."* Of equal relevance, is the observation that it is something that cannot be redressed by compensation alone. However, there is something more significant than the act (of wrongdoing) itself, which this definition fails to address i.e. the *mens rea* of the accused.

International criminal jurisprudence acknowledges that there can be no crime, large or small, without an evil mind,[2] as the essence of a crime is its *wrongful intent* without which it cannot exist.[3] Consequently, to punish conduct without reference to the state of mind of an actor is both inefficacious and unjust.[4]

[1] SMITH, HOGAN, & DAVID ORMEROD, CRIMINAL LAW 5 (15th ed., 2018).
[2] Francis Bowes Sayre, *Mens Rea*, 45 HARV. L. REV. 974 (1932).
[3] BISHOP, CRIMINAL LAW 287 (9th ed., 1930).
[4] Herbert L. Packer, *Mens Rea and the Supreme Court*, 1962 SUP. CT. REV. 109 (1962) (hereinafter "Packer").

I. SECTIONS 70 & 66F OF THE IT ACT: AN INSIGHT INTO THE AUTHOR'S CONCERNS

A strong foundation for introducing the author's argument is the gripping question raised by Subba Rao J. in a famous dissenting opinion: "*whether the intention of the Legislature is to punish persons who break the said law without a guilty mind?*"[5]

First, what exactly constitutes a guilty mind? The answer to this question would be different for different crimes,[6] as each crime consists of a prohibited act or omission coupled with whatever state of mind is called for by the statute which sanctions it.[7] In this regard, the Indian Penal Code, 1860 provides for various ingredients related to *mens rea* which are incorporated in phrases such as "*intentionally*", "*knowingly*", "*dishonestly*", etc.[8] Such phrases have been provided for in the Information Technology Act, 2000 (hereinafter "IT Act") as well. However, no requisite intention has been provided in the language of Section 70(3), which penalises mere access to a protected system: "*Any person who secures access or attempts to secure access to a protected system in contravention of the provisions...*"[9]

Second, this question leads us to another question which, at first, seems quite futile but is worth analysing once we carefully reconsider it: *can the intention of the legislature be to acquit a person even when he has committed the act with the intention "required" by the statutory provisions?* This question will be answered in the affirmative in two situations: first, when the legal provision is not worded according to the intention of the legislature; and second, when the implementation of the provision is not in accordance with the legislative intent.

Both these situations are of great relevance in the case of Section 66F of the IT Act. The provision defines the scope of cyber terrorism under two parts: Section 66F(1)A and Section 66F(1)B of the IT Act. The problem arises due to the latter which penalises anyone who:[10]

> "*knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such*

[5] State of Maharashtra v. Mayer Hans George, AIR 1965 SC 722.
[6] KD GAUR, COMMENTARY ON THE INDIAN PENAL CODE 132 (2006 ed., 2006).
[7] SMITH & HOGAN, CRIMINAL LAW 116 (14th ed., 2015).
[8] K.N.C. PILLAI, GENERAL PRINCIPLES OF CRIMINAL LAW 8 (2nd ed., 2011).
[9] §70(3), Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (hereinafter "IT Act, 2000").
[10] *Id.* at §66F(1)B.

> *information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise."*

Despite governing an offence as grave as cyber terrorism, the provision has been worded too broadly. It is the *mens rea* required under the provision that broadens it and becomes a cause of concern in two ways.

First, "*knowingly*" accessing a computer system without authorisation becomes fairly easy to prove once we consider the fact that an unsafe system like the Aadhaar scheme comes within the ambit of the provision. This is because the Aadhaar scheme is a system, which can be legally accessed by certain authorised persons only. Additionally, any leak of information from the Aadhaar database would be gravely detrimental to the country due to the contemporary relevance that such information assumes. Due to this, it will be easier to establish that the unauthorised access was accompanied by reasons to believe that such information may be "*likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State,… public order*". Hence, it can be concluded that the Aadhaar scheme is a system "*restricted for reasons of security of the state*" and falls within the scope of Section 66F(1)B of the IT Act.

