CYBERSPACE AND ITS RULES

Recognition Of Legislature's Authority

Cyberspace actors are unlikely to follow the law if they do not recognize the legislator's right to control their online behavior. Players will have to make a decision between conflicting and overlapping claims to authority. Its authority may be acknowledged if there is a reasonable chance that the actor may be subject to legal action. However, in other situations—which will be by far the majority—a legislator's authority will only be recognized inasmuch as the online player has integrated themselves virtually into the community which is governed by that legislator. However, this does not imply that the online actor will recognize the legitimacy of every bill that comes from that legislator.

The actor has to decide which specific laws he accepts as establishing legally obligatory obligations, just as he must decide between the opposing assertions made by legislators. A law's legitimacy is likely to be questioned if it calls for actions that are unrealistic or even unfeasible, contradicts with other commitments that the actor acknowledges as binding or with accepted cyberspace norms, or is out of date due to advancements in technology. Like in India in 2021 Whatsapp LLC filed a petition with the High Court of Delhi, requesting the issuance of a writ of mandamus or an alternative appropriate writ, direction, or order, declaring that: (i) the impugned rule 4(2) violates Articles 14, 19(1)(a), 19(1)(g), and 21 of the Constitution; (ii) the imposition of criminal liability for noncompliance with the impugned rule 4(2) is unconstitutional; and (ii) any attempt to impose criminal liability for noncompliance with Impugned Rule 4(2) is unlawful, ultra vires the IT Act[...]. [1]

To put it another way, we need to consider both the substance and the source of the legislation. For lack of a better phrase, lets characterize the provisions of such statutes as having "meaningful" content. It is necessary to evaluate meaning from the actor's point of view. Regretfully, a lot of initiatives to enact meaningful laws in cyberspace have fallen short of this goal.

By assuming that it has a right to control, the legislator limits the scope of legislation to the community (as it relates to cyberspace) . This is insufficient on its own to guarantee that its laws

1 Scc Online Times, *Del HC| Whatsapp challenges Intermediary Rules, says traceability will break end-to-end encryption, breach privacy; Union of India says no Fundamental Right is absolute, available at* <https://www.scconline.com/blog/post/2021/05/27/del-hc-whatsapp-challenges-intermediary-rules-says-traceability-will-break-end-to-end-encryption-breach-privacy-union-of-india-says-no-fundamental-right-is-absolute/> (last visited on 10.07.2024)

will be followed. The legislator still has to make sure that the community's members understand the rules they are imposing and that they carry significant obligations.

Transposing the current legal standards that govern that community to the larger online community is one approach that shows promise. Since the legislators' physical world society already recognizes the significance of such standards, there's a good likelihood that the larger cyberspace community will do the same if they can be properly translated. As it will be evident, however, transposing standards in a fashion that makes sense to the cyberspace actor is not always feasible. Even if this strategy may work, it will only work if the participants are aware of the methods that must be employed to guarantee normative parity between the obligations placed on members of the community who are physically present and those who are not.

Acknowledgement Of Different Kinds Of Subjects Before Legislating

It is imperative for lawmakers to acknowledge that an individual operating in cyberspace is probably involved in several communities. These will comprise groups that are solely in cyberspace as well as the actor's "home" physical world community. Numerous members of these latter groups have established their own internal standards. A cyberspace actor is less likely to understand the significance of competing normative responsibilities that another legislator tries to impose on him if he is a member of one or more communities that impose normative obligations on him and that he views as meaningful. That being said, one of the purposes of law is to establish or reinforce norms by giving them greater authority that stems from the lawmaker's status and the consequent possibility of their enforcement via the legal system's mechanisms. This is not to say that a legislator is limited to creating laws that mirror existing norms in cyberspace. However, a legislator must be aware of the challenges it will have in convincing online actors to submit to the authority of laws that are in such contradiction.

Bringing Offline Legal Standards Online

Legislators generally agree that the same legal standards that govern the real world, whenever feasible, should also be to govern online. The idea is most commonly articulated as follows: online and offline activity should be treated equally under the law.

The Bonn Ministerial Conference Declaration of July 6–8, 1997, contains the first official declaration to this effect in principle[2].

2These are Berne Convention rights, and so almost all countries will have equivalent rules.

The general legal structure should be enforced online, just as they are offline, according to ministers. They will work to create laws that are technology-neutral while keeping in mind the need to prevent needless regulation, given how quickly new technologies are growing.[3]

This statement alluded to the overall corpus of current law because it was believed that, on a case-by-case basis, cyberspace-specific legislation would need to be created when concerns that were only related to cyberspace were discovered. But after a few years, legislators started to see the idea as having broader applicability, which resulted in a legislative strategy that aimed to make all rules and regulations, as much as possible, identical both online and offline. Stated otherwise, the laws governing an activity conducted online ought to be the same as those governing an activity conducted analogously offline.[3]

The need of equivalence between online and physical world rules

It is imperative that laws that are intended for offline spaces be equivalent to those that apply online in order for legislators to capitalize on the normative power that offline spaces currently have. It is less likely that the acceptance of the authority of the new rule by cyberspace players will be influenced by the acceptance of the authority of the comparable norm in the physical world if the new rule places different requirements on them. Even worse, the absence of equivalency could convince the actor operating in cyberspace that the new rule's requirements have no bearing on him. He expects that rules in cyberspace would function exactly like they do offline, and if they don't, this raises questions about the legitimacy of the lawmakers.
It is important to note that equivalency and technological neutrality are not interchangeable terms. Equivalency influences the substantive norms of any law by directing legislators toward the legal principles that ought to govern actions conducted online. Technology neutrality seeks to future-proof the law by preventing technological advancements from rendering its regulations obsolete. It tackles the decision of which substantive rules are available to apply those legal principles.

Risk in applying the principle of Equivalency

3 See eg Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee, and the Committee of the Regions, 'Principles and Guidelines for the Community's Audiovisual Policy in the Digital Age', COM (1999) 0657 final, note 17: 'identical services should in principle be regulated in the same way, regardless of their means of transmission'.

One interpretation of this rule could be that it must be followed in both online and offline contexts. Stated differently, the goal is to find a single rule that works in every circumstance. This could be referred to as form equivalency. From the decisions that extended pre-cyberspace rules to online activity, it is widely established that there are risks involved in attempting equivalency in this strictly formal sense. These incidents brought to light the issue that rules can have significantly different effects depending on whether they are applied online or offline due to differences in technologies and practices. For instance, the long-standing offline rule in defamation law said that a publication would be held accountable to both the author and the person who was defamed. If this rule was applied to cyberspace without any modifications, the outcome would be that the host of an online resource, like a website or newsgroup, would be responsible for any defamatory content that it was unaware of and could not find without taking extraordinary measures. For an offline publication, which hardly ever publishes anything without first having editors or other publisher representatives evaluate it, the regulation has a completely different consequence.

An other method of applying the idea as a substantive guideline is to aim for a legal treatment of an activity that is functionally identical, regardless of whether it occurs online or offline. This strategy aims for equivalency of application, or the general equivalent burden of duties placed on the subject of the rules once the distinctions of the online from an offline versions of the activity have been taken into account.

The advantages of adopting policy of equivalence

The significance of laws in cyberspace can be increased by implementing an equivalency policy between offline and online legal systems. A regulation like this establishes norms around acceptable behavior for online actors. The standards that apply to them are the same as those that apply offline. The offline component of the legislator community has already acknowledged the significance of those norms. However, a policy of equivalence can only be successful in achieving this normative effect if there is a close match between the policy and reality. This does not, of course, mean that there must never be a difference between online and offline law. But those differences need to be kept as few as possible, and to be justified, if the policy is to have any meaning.

How easy it is to achieve equivalence depends very much on the way in which the law in question is framed. Laws which address the mental states of actors, or the outcomes of their behaviours, tend to require little adaptation to achieve equivalence. By contrast, laws which address the ways in

which behaviour is undertaken can pose difficult challenges for lawmakers, because the cyberspace technologies tend to incentivize actors to undertake those behaviours very differently.

Adopting a policy of equivalence also highlights unstated assumptions in the law, and these assumptions often prove not to hold when an activity is translated into cyberspace. It is usually impossible to achieve equivalence here unless the law is reformed on the basis of accurate assumptions.

State of mind of users and the consequences of activities

Many laws that govern routine human behavior do so by expressing their requirements in terms of the actor's mental state at the time of the activity. Because a user's state of mind will typically be similar whether behaving online or offline, these criteria can be applied to online actions with little to no modification. Criminal law regulations frequently characterize offenses in terms of the defendant's motive, and it has proven relatively easy to apply general purpose laws, such those prohibiting exploitation, to online players who are merely utilizing the internet as a new platform for illegal activity. However, there have been instances where the victim's mental state—rather than the defendant's—is a crucial component of the offense. There's a chance that identifying a human victim with the necessary mental state won't be feasible because computer and communications technology allow for automated decision made. This problem surfaced in the UK with regard to the fraud offense, which necessitated deceiving a victim. Initially, the Law Commission recommended comprehensive reform of the fraud law after determining that the piecemeal revision of specific charges was not a sufficient answer to the problem.
In order to address the issue, the UK Fraud Act of 2006 redefines the offense only in terms of the defendant's intention, creating a single regulation that is equally effective online and offline.[4]

Non-criminal rules are likewise influenced by mental states. One clear example is the establishment of contracts, which necessitates agreement between the parties. Legal systems that establish formal criteria for such agreements to be legally legitimate contracts have given birth to the main legal challenges in this field, regardless of the mode of communication used to make the agreement—online or offline. [5] The obligation under the Electronic Commerce Directive for firms to identify themselves and provide an offline address and contact details is an example of establishing

4 See also Council of Europe Convention on Cybercrime (2001, in force 2004), Art 8 for a similar approach.

5 See further Chris Reed, 'Electronic Commerce' in Chris Reed (ed), Computer Law, 7th edn (Oxford: Oxford University Press, 2010), Ch 4.2.2. 15 Directive 2000/31/EC on electronic commerce OJ L 178/1, 17 July

equivalency in respect of the effects of behavior.[6]This is just an extension of the long-standing offline principle—which can be observed in the UK Business Names Act 1985, s. 4—that dealers should be identifiable. The Distance Selling Directive lays out the requirements for identification of both offline and online vendors at the EU level. [7] To ensure that there is a standard minimum of information disclosure in cross-border trade, the Electronic Commerce Directive imposes extra responsibilities on online traders that essentially follow these offline standards.

The directive's provision might be extended to offline cross-border merchants in the event that reverse equivalency was required, without requiring any additional changes for offline communication.

In contrast to this in India, organizations may lawfully use a virtual office address as their official Registered Office address for incorporating purposes in accordance with India's Companies Act of 2013. According to Section 2(71) of the Act, the registered office is the location where the essential company records, registers, and documents are kept. An online office satisfies this legal obligation. Thus, virtual offices are completely legitimate and allowed to be used as proof of incorporation address for any kind of business, including limited liability partnerships, private limited companies, one-person businesses, and partnership firm registrations. This means that we need to ponder upon equivalency principle to bring online and offilne regulations in parity.

Technology and Conduct

On the other hand, it may be more challenging to achieve functional equivalency between the online and offline applications of legal norms when they focus on the actions of actors, regardless of their intentions or the results of those actions. Many examples of non-equivalent effects emerged in the early days of public internet use, when the courts were forced to apply the offline regulations that were in place at the time. Several instances of non-equivalent effects emerged in the early days of public internet use, when the courts were forced to apply the offline regulations that were in place at the time. This is typically because activities conducted offline and online differ so greatly that it can be nearly hard to evaluate how the rules are applied and what happens as a result on an equal footing. For instance, several jurisdictions have changed their laws regarding defamation to include new regulations that are only applicable online. By granting some immunity to an online host of defamatory content [8] or by redefining the term "publisher" to exclude specific kinds of online

6 Directive 2000/31/EC on electronic commerce OJ L 178/1, 17 July 2000, Art 5.
7Directive 97/7/EC on the protection of consumers in respect of distance contracts, OJ L 144/19, 4 June 1997, Art 4.

7 See eg Directive 2000/31/EC
8 See eg Directive 2000/31/EC on electronic commerce OJ L 178, 1, 17 July 2000, Art 14.

actors, these laws aim to ensure equivalency of application.[9] Nonetheless, the outcome might have been to favor online publication over offline in certain situations. It is far from obvious what treatment equivalency there might be between offline publication and internet hosting given their significant operational differences. Rather than the consequence of that behavior—reputational harm—defamation law concentrates on behavior—publishing. The difficulty in achieving equivalency stems from the concentration on publishing behavior, which in cyberspace may involve a significantly larger spectrum of actions than in the real world.

Conclusion

There is a dire need to reformulate the cyberspace law which are conducive to follow and implemented as well. The theory of equivalency provides us with an option where the legislature can attempt to successfully formulate the law of a critical and ubiquitous subject of cyberspace with a better perspective. Although the principle of equivalency prompts several challenges like difference of consequences. There is a substantial variation in the outcome based on whether an activity is online or offline. But even after being challenging the rule of quivalency can create greater acceptability among the subjects.

9See eg US Communications Decency Act 1996, 47 USC § 230.