Legal Issues in the Digital Age. 2021. Vol. 2, no. 4

*Research article*
UDC: 342
DOI: 10.17323/2713-2749.2021.4.70.97

# Understanding the Algorithm: Meaning, Socio-Legal Context and Concerns

**Nabil Ahmad Afifi**[1],
**Reeta Sony A.L.**[2]

[1, 2] Jawaharlal Nehru University, New Delhi, India

[1] nabil58_sse@jnu.ac.in

[2] reetasony@mail.jnu.ac.in

**Abstract**

At present, algorithms are becoming the heart of society by taking control over the decision-making process as societies are increasingly getting digitalised. There is a consistent theme that an unaccountable, black box technology has taken over the stage and is now making decisions for us, with us, and about us. But the contention around public participation in making decisions in science and technology needs to advance to a stage where there is a more direct conversation between the public and those developing the technologies. With the above mentioned conception of moderating emerging technologies' development, primarily digital technology due to its overreaching effects on humans and what humans interpret it to be. Firstly, the research through a literature survey is aimed to understand the meaning and nuances of the word *algorithm*. Then the analysis based on case study is focused on the algorithmic questions, such as bias, privacy, design, transparency, and accountability. In a larger context, concerns over jobs, ways of social interactions, etc., had been discussed, since these concerns are the result of the application of algorithms. The analysis of academic literature pointed out the vital facet of multiple understanding of the word *algorithm*. Further, the research also emphasizes the meaning of philosophy and politics in technology and its non-neutral nature.

**Keywords**

algorithms, technology, automated decision-making, algorithmic culture, bias, design

***For citation:*** Afibi N.A., Sony R. A. L. Understanding the Algorithm: Meaning, Socio-Legal Context and Concerns. *Legal Issues in the Digital Age.* 2021, vol. 2, no. 4, pp. 70–97. DOI: 10.17323/2713-2749.2021.4.70.97.

## Introduction

The modern world has made quite a shift in functioning, from socio-economic developments to working culture due to the dramatic and drastic digitalization of human life during the Covid-19 pandemic. The digitalisation efforts are changing the very nature of society its approaches to using technologies. Soft technologies[1] have taken centre stage, and algorithms, being the heart of technologies, have intertwined their logic into social interactions and experiences. Thus, it would be safe to say that the thin line of control about humans having agency over technology is diminishing fast. As the world is moving towards the Fifth Industrial Revolution, trying to incorporate a more balanced relationship between intelligent technologies and humans, we stand on the brink of a technological revolution that would shape the future of life, work, and relations. But the widespread propagation of algorithms epitomises a challenge for society and social sciences research.

The all-embracing use of search algorithms, social media, and other digital platforms for browsing, posting, promoting, and advertising has made the human experience more routine. In return, these cyclic activities generate relevant data on user engagement, retention, and research through comments, page views, search ranks, etc., for the corporations owning these technologies. The data collected is integrated on a scale unimaginable for both benefits and unintended consequences [Conger S. et al., 2013]. These practices also foster *cultural production* and *cultural contingent*[2] [Nieborg D.B., Poell T., 2018]. But when culture is numerically sorted, analysed and stored, it becomes crucial to understand that how are these decisions made and how laws and policies are laid out to map, scrutinise, and regulate them.

Law and policy-making are the guardians of digital space to save society from malicious intentions and various concerns that arise due to the usage of digital technology. The law and policy-making both depend on what the diagnosed problem is. To generalise, both law and policy function on stan-

[1] Soft technology should exhibit two main characteristics, i.e., it should be technological and also soft. The technological part includes a knowledge system of rules or procedures for the solution, bringing social or economic change. The Softness part should consist of an internal human conscious activity and affect our understanding of the world.

[2] Contingency in digital platform studies suggest two distinct but interrelated ideas.

dardising definitions of specific terms. This article explores the meaning of the term algorithm, moving beyond the computer science or mathematical description of the term towards social understanding and identifying concerns arising around them.

In order to explore the understanding of the term *algorithm*, authors of the article try to comprehend the meaning through the lens of algorithmic culture. This implies an extensive review of various articles, papers, and books on algorithmic culture and various themes revolving around it. The methods applied in these literature ranges from semantic understanding, etymological to anthropological approaches.

The concerns arising from the digital platforms and software are predominantly the intended or unintended consequence of coding social activities by computational instructions using algorithms. The emphasis in this article is to understand the role law and policy-making had played or could play rather than revolving around definitional and explanatory ideas of the notion of algorithm.

## 1. *Algorithm* in General Understanding

The study about algorithms is incomplete or, so to say, inaccurate without pondering upon the definition of algorithm. The common understanding of algorithms is more related to computer science and mathematics than having a robust conceptual ground in social sciences. The terminological evolution gives a glimpse of how the understanding of the idea of algorithm changes with(in) publics. Thus, the idea of an algorithm requires deliberation of its own.

The term *algorithm* has no uniform definition, so to begin with most conventional understanding about algorithms, R. Kowalski describes algorithms in the very specific sense of computer implementation as the summation of logic and control, where logic represents the understanding of a problem and control is about the strategies to solve that problem. The history of algorithms is embedded within the history of logic, i.e., instruction-based procedures for solving mathematical problems, but these are now applied to other areas of life. Algorithms are also referred to as the components of software that form the information and communication infrastructures. For such a conclusion, P. E. Ceruzzi [Ceruzzi P.E.,1998: 80) consider algorithms as "the set of instructions that direct a computer to do a specific task." Further, when algorithms are also denoted as instructions, A. Goffey [Goffey A., 2008: 17] states that algorithms "do things and

their syntax embodies a command structure to enable this to happen." The formality and technical undertone in these definitions impede the understanding of algorithms in different publics, and the sense of an informed understanding of the algorithm is lost. Although, the government and industry are trying to create standards for various algorithmic actions which have to be based on the uniformed definition. Lum and Chowdhury argue for this same reason that the description of an algorithm should be based on their impact [Lum R., Chowdshury K., 2021]. They argue that by focusing on the output, avoiding the technical complexities of the input aspect of the algorithm. This argument offers us the opportunity to focus on the themes that affect us, regardless of whether it is an algebraic formula or artificial intelligence. This line of argument has allowed us to dive deeper and scrutinise the idea of an algorithm with respect to the culture they exhibit.