Second, it brings within its ambit anyone, who "*knowingly*" accesses any restricted information or database in relation to "*contempt of court*" or "*defamation*". It may be noted that defamation or even contempt of court has no bearing on the security of the State, and it is difficult to justify its inclusion. However, this Essay does not deal with the inclusion of defamation and is confined to the ease of proving access to a computer system. The next segment, with the help of an illustration, discusses the same.

An Illustration

The Aadhaar scheme of the Unique Identification Authority of India (hereinafter "UIDAI") involves the collection of biometric and demographic information of 1.3 billion people.[11] It has created the largest biometric identity project in the world and must be scrutinised carefully to assess its compliance with human rights.[12] In fact, the inefficient management of the database is not publicised.[13] Notably, the UIDAI has not only declared the Aadhaar database as a "*protected system*"[14] under Section 70(1) of the IT Act,[15] but has also provided that the biometric information stored amounts to "*sensitive personal data*" under Section 43A of the IT Act.[16]

The latter provision imposes a duty of care on the UIDAI, which is a body corporate,[17] to implement and maintain reasonable security practices and procedures. The practices and procedures that need to be maintained in the case of protected systems (like the Aadhaar database) have been prescribed in the Information Technology (Information Security Practices and Procedures for Protected Systems) Rules, 2018 (hereinafter "2018 Rules"). The author asserts that the UIDAI's compliance with most of the obligations under the 2018 Rules is uncertain. This is due to the non-compliance that has been reported. For instance, the 2018 Rules require the UIDAI to nominate a Chief Information Security Officer (hereinafter "CISO").[18] However, it has been reported with evidence that the UIDAI does not have a CISO to date.[19] Accordingly, far from fulfilling its obligations, the authority has been unable to keep the information secure. What the author wishes to highlight is that the Aadhaar database is a protected system only for namesake, and the UIDAI is

---

[11] *Aadhaar in numbers: key figures from UIDAI CEO's presentation to the Supreme Court*, THE HINDU, March 22, 2018, https://www.thehindu.com/news/national/aadhaar-in-numbers-key-figures-from-uidai-ceos-presentation-to-the-supreme-court/article23323895.ece (last visited May 30, 2020).

[12] K.S. Puttuswamy v. Union of India, 2018 SCC OnLine SC 1642.

[13] *Editors' Guild, Others Condemn FIR Against Journo For Exposing Aadhaar Data Leak, Demand Centre's Intervention*, LIVELAW.IN, January 7, 2018, https://www.livelaw.in/editors-guild-others-condemn-fir-journo-exposing-aadhaar-data-leak-demand-centres-intervention (last visited May 30, 2020).

[14] Declaration of CIDR facility of UIDAI as 'Protected System', MeitY Notification no. G.S.R. 993(E), (December 11, 2015), *available at* http://meity.gov.in/writereaddata/files/UIDAI%20as%20Protected%20System.pdf.

[15] §70(1), IT Act, 2000, *supra* note 9

[16] §43A, IT Act, 2000, *supra* note 9.

[17] §11(2), The Aadhaar Act (Targeted Delivery of Financial and Other Subsidies, Benefits and Services), No. 18 of 2016, Acts of Parliament, 2016.

[18] Rule 3 (3)(a), Information Technology (Information Security Practices and Procedures for Protected Systems) Rules, 2018, THE GAZETTE OF INDIA (2018), pt. II sec. 3 (May 22, 2018).

[19] *Aadhaar Truth: UIDAI Never Appointed a Chief Information Security Officer, Reveals RTI*, MONEYLIFE, February 5, 2019, https://www.moneylife.in/article/aadhaar-truth-uidai-never-appointed-a-chief-information-security-officer-reveals-rti/56267.html (last visited May 30, 2020) (hereinafter "Moneylife").

not employing reasonable security practices for the fulfilment of its duty under Section 43A of the IT Act.[20]

With this backdrop, let us consider an event of a data leak. Say, "A", an information technology student, after having been able to access the Aadhaar database, has circulated a link on WhatsApp, reporting the 'mismanagement' in the Aadhaar database. The WhatsApp link shared claims that the personal details of 1.3 billion Indian citizens have been easily hacked by him and are accessible therein. As a consequence of the ensuing sharing, the link has now reached thousands of people.

Legalistically, access to a computer system may or may not be criminal.[21] To become criminally liable, the concerned people should be able to form the requisite criminal intent in committing the crime.[22] Ethical hackers who penetrate a computer system to merely learn about the actual working of the computer system do not intend to engage in any criminal activity.[23] Resultantly, anyone who tries to expose the fallacy in the Aadhaar system to make the public aware of such a relevant problem does not engage in criminal activity by merely accessing the database. Hence, "A", who managed to penetrate the database, should ideally not come within the scope of any provision, which governs cyber offences.

Interestingly, as per a literal interpretation of the provision, "A" as well as those who opened the link that was shared would fall within the purview of Section 66F of the IT Act. These individuals not only lacked the authorisation but also accessed the system 'knowingly'. This amounts to saying that they committed an act that satisfies the essentials of the provision.

To buttress the argument, the author now introduces a turn of events in the illustration presented above (hereinafter "the modification"). Let us suppose that the link shared by "A" does not actually provide access to the database and has come to the reach of the public as a consequence of a mere publicity stunt by "A". In such a scenario, opening the link in itself would amount to an 'attempt' to access the system which is an offence punishable under Section 70 of the IT Act.

[20] §43A, IT Act, 2000, *supra* note 9.
[21] R.K. CHAUBEY, AN INTRODUCTION TO CYBER CRIME AND CYBER LAW 372 (2nd ed., 2012).
[22] Packer, *supra* note 4, at 109.
[23] Abhinav Gupta v. State of Haryana, 2008 Crim LJ 4536.

Considering such circumstances, attention must be paid to the intention of the legislature: *was the intention of the legislature to convict the people, who have accessed the link shared on WhatsApp for offences as grave as cyber terrorism under Section 70 of the IT Act?* Certainly, it was not. However, these individuals "*knowingly*" accessed the information protected for the reasons of the security of the State and attempted to access a protected system. Hence, as per the prevailing regulatory understanding, they would be liable under Sections 66F and 70 of the IT Act.[24]

At the same time, the UIDAI, which has never provided clarity about the security framework that is in place to safeguard the "*sensitive personal data*" of citizens, would evade liability under Section 43A of the IT Act. This is because the compliance of the UIDAI with the 2018 Rules is not known due to the lack of requisite information on the UIDAI's website. This is pertinent because the 2018 Rules form the relevant standard in the case of protected systems such as the Aadhaar database. Additionally, due to the reporting of non-compliance with respect to the obligation of nominating a CISO,[25] there is an increased apprehension that the UIDAI has not employed adequate security measures.

A different perspective, to address the author's concerns, regarding *mens rea* would be the principle of proportionality which holds that penalties should be proportionate in their severity to the gravity of a defendant's criminal conduct.[26] Applying this principle to the illustration, the thousands of people that have out of concern for their personal information, opened the link, would be criminally liable and come within the domain of offences punishable by imprisonment extending up to 10 years[27] or even lifetime.[28] However, the UIDAI which has breached a serious obligation to keep the information secure is liable merely for a civil wrong under Section 43A of the Act,[29] which, in any case, it escapes because of the requirement of 'reasonable' measures. Consequently, the trap of words laid by the statute disregards the principle of proportionality, which, like *mens rea*, is a fundamental principle of criminal law. The same should be an important consideration during the framing of penal statutes.

[24] §§66F-70, IT Act, 2000, *supra* note 9.
[25] Moneylife, *supra* note 19.
[26] Andrew Von Hirsch, *Proportionality in the Philosophy of Punishment*, 16 CRIME & JUSTICE 56 (1992).
[27] §70, Information Technology Act, 2000, *supra* note 9.
[28] §66F, Information Technology Act, 2000, *supra* note 9.
[29] APARNA VISHWANATHAN, CYBER LAW 97 (1st ed., 2012).

Having determined the whereabouts of the problem, it is desirable to take into account certain definitions and provisions that can assist in crafting a solution for the problem.

II. DEALING WITH THE CYBER TERRORISM CONUNDRUM

As can be gauged from the illustration, the over-inclusively drafted Section 66F(1)B demands scrutiny, particularly, because it might have the effect of bringing ethical hackers within its scope. In this part, the author elaborates on the essence of cyber terrorism from the definition proposed by Dorothy E. Denning, whose research in the field of cybercrimes has been internationally recognised. Apart from this definition, the author also refers to the definition given by the Federal Bureau of Investigation (hereinafter "FBI") and suggests modifications to the Indian provision, i.e. Section 66F of the IT Act.

Denning's definition is instructive in carving the essential ingredients of cyber terrorism. In her words:[30]

> "*Cyber terrorism is the convergence of cyberspace and terrorism utilizing the computer as the weapon and the target. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives*."

Segmentation of this definition aptly depicts the requirements that constitute cyber terrorism: *first*, unlawful access or a threat to access computers, networks or information stored in them, i.e. the act; and *second*, the act must be done to intimidate a government or its people in furtherance of political or social objectives, i.e. the intention.

The *first* ingredient is linked to cyberspace, and the *second* one is very much concerned with terrorism. Thus, the co-existence of these two ingredients is what has been regarded as the "*convergence of cyberspace and terrorism*" in the abovementioned definition.

Mindful of the two ingredients, let us reconsider the illustration (without the modification) discussed in the previous part of the Essay. It must be noted that the act of "A" was not aimed at frightening or intimidating anyone. As stated earlier, the act of "A" was driven by his concern for

[30] Dorothy E. Denning, *Cyber terrorism: The Logic Bomb versus the Truck Bomb*, 2 GLOBAL DIALOGUE 29 (2000).

the security of sensitive personal information. There is no denying that the act of "A" was linked to cyberspace. However, "A" is an ethical hacker whose act was aimed at learning about the security framework. Accordingly, terrorism and its convergence with cyberspace are evidently absent. Even if the act stands established and the first ingredient is satisfied, the intention of doing the act for the purpose of intimidation is missing. As a result, the second ingredient is not satisfied and the act of "A", correctly falls outside the purview of the definition.

This would be the outcome if the definition offered by Mark M. Pollitt, a special agent for the FBI, were to be followed. This definition has been derived from the US Code's definition of terrorism and is an acceptable definition in this regard:[31] Cyber terrorism is:[32]

> "*a premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents.*"

To ascertain the culpability of the act of "A" under this definition, a blow-by-blow analysis of the definition is not required. The phrases "*politically motivated attack*" and "*which results in violence against non-combatant targets*", which find a place in the definition, make it clear to exclude the act of "A". Not only was the act of "A" in furtherance of a completely different object but it also did not result in any violence against any civilian.

Such an outcome is clearly not as off-putting as the one in the case of the Indian provision. Conspicuously, this difference in outcomes arises from the different intentions demanded by the definitions. The requisite intention of "*knowingly*" under Section 66F makes it all-encompassing. Consequently, Section 66F conveniently includes the act of "A", who is merely an ethical hacker.[33]

The author is of the opinion that to better suit the intention of the legislature, the provision could be narrowed through two simple steps. *First*, the phrase "*knowingly or*" which finds a place in the current provision, be omitted. *Second*, restrictive phrases such as "*in furtherance of political objectives*" or "*politically motivated attack which results into violence against non-combatant targets*" be included. This would ensure that the wording of the provision meets the ends sought.

---

[31] 22 U.S.C. §2656f(d)(2).
[32] Mark M. Pollitt, *Cyber terrorism – fact or fancy?*, 1998 COMPUTER FRAUD & SECURITY 8-10 (1998).
[33] §66F, IT Act, 2000, *supra* note 9.

III. ADDRESSING THE CONCERNS REGARDING SECTION 70

In this part, examining the general provision with respect to "*computer related offences*" in the IT Act, i.e. Section 66 of the IT Act, the author suggests rephrasing Section 70 of the IT Act to suit the intent of the legislature.

Section 66 of the IT Act,[34] which is a criminal provision, punishes acts, falling under Section 43 of the IT Act when done "*fraudulently or dishonestly*". Essentially, two broad ingredients must be satisfied to bring an act within the ambit of Section 66 of the IT Act. *First*, the *act* should come within the ambit of Section 43, and *second*, the act must be done either fraudulently or dishonestly, i.e. the *intention*.

As regards the first ingredient, Section 43 of the IT Act, in its relevant part, covers the *act* of accessing a computer, downloading, copying or extracting any data or information from such a computer.[35] The analysis undertaken, however, has little to do with the first ingredient. For our purposes, it is the required *intention* which is pertinent to highlight. Briefly, the two degrees of intention mentioned in the provision, could be understood as follows:

Fraudulently - An *act* is done fraudulently when done with an intention to defraud.[36] Where there is a benefit or advantage or even the likelihood of advantage to the deceiver as a result of the deceit, he is said to have an intention to "*defraud*".[37]

Dishonestly - An *intention* to gain wrongfully by getting what one does not have amounts to a dishonest intention.[38] To gain wrongfully simply indicates towards gaining unlawfully.[39]

Applying this legal matrix, let us determine whether the *actions* of the individuals who attempted to access the Aadhaar database by opening the link satisfy the requisite intention. Neither does their *act* deceive anyone nor does it involve an advantage or even its likelihood for that matter. Accordingly, it does not amount to a fraudulent act. Similarly, in the absence of an *intention* to gain wrongfully, their act is not dishonest.

---

[34] §66, IT Act, 2000, *supra* note 9.
[35] §43, IT Act, 2000, *supra* note 9.
[36] §25, IND. PEN CODE, 1860.
[37] *In re* B.V. Padmanabha Rao, 1970 Crim LJ 1502 (1969); Vimla v. Delhi Administration, AIR 1963 SC 1572.
[38] §24, IND. PEN. CODE, 1860; §5(3), Ch. 6, The Fraud Act 2006 (Eng.).
[39] KN Mehra v. State of Rajasthan, AIR 1957 SC 369.

Therefore, the *actions* of the people, though not satisfying the ingredients of the less serious offence punishable under Section 66 of the IT Act, clearly satisfy the essentials under the more serious offence punishable under Section 70 of the IT Act. Hence, the addition of either of the two degrees of intention appearing in the former provision to the latter, as an essential requirement would restrict the ambit of the provision. Consequently, the instances such as the above illustration will not fall within the ambit of the provision and would thereby solve the problem to a great extent.

CONCLUSION

This Essay elucidates how certain criminal provisions of the IT Act drafted in an all-embracing manner, require a stricter wording to exclude ethical hackers. This exigency demands that other degrees of *mens rea* be incorporated in the provisions of Sections 66F and 70 of the IT Act.

Alternatively, there is a solution in the event that an amendment making the inclusion of *mens rea* as an element of the offence is considered to be inappropriate. The problem with respect to ethical hackers could be solved by a method of formally authorising ethical hacking either by legislation or by way of inclusion in subordinate legislation. This would to a great extent, suffice in addressing the concerns of the author.

While the government and upon its failure, the judiciary need to take care of the UIDAI's compliance with the 2018 Rules, the solutions proposed regarding Sections 66F(1)(B) and 70 of the IT Act require legislative or executive intervention in the manner recommended in the preceding paragraphs. These provisions must be worded in a manner that reflects the intent of the legislature and facilitates their proper implementation. Admitting that the IT Act is a relatively new law and is still undergoing significant changes, the author highlights these issues that require prompt attention.