Although in 2019, Algorithmic Accountability Act (HR2231) was introduced in the U.S, which tried to standardise the meaning of algorithm using the term "automated decision-making system" and defining it as "a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that makes a decision or facilitates human decision making, that impacts consumers" (Text — H.R.2231 — 116th Congress (2019–2020): Algorithmic Accountability Act of 2019, 2019). It is imperative that laws and legal rules would come up for algorithms on various accounts in the future. So, for the precedential nature of law and holistic policy-making, understanding the term and how the public associate with it is essential. Though HR2231 includes a broad definition of the algorithm, it avoids major perplexities like the distinction between high and low-risk automated decision making, the non-linear nature of software development, and only considering large technological companies.

## 2. Multiplicity in Meaning

Societies in the wake of the pandemic have swiftly digitalised platforms for most of the human activity. People are experiencing algorithms such as ranking, profiling, tracking, recommending, filtering. The algorithms work through both human subjects and objects shaping behaviour, way of thinking, preferences, and tendencies. These algorithm functions are made possible by their features like autonomy, decision-making power, and value-laden nature. Thus, algorithms have logic and control and help in subjective and more complex notions, i.e are able to decide what is essential and what is not [Tufekci Z. et al., 2015]. Striphas describes these phenomena with regards to digital processes as *Algorithmic Culture* [Striphas T., 2015].

Pierre Lévy, the French sociologist and philosopher, is one of the most important thinkers in the field of virtual culture. His enthusiasm focuses on the cognitive and anthropological dimensions of the Internet. Lévy defined cyberculture as a set of substance and intellectual theories like practices, attitudes, and values that emerged along with cyberspace. He defends this idea by arguing that cyberspace was a product of real social movement, as the personal computer was created by people who wanted to develop new information bases to revolutionise societies [Levy P., 2001]. Thus, along with the personal computers came digital networks, which coincided with aspirations of cultural streams and echoed with the development in communications and intelligence. Lévy has highlighted four functions: production of data through software or audio-visual devices; cleaning of data, sounds, and images; transmission by using digital networks; storage of data [Teixeira A.S. et al., 2017]. The functions are even valid for the current digital platforms. According to him the digital models are not to be read but to be interacted with, as the knowledge in this system is produced by simulation. The manipulation of parameters and simulation of all circumstances by the software gives the user a feel of a cause-and-effect relationship. Lévy's characterisation of cyberculture can be seen true as the society is facing new complexities caused by change in thinking provoked by intellectual capacities of cyberspace. The question that arises from his work is that are we structured enough to face the complexities of cyberspace. Further, his arguments lead us to the debate of technological determinism and the social dimension of technology which are part of the science and technology studies.

Tarleton Gillespie [Gillespie T., 2016] brings an exciting perspective to the algorithm debate; he is more concerned with semantics. He implies that the word algorithm could mean different for different publics. For software engineers, algorithms are simple procedures, but they are something unattainably complex for the broader audience. With this argument, he describes algorithms as a Trick, Synecdoche, Talisman, and Committed to Procedure.

Gillespie elaborates that algorithm is merely the procedure that addresses a task as operationalized for algorithm to be a trick. Additionally, to improve an algorithm is rarely about redesigning it rather it is about tuning the parameters and limits. To explain algorithms as synecdoche, Gillespie borrows from Goffey that algorithms' actions are part of an ill-defined network. It is this ill-defined network that we refer to when using the word algorithm. Further, algorithmic systems are not standalone, they are massively networked, and users tune and tweak them; thus, we need to examine the logic which guides these people [Seaver N., 2013]. In this sense, Gillespie

says that qualifying sociotechnical assemblage an algorithm allows to avoid the need to understand different elements like models, cleaning, sorting etc.

The technology industry quite often does the invocation of the term algorithm for the wide public. Calling a process or service an algorithm is associating it with the idea of being logical, mathematical, independent. That is making it the pinnacle of objectivity. Thus, the results provided by algorithms wear complete legitimacy, so the notion of algorithm acts as a talisman.

Subsequently, as Gillespie claims, the word "algorithm" is lately being used as an adjective rather than as a noun. The terms like "algorithmic identity", "algorithmic regulation", "algorithmic power", "algorithmic ideology", or "algorithmic culture" highlights this social phenomenon. These ideas include algorithms and the networks in which they function, the people designing them, data, and users. Through this, he deduces the invocation of the term algorithmic is not an algorithm per se. Still, it is about the insertion of the procedure in the knowledge system and mainly social experience. Further, Gillespie points out that, "we rarely get to watch algorithms work; but picture watching complex traffic patterns from a high vantage point: this algorithmic system privileges the imposition of procedure, and— to even participate in such a complex social interaction— users must in many ways accept it as a kind of provisional tyranny."

These notions about algorithms make it clear that there is sense of friction between human sociality and procedural systemisation. But algorithms are at the centre of the network technologies we are surrounded by, and human life is increasingly dependent on them.

Through historical analysis, Ted Striphas has tried to trace the conceptual understanding of the emergence of algorithmic culture by focusing on the words that substantially affected the culture. He claims that the cultural work has been passed on to the digital technologies using computers and databases, which has rearranged some of the words closely associated with culture. Striphas, like Gillespie , focuses on the semantic dimensions of algorithmic culture, and both derive their inspiration from Raymond Williams' book "Keywords" (1983). According to Williams, the term "culture" previously has been a relatively vague word, but since the beginning of the 20th century it has become one of the most complicated and multifaceted notions. To conceptualise this understanding he traced semantic shifts among certain terms which formed the basis for his book.

Striphas , for his case, identified three words: "Information", "Crowd', and "Algorithm". Using etymological analysis, he has tried to map the threshold of the meaning of these selected words. However, he sketches the

history of the word information from the 12th century to modern times. To summarise his effort, cultural life is becoming a type of information processing task among many other affairs. Further, he believes "humans no longer hold exclusive rights as cultural producers, curators, or interpreters, which has been passed to the digital technologies" [Striphas T., 2015]. This brings the question of uniformity between humans and technologies as to what would happen if the cultural practices and decision-making arguments were not well-informed.

Similarly, for the word "*crowd*", Striphas founds parallels with *community* or common culture, as proposed by Williams, the word relates to the denial of individuality or full participation, and this has its shadow over the words like *crowdsourcing*, *collective intelligence*. Williams affirms that solidarity is an essential element for the sustenance of common culture, but what he could not predict was the computational nature of solidarity that exists today.

Striphas identified that the word *algorithm* comes from the word *augrim* or its more conventional version *algorism* following orthographic transformations. But he emphasises that the semantic perspective of the word *algorism* includes secondary meaning that is key to the manifestation of the algorithmic culture. He further moves on to the papers by Ralph Hartley and Claude Elwood Shannon, both of whom worked at Bell Laboratories in the United States. Hartley was more focused on the process of communication, but Shannon was more concentrated on the signal and noise as he believed communication is something to be engineered rather than letting uncertainty seep in. Consequently, Shannon believed in devising an arrangement of procedures or algorithms that could cascade with the governing process of communications. This, Striphas believes, is among the first algorithmic theories of information.

Paul Dourish initiates the discussion on digital culture by contemplating the work of Niklaus Wirth [Wirth N., 1975], who advocated a structured approach to programming in the area of design and software engineering. Wirth's approach was to dissect problems into smaller bits and then follow a structured approach to solve them. Such an approach helped in the easy development of computer programs and their analysis. Wirth also focused on the importance of the relationship between data structures and algorithms. Skipping the technical differences between program and algorithm, Dourish concludes that it is essential for us to understand algorithms in connection with computational procedures such as data structures. Dourish further concludes that "the limits of the term algorithm are determined by social engagements rather than by technological or material constraints." He argues

that the boundaries of the term algorithm are the social boundaries, i.e., between technical people and non-technical people, who may not understand the explanations in play. This conceptualisation of algorithms by Dourish uses a different approach from the previous inquires on algorithms carried out by Striphas (2015) and Gillespie (2014, 2016).

Nick Seaver's [Seaver N., 2017] approach to algorithms is in response to the most usual definition of the term *algorithm* in computer science. Seaver builds on the work of [Devendorf L., Goodman E., 2015], who opted for a new approach towards algorithms by arguing that algorithms are multiple systems otherwise assumed as singular and material accumulations rather than protracted texts which opened new entry points for critical practices in design and engineering. Another interesting inclusion in the study by Seaver was developed in the works of Annemarie Mol [Mol A., 2002].

Mol's work is an ethnographic study of atherosclerosis; instead of restricting the topic to theoretical definitions, she investigated how atherosclerosis problem is being understood in practice in a Dutch hospital. Her STS analysis is a rich multi-layered text with an undertone of anthropology but also with contemplation on the multiplicity of reality in practice [Jensen T.E., 2005]. Thus culture, in reference to Mol's work, as Seaver writes, is "not one coherent thing, nor is it a set of disparate things, such that every person enacts and imagines their own in isolation."

Seaver also elaborates on the terminological anxiety of word "algorithm"; for him, a terminological definition is about drawing the boundaries for the disciplinary authority of critical algorithm studies. But rather than offering the concrete definition, Seaver tries to look into an anthropological approach because anthropology for him is a valuable tool for thinking through the engagements between incongruent knowledge traditions. The ethnographic approach to algorithms essentially helps critical scholars in understating the formalist approach to the culture.

While deliberating about algorithms in culture, Seaver elaborates on the work of Dourish, where he hinges his arguments on the definition as a set boundary. Seaver argues from the merit of his ethnographical work that the term algorithm's meaning evolved even between two technical people. What he finds interesting is that scholars could say for an emic definition of the word algorithm, but we cannot know these definitions in advance. He also points out that technical people are not the only crowd responsible for generating the algorithms; thus, a very diverse group of people with varied skillsets produce algorithms. Seaver essentially feels that a more precise definition is mainly used to isolate the concerns of algorithms from the

social sciences or critics of algorithms. His understanding of a proponent of facial recognition and a critic of recommender system is situated in the fact that both rely on the deductive distinction between culture and technical people. This is what he refers as the *algorithm in culture* i.e., the notion about algorithms centres around the belief that they are discrete objects and could be located in the cultural context. Algorithms themselves are not culture, they could shape culture or might be shaped by it, but they are two different things.

The scepticism in term "culture" as a concept of study has been a common place among anthropologists. The problem began from homogenising the political nature of essential tendencies of culture, and the speed of life changing [Abu-Lughod L., 1991]. The concept of culture has evolved from the traditional domain and has found its dominance in ethno-nationalism, business establishments, etc. While a social scientist could criticise the people's use of culture, these users are usually the influential part of the culture. Bourdieu takes the practice approach towards culture, where he points out that many anthropologists view culture as an order of practice as part to form a cultural life [Burris B., 1980]. But rather than the setting of practice, culture might be something people perform. Thus, Seaver is more interested in the multiples of culture, i.e., culture not as a unified means instead of loosely collaborative practices that sometimes compete or interact. He takes supports Mol's ethnographic work and case studies by Laura Devendorf and Elizabeth Goodman for this conclusion. To understand this as an argument for algorithms, different actors shape algorithms in different ways, technical people try to mediate by coding, and some non-technical people see it as magic. But, as Seaver writes, "no inner truth of the algorithm determined these interactions, and non-technical outsiders changed the algorithm's function: machine learning systems changed in response to user activity, and engineers accommodated user proclivities in their code" [Seaver N., 2017].

The above-discussed literature on the conceptualisation of algorithms in culture and culture in algorithms presents an opportunity to explore the concept of the term *algorithm* within society and how society shapes the notions on algorithms. The significant gap that exists is the lack of empiricism in the methodology to understand the algorithmic culture.

## 3. Ideating Algorithm through Concerns

With no set boundaries pertaining to the definitional clarity on the term *algorithm*, algorithmic concerns help define the scope of the algorithm. But, as the advancements in information technology are seeping into our

lives more than ever, we can now create more customised services and outsource specific routine tasks such as shopping, vacuuming floors, education, etc. Still, everything has a potential cost attached to it. In a larger context, concerns over jobs, ways of social interactions, virtual reality, etc., had been discussed, though algorithmic concerns are the result of the application of algorithms. But algorithmic concerns evolve in due process of the application. So, to ask, are we designing algorithms, or are algorithms designing us?

The heterogeneity in algorithmic concerns raises the argument about the understanding of algorithms; thus, the more we inquire, the more accurately we can understand their essence. Therefore, without deep-diving into the literature on each concern, the strategy is to focus on the case studies to understand how law and policy-making build its perception around the term *algorithm* through various cases.

M. Kranzberg (1986) writes: "Technology is neither good nor evil; nor is it neutral" as his first law of technology. Even though algorithms to the general publics are "mysterious and inscrutable machinations of big data, big government, and big business increasingly part of the infrastructure of the modern world, but hardly a source of practical wisdom or guidance for human affairs" [Christian B., Griffiths T., 2016] or is becoming a guiding force. Still, people fail to recognise or are ignorant of its effect. In the current phase, algorithms interact with humans in the form of technology, and the fact that it has become a part of our life makes it scrutable. To scrutiny is to raise the concern over the black-box nature of algorithms. Another point that raises concerns is when making an informed decision, the very act of informing jeopardises the outcome.

Against the claims of what algorithms can do, they deserve some scrutiny, but it is essential to know what to scrutinise before that. We have tried to highlight specific concerns about algorithms.

### A. Bias

One of the standard and important concerns about algorithms is bias. The explosion in the widespread use of algorithms has introduced biases created by algorithms at the forefront of technology, academia, and media. Even policy-neutral algorithms had, in some cases, imitated historical inequalities and societal prejudices [Tene O., 2017]. *Bias* as a word that primarily implies a negative connotation, i.e., it has to be avoided or is problematic. Instead, in this article, we would take a more neutral approach for the term *bias*; as Danks and London explain, the term is about deviating

from a standard. To elaborate, a moral bias would conclude to a deviation from a moral norm or, in any case, social bias, regulatory bias, etc. To synthesis, the point is that something can be biased based on one view but not by another view. Although bias can exist in various forms, which can also be subdivided, not all forms are on par with each other. A section of academia believes that these value-laden arguments cannot be solved just by technology [Danks D., London A., 2017]. Some might be more problematic, and others might be a result of an ethically desired system. There are numerous examples of algorithmic bias, but some have caught the headlines like the racially bias algorithm in Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) used in the United States to provide sentencing advice, Google's advertising algorithm, which appeared to be gender-biased by showing higher-paying jobs to men than women, etc. [Koene A., 2017].

It is important to deliberate on the case of the COMPAS algorithm to understand why there is a need to scrutinise the algorithm and how is the system is biased. This is about the epistemic agency[3], as [Rubel A. et al., 2018] write. To have a convincing level of agency, a person needs to know where they stand even though they might or might not have the power to take action. The basis for this argument is that people are reasonable beings who are also part of a community. So, people and institutions related to us exercise power over us, matter for us. Thus, denying someone the ability to understand the reason for the action taken against them is a failure to respect them as an agent. In a similar context, one can find superficial information about the algorithm used in COMPAS, but getting access to the algorithm is impossible. This implies people lack access, and without access, they cannot improve their understanding of how they are being treated by COMPAS. But the argument is two-fold; that is, in the case of both the COMPAS and the judge, the root cause of the problem is the inscrutable process. For COMPAS, it is the algorithm, and in the case of a judge, it is his mindset. The argument begins with the effect of the agency. Judge psychology could be as obscure as the algorithm of COMPAS; thus, the purpose of understanding the reason would fail. But there is a difference between human and algorithm in making the decision. The former one is culpable, but the latter cannot be made morally responsible. That being said, as Rubel et al. concurred algorithms are not agents.

To sum up the argument, if the algorithm of COMPAS gets it wrong, the moral responsibility lies with the person or the group responsible for

[3] Epistemic Agency can be explained as learning efforts taken by oneself and the advancement in understanding.

developing and designing that algorithm. It is important to consider European Union's General Data Protection Regulation (GDPR), which came into effect in 2018, stating "a data subject has the right to an explanation of the decision reached after (algorithmic) assessment." However, the extent of the right to an explanation depends on the court, and its interpretation is yet to be seen [Voigt P., von dem Bussche A., 2017].

The biases in algorithms seep into our lives through its most common implementation, i.e., computer systems and the internet. There have been numerous accounts where the software or the internet has shown to contain biases that both unjustly and systematically discriminate or favour certain individuals or groups. As [Bozdag E., (2013] points out about the current trend of personalised algorithms, though it had existed since the 1990s but are now part of a much-blown idea of algorithmic filtering due to the availability of cheap and efficient infrastructure and also due to the increased popularity of social networks and search engines. To increase relevancy, it utilises interpersonal information about the users and tailors that information according to the need. This is where the biases percolate and have severe implications on human values, transparency, trust, privacy, etc. [Granka L.A., 2010] also points that information diversity is a relevant function of bias, which implies, for example, if a social media platform exercises a bias with respect to an advertiser, then it would be limiting the diversity and democracy integral to information. Even the IEEE project on Algorithmic Bias Consideration is primarily about providing a clear picture to the organisations dealing with algorithms on how algorithms are assessing, targeting, and influencing users.

### B. Privacy

Amongst all the development in information and communication technology an extremely prominent issue is privacy. With the ever-increasing use of social media, search engines, and the power of algorithms to influence people's choices, people themselves grant their privacy with their own hands to the government or the private organisations, and then things like the Cambridge Analytica scandal wakes them up. These recent examples, have made clear the crucial importance of privacy. This brings another question, that who can make the decision about the privacy of others, and how these decisions can be made [Goldberg L. et al., 2001].

Privacy, as in law and ethics, is a blanket term and, in a loose sense, means "having control over the information about oneself" [DeCew J.W., 1986]. It is critical to this analysis that we discuss the concept of privacy in a

more elaborative sense to make the argument more visible and exhaustive. To begin with the definition of privacy, [Parent W.A., 1983] defines privacy as "the condition of not having undocumented personal information (knowledge) about oneself known (possessed) by others." The definition by Parent is motivated by the fact that it should be easy to understand and should not cross over to the boundary of other related concepts. He goes on to defend the point that his definition is more about the moral value of protection of someone's freedom and individuality against a gratuitous invasion.

Additionally, it is essential to understand what information is considered personal. Firstly, it includes facts that people do not want or choose to reveal to society (except family and friends) or information about which an individual is sensitive even though similar information about other people may be widely known . Parent not only sees privacy as a coherent concept but also believes there is a degree of uniqueness and fundamental value attached to it. In contrast to Parent's view about privacy, [Thomson J.J., 1975] argues that the right to privacy is derived from other rights, mainly property rights. Her approach is considered reductionist, as according to her, there is no such thing as the right to privacy, and for any violation of the right to privacy some other non-identical right is violated. What strengthens the Parent's claim is the reverse reductionism of Judith's idea about the right to privacy [Fried C., 1984] broadened the previous approach and defined privacy as not only the absence of information about us in the mind of others, but it is about the control of information about us. The idea of privacy is also based on trust, i.e., other people would display integrity, reliability, justice, and other ethical behaviour.

Further, the European Union's General Data Protection Regulation (GDPR) has connected the right to privacy with human dignity. As Article 88 of GDPR points out, rules would include appropriate and explicit measures to protect the data subject's *human dignity* by taking into account the due process and transparency. However, human dignity does not come up in GDPR but is fundamental to its core and is an important consideration when interpreting privacy ('European Parliament and Council of European Union (2016) Regulation (E.U.) 2016/679,' 2016). [Floridi L., 2016] elaborates that in post-modern philosophy, lack of privacy could arise due to the fact that mutual recognition encourages it. Thus, explaining the circumstance of why we care so less about what we share online. Floridi goes further to make a point that the philosophy of information assumes human nature in the form of an informational pattern and argues that under this consideration, a breach in privacy has an ontological influence.

In the digital world, the algorithms employed by search engines and platforms track and cater to individual behaviour to provide recommendations. Still, this data is not necessarily created by them solely but still end up on internet as a result of public, government, and other databases. This makes internet footprints of the individual without any online accounts. In that sense, an important idea which European Union's GDPR has embraced under Art. 17(2) make the concept of privacy more robust with the concept of the Right to be Forgotten[4]. The inception of this right can be traced back to the judgment of the Court of Justice of the European Union, where the court ordered Google to remove debt recovery details of a Spanish citizen (Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, 2014). Following the precedence set by the Google ruling, countries like France have both civil and criminal counts on privacy.

In context of India, the judgment by the Supreme Court of India in Justice K. S. Puttaswamy (Retd.) and Anr. Vs. Union of India and Ors., which was about the constitutional validity of Aadhaar an Indian biometric scheme, was instrumental in shaping the notion of privacy in India. The judgment endorsed the right to privacy as a fundamental right; the one-page order read, "The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution" (Panday, 2017). The judgment acknowledged that privacy is an aspect of human dignity and also advocated for the creation of a legal framework around the privacy concern (Puttaswamy v. India, 2017). With the above conception of privacy in the Indian context, the right to be forgotten has found its place in Personal Data Protection Bill, 2019, which had been missing from the Information Technology Act 2000. But the balancing test it faces is yet to be seen.

There is a belief that when algorithms compute *correct possibilities,* they are exempted from being considered harmful to privacy and many other things since they produce exact output for the given input. But, when it comes to subjective decision making, which does not have a correct answer, this may involve relying on algorithmic operations applying a large number of metrics and different things. Tufekci believes this is where the argument about privacy begins. An example of this is how the popular mobile game *Pokémon Go* required access for the entire *Google* account on *iOS*, including emails, browsing history. Similarly, *Uber,* in one of its updates, collected

[4] The right to be forgotten gives the right to the individuals to correct, restrict, delink or delete their personal information on the internet platform.

user location even when people were not using the application on their mobile [Hayes D. et al., 2017].

It is important to separate the idea of violation of privacy through algorithms and social media through an interconnected area, as algorithmic concern is a far more significant problem than privacy invasion.

Today, every website people visit and every software they use flashes, "your privacy is important to us." Still, users evaluate this on varying factors like the investment in privacy, type of information collected, and its use, but recent cases have displayed the above pretence being not so robust. Some scholars consider that with technology evolving, the loss of privacy is inevitable. PEW Research published a report Digital Life in 2025 in 2014, which revealed that "everyone will expect to be tracked and monitored, since the advantages, in terms of convenience, safety, and services, will be so great that continuous monitoring will be the norm" [Anderson J., Rainie L., 2014].

### C. Design

With the increase in the scope of algorithms, the future application of algorithms is becoming ambiguous. This makes it more difficult to predict the future use, thus posing the question that was the design ethical enough to cope with the future scope? Every technology which finds its way to society will arbitrate human experience, action and, in the end, helps in forming moral decisions [Verbeek P.P., 2008]. [Freidman B., Kahn H. (2002] put a very interesting argument in the sense of design and ethics. Their reasoning is based on the view that in computer science and technology literature, the word *trust* is frequently used as synonymous with *security*, even though these two terms mean different in ethics. They go further by detailing out that there two ways of design can help in making online interaction safe. One way is to move towards solutions like passwords, encryption, locks, etc. The other idea is to understand how a trust-based relationship can be fostered and created, therefore designing systems around them.

There is a point of view that technology influences humanity also by the function of its design, in the context it is used, and the people are involved. The process of design, implementation, and adoption of technologies is complex, and within it, algorithmic concerns have very little influence on the designing process. A significant portion of the ethical design in algorithms is related to dataset, as biases in the dataset can be mitigated to the designing process [Brauneis R., 2017]. This can be elaborated with an

example of biases in Amazon.com Inc's recruiting engine, which was later shut down. Since 2014 Amazon was utilising an artificial intelligence tool to sort resumes [Kearns M., Roth A., 2020]. But in 2015, they realised the system was not gender-neutral. It rated male resumes higher than female, even though Amazon edited the program in particular terms to make it more gender-neutral but the system taught itself to find ways to search gender by using terms such as all women college, women's club, etc.; finally, the program was abandoned. The cause of this problem was the model, which was used to train the program, that consisted of previous ten-year resumes which were mostly of men; thus, the machine realises that women are not preferred. The root cause, in this case, was not some apparent negligence on the part of the development team. The resulting algorithmic bias was the unanticipated outcome of abiding by the standard procedure of machine learning. Thus, beginning from the specified objectives mostly for efficiency or accuracy or both and algorithmically exploring the model that maximised it by using a large amount of data. In turn, revealing the design flaw of the solution proposed by the designer.

The idea of design ethics also goes beyond just the inherent value of the work itself; it should also align with the values of designers and industry. In this networked society, data-driven designing of algorithms is proposed for good but often has ulterior motives. There are ways to address these issues by utilising frameworks such as *human in the loop*[5] and *society in the loop*[6]. Conversely, we lack the comprehensive practicality to transform values, organisational, and societal realities into the process of algorithm designing. [Martin K., 2019] believes that algorithms are embedded with morally important decisions taken by firms and individuals, which have specific implications on accountability, and design decisions can amplify the role of algorithms. Abelson and Sussman's phrase "programs must be written for people to read, and only incidentally for machines to execute" captures the essence of design in algorithms.

Recently, as our understanding of technological innovation, competitiveness, or in the case of creativity have increased, there is a growing sense that a design-thinking perspective must be induced in it. On a similar notion, we have privacy by design. Privacy must be incorporated into organisation values, objectives, design processes, and planning rather than introducing it at the end of the process. [Campisi P., 2013: 364] defines the

[5] Human have monitoring and supervisory control at the important junctions in the system.

[6] Society in the loop in short is human in the loop in addition with social contract.

principle of privacy by design as "privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use, and ultimate disposal." Privacy by design is more about preventing breaches from occurring than just providing a solution for settling them. According to Article 25 in GDPR, companies involved in processing personal data should device fitting measures and defences which observe the privacy principle and such should be built into the system by default (European Parliament and Council of European Union (2016) Regulation (E.U.) 2016/679, 2016). Even though GDPR has a detailed description of privacy by design, it is still not clear about the obligation to ensure it and the technical specification part. As Christl, Kopp, and Riechert wrote: "Systems that make decisions about people based on their data produce substantial adverse effects that can massively limit their choices, opportunities, and life chances."

### D. Transparency

A common phrase for reference to algorithms is black-box, used to define its opaque nature. Transparency acts as a tool for ethical development and tries to make use of algorithms in such a manner that they promote human rights and aid society (European Parliamentary Research Service, 2019). The opacity around algorithms can be highly complex due to the involvement of machine learning, which is not only dependent on design choices but also on the data it is trained. The value proposition of transparency is not about being a tool but about the purpose it serves. Looking at the recent attention on transparency as a mode of algorithmic accountability, it is important to consider what transparency brings to the table or how it has functioned historically and technically.

To begin the discussion about transparency, firstly, we need to understand the idea of opacity in algorithmic applications. As [Burrell J., 2016] writes, opacity can be of various forms, beginning with the secret kept by state or corporate as a strategy of self-protection or coping with the competition. Search engine optimisation is a classic example where big corporations do not reveal their algorithms for ranking, filtering, and recommending searches. But the open-source movement has tried to change this notion. [Diakopoulos N., 2015] believes that making code available for review under certain regulations can also be a way forward. Secondly, opacity also occurs since coding and designing algorithms is a specialised skill both in terms of reading and writing, which makes it unapproachable for the ordinary population. As [Mateas M., Montfort N., 2005] have concluded,

codes that are written in a holistic manner perform *double-duty*, that is, to say that it can be interpreted by the programmer and someone maintaining the code and as well as by the machine utilising it. Then, within this arises issues like diversity and mass dissemination of the algorithm for common use. Lastly, Burrell argues about the scale of scrutiny of algorithms which poses an opacity dilemma even when we decide to audit these algorithms. The argument is not per se about the inability to scrutinise but about the point that specific algorithms, for example, in machine learning, are so extensive, interlinked and require large datasets to test. Even then, every dataset cannot be tested, thus being opaque.

After an inquiry about the opacity in algorithmic operations, it is important to understand the aim of transparency or, in that case, what transparency is and why do we need it, and from whom. Turilli , Floridi (2009) argue that transparency is not inherently an ethical condition, but it enables the conditions fostering it. Secondly, they point out that transparency has at least two different connotations, which are usually used similarly but are deceptive. For business ethics, information ethics, and information management, transparency is about the visibility of information, which can be increased by removing obstacles. However, in the case of disciplines like computer science, transparency is about information invisibility.

Historically summarising, transparency is not a result where everything is clear and evident, but it creates a system of perceiving and knowing that maintains a form of control [Phillips J.W., 2011]. The idea of transparency leads us to be accountable, but if transparency has no meaningful effect, it can lose its purpose. The meaning of transparency also depends on the use and type of algorithmic operations, i.e., which aspect of algorithms like codes, logic, goals, variables, etc. Thus, algorithmic transparency is about seeking insight into the system's behaviour about any input, trying to get an explanation for the output.

Accountability is a consequence of transparency; hence, we cannot hold anyone accountable if we do not know what and where things are wrong. So, it is important to understand the areas where transparency is demanded. Transparency in the algorithmic system can range from transparency in data, goal, outcomes, influence, compliance and usage (European Parliamentary Research Service, 2019). In the argument about transparency, it is essential to understand who gets to view what. The potential viewer might be everyone, certain parts made available for the public, researchers, accreditation agencies, third-party experts, etc.

To concretise our arguments about transparency, it is important to put it in with relevant cases. Many financial services use all sorts of algorithms to process loans that are not transparent in their function, as people might know the reason behind their loan rejection. Another example is the Yelp review filtering algorithm, which created dissatisfaction among users for being opaque and manipulating businesses to pay for advertising in return for the higher rating. Yelp not only hides the way its review filter works but even hides its existence altogether [Eslami M. et al., 2019]. Even the idea of transparency is not infallible, merely seeing what is inside the system does not provide any understanding of its comportment [Ananny M., Crawford K., 2018].

### E. Liability

The majority of our interaction with the algorithm takes a form of product or services, but as the birth of commercialisation of products could be attributed to technological advancements and globalisation of human efforts, this has also created a problem of lack of liability, which is more than true for algorithmic systems. There are numerous examples in which it would be difficult to attribute liability, like in the case of Samathur Li Kin-Kan, who filed a suit against the salesman who convinced him to put a large piece of his wealth for stock trading with the help of a supercomputer (K1) [Elish M.C., 2016]. Today, most software, website, program, etc., are built from preconstructed algorithms, which act as a base for them. It is also essential to differentiate between the term's accountability and liability as both are used as synonyms most of the time. Nissenbaum (1996) wrote that difference between accountability and liability is mainly a legal one. Liability is *evaluated* on the victim's plight, whereas accountability is about the relationship of the agent to the outcome. To sum this, liability tends to bind more largely than accountability. It is more about the actor than the action, though their efforts might contain the liability [Haines N., 1955].

Giving algorithmic subjects the right to understand the logic behind the cryptic system is seen as the first step towards an intelligible society [Hildebrandt M., 2014]; [Pasquale F., 2013]. Even GDPR includes clauses for an individual's right to demand a description for *logic* behind the automated operations made for them, thus enabling the public to examine and challenge these opaque systems.

Liability for the system can include hardware and software. Though hardware liability would be easy to define, the software liability is difficult to put on. The producer of the algorithm could theoretically be held

responsible for the defects, but this rarely occurs in practice [Tjong Tjin Tai E., 2018a]. The contractual liability is limited by the disclaimer of warranties, and product liability ceases to exist due to the intangible nature of the software (algorithms). M.C. Elish argues that the discrepancies between liability and control when control is shared by many actors (human and algorithms) and its implications for legal regulations and liability. She developed the term moral crumple zone to identify the ambiguous nature of "distributed control, automated and autonomous systems[7]". It is similar to the crumple zone in a car, designed for the purpose of absorbing the force of the crash; similarly, the human takes all the wrath of the moral and legal obligations when a system ill performs. This emphasises the structural feature of the system, which might take undue advantage of human operators. Liability is more part of a governance issue in algorithmic decision making, but this research would not try to explore the governance field.

When viewing the liability aspect, it is imperative to scrutinise the legal personality of algorithms: anything or anyone the law recognises as a legal actor is considered a legal entity. Thus, legal entities can enter in a contract, can be sued, and can sue. [LoPucki L., 2018] suggests that an entity can be recognised as algorithmic if it is controlled by an algorithm. The creators of algorithms have not discarded the idea of them being a controller with the condition that users do not modify the algorithms in use. Although the algorithm has no rights of its own, Bayern et al. (2016) point out that by preparing algorithms as a legal entity, it can be given the power to exert the rights of an entity. Thus, the concerting idea of the personhood of the algorithms. But presently, algorithms are not recognised under any legal entity. The algorithm as the software is protected under the Copyright Act, 1957, in India [Nayak S., 2013].

Data and algorithms are inherently connected to each other. Thus, data need algorithms to be meaningful, and algorithms without data are just a dead horse in this knowledge-based society. With an understanding of how this combination affects society at large, the need for liability arises. Algorithms, in some instances, require databases either to train or to develop the algorithms for them to function. These databases, in India, are protected under Information Technology Act, 2000; Indian Penal Code, 1860 and supplemented by Copyright Act, 1957 and Indian Contract Act, 1872 to tighten further the grip on data mishandling [Shabana N., 2015]. However, these laws per se do not consider the liability of any mishappening resulting from the algorithms themselves.

[7] Related to computational technologies.

The increasing autonomy of the algorithmic systems also acts as an impediment to holding humans liable, but this autonomy is a function of scale [Karnow C.E.A., 1996]. Certain systems work only on their own for small tasks like trading algorithms, which also requires permission when boundaries are reached. In contrast, a computer virus runs without any possible intervention or communication from its makers at times. Even though autonomy is a relative concept and can be interrupted by an outside force, with such references to autonomy [Bertolini A., 2013]; [Beard J. , 2014] has argued that human judgment may be required for such systems and the matter of law, such systems should always be under human control. This leads us to the arena of who should be liable and under what grounds. It is crucial to determine what gives rise to the liability, that is to say, under what circumstances someone or something become liable for their action. The possibilities can range from taking inadequate deterrents while creating or designing the algorithmic system, i.e., dropping the risks on the users, which could have been averted.

Further, this also includes paying insufficient attention when owning or using a system like not floating updates for the system. Lastly, there can also be a risk-based liability, i.e., there is a possibility that any autonomous algorithmic system can produce a detrimental outcome. The only way to avoid such an outcome is not to make such systems, which is not an option [Tjong Tjin Tai E., 2018b].

Under the circumstances such as the above provides the ground for liability, thus it important to investigate the fact that who liable. In most specific cases, liability rests on the person in a spot to avert the harm; to rephrase, the person in control of the environment or system. Many a time, various people occupy such positions, but certain positions stand out in terms of liability, as Tjong Tjin Tai mentions, firstly, the producer of the algorithmic systems. The producer can be the designer or creator of the system, thus reducing the risk. Secondly, the owner of such systems has the control to alter and restrict the system. More than often, the owner is deemed liable as it is easy to identify the owner. Lastly, the operator of the system, as this is the position that has the power to control and direct the system, thus can prevent the damage. The position of liability cannot be restricted to these positions as the algorithmic systems are increasing their exposure.

To understand the complexity of liability, let's take the case of the Tesla autopilot car crash. In March 2018, an Apple employee died after his Tesla car crashed into a concrete barrier in Silicon Valley [Rushe D., 2020]. The

US. National Transportation Safety Board (NTSB) investigation found that the car was in autopilot mode (semi-autonomous) using Tesla Autopilot algorithms. The driver was found liable since he was playing a video game while driving in semi-autonomous mode. Even though Tesla instructs drivers to keep hands on the driving wheel while in autopilot mode. But the NTSB report further implied that the Tesla autopilot system did not provide the "effective means of monitoring the driver's engagement." NTSB chairman said, "If you own a car with partial automation, you do not own a self-driving car. So, don't pretend that you do" (NTSB, n.d.). The critics also pointed out that Autopilot branding gives drivers an illusion that cars can drive themselves fully autonomously. It is visible that liability is not easy to exercise when power dynamics come into play. Still, as the case is in court (Siddiqui, 2019), its ruling will help us to improve our rationale on liability.

## Conclusion

From being attributed to culture or evolving inside the culture, the algorithm had become equally contested as the word *culture* itself in terms of the terminological anxiety they both raise. The boundaries of the definition of "algorithm" are vague. So, it is important to understand that the multiplicity in its meanings and offers us more proof of its effects and how it has become part of sociality. The more we probe the term *algorithm* with respect to different academic streams, the multiplicity increases, which results in refining the understanding as the meaning evolved for various public to even becoming multiple with the same set of publics.

Concerns arising from algorithms also add substance to the different meanings attached to it. The difference in experience with diverse sociotechnical assemblages utilising algorithms yields a different set of problems though not for everyone; still, the scope should exist to acknowledge those future complexities. Thus, ethnographic and anthropological studies are required to expand and interpret such experiences.

A significant point of consideration is the fact that technical people are not the only ones engaging with and producing algorithms. A diverse set of people with varied skills, when interacting with algorithms, produces an additional set of networks involving them. Thus, simplicity in understanding algorithm offered by computer science is deceiving in regard to dependency attached to it in the networked society. Their definition closes more doors of exploration by shutting the larger publics out of its scope. Thus, it is imperative for social sciences to explore what affects the society. Standardising the definition of algorithm although helps in the law and

policy making process but also restricts the stakeholding in terms of how and whom it affects.

Even though different nations and groups are coming with various legal approaches regarding automated decision-making systems or algorithms building on their standardise definitions. Though late enough, the idea of regulating algorithmic assemblages is appropriate, but without constant evolution around, the understanding would not be adequate enough to uphold the rights of the ones it affects the most.

## References

1. Abu-Lughod L. (1991) Writing Against Culture. In: R. Fox (ed.) Recapturing Anthropology: Working in the Present. Philadelphia: School of American Research Press. pp. 137–162. https://philpapers.org/rec/ABUWAC

2. Ananny M., Crawford K. (2018) Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media and Society*, no. 20(3), pp. 973–989. https://doi.org/10.1177/1461444816676645

3. Anderson J., Rainie L. (2014) Digital Life in 2025. The Future of Internet. Pew Research Center (accessed: 25.11.2021)

4. Arooni J. (2017) *Algorithmic Harms: Simultaneous Results and Proponents of Privacy Violations for Individual Users*. Algorithmic Harms: Simultaneous Results and Proponents of Privacy Violations for Individual Users. (accessed: 25.11.2021)

5. Beard J. (2014) Autonomous Weapons and Human Responsibilities. *Georgetown Journal of International Law,* vol. 45, no 6, pp. 618–678.

6. Bertolini A. (2013) Robots as products: The case for a realistic analysis of robotic applications and liability rules. *Law, Innovation and Technology*, no. 2, pp. 214–247. https://doi.org/10.5235/17579961.5.2.214

7. Bozdag E. (2013) Bias in algorithmic filtering and personalisation. *Ethics and Information Technology*, no. 3, pp. 209–227. https://doi.org/10.1007/s10676-013-9321-6

8. Brauneis R., Goodman E. (2017) Algorithmic Transparency for the Smart City. *SSRN Electronic Journal*, no. 103, pp. 103–176. https://doi.org/10.2139/ssrn.3012499

9. Burrell J. (2016) How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, no. 1, pp. 1–12, 205395171562251. https://doi.org/10.1177/2053951715622512

10. Burris B. (1980) Book Review: Outline of a Theory of Practice. *Critical Sociology*, pp. 89–91. https://doi.org/10.1177/089692058000900410

11. Campisi P. (2013) Security and privacy in biometrics: Towards a holistic approach. In: Security and Privacy in Biometrics. L.: Springer. pp. 1–23. https://doi.org/10.1007/978-1-4471-5230-9_1

12. Ceruzzi P.E. (1998) *A history of modern computing*. Boston: MIT Press, 438 p.

13. Christian B., Griffiths T. (2016) *Algorithms to live by: the computer science of human decisions*. N.Y.: Henry Holt, 368 p.

14. Conger S., Pratt J.H., Loch K.D. (2013) Personal information privacy and emerging technologies. *Information Systems Journal*, no. 23, pp. 401–417. https://doi.org/10.1111/j.1365-2575.2012.00402.x

15. Danks D., London A. J. (2017) Algorithmic bias in autonomous systems. IJCAI International Joint Conference on Artificial Intelligence, pp. 4691–4697. https://doi.org/10.24963/ijcai.2017/654

16. DeCew J.W. (1986) The Scope of Privacy in Law and Ethics. *Law and Philosophy*, no. 5, pp. 145–173.

17. Devendorf L., Goodman E. (2015) The Algorithm Multiple, The Algorithm Material: Reconstructing Creative Practice. Contours of Algorithmic Life Conference. http://www.confectious.net/may-15-the-algorithm-multiple-the-algorithm-material-reconstructing-creative-practice-uc-davis/

18. Diakopoulos N. (2015) Algorithmic Accountability: Journalistic investigation of computational power structures. *Digital Journalism*, no. 3, pp. 398–415. https://doi.org/10.1080/21670811.2014.976411

19. Dourish P. (2016) Algorithms and their others: Algorithmic culture in context: *Big Data & Society*, no.11, pp. 1–16, https://doi.org/10.1177/2053951716665128

20. Elish M. C. (2016) Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction (WeRobot. *SSRN Electronic Journal*, no. 1, pp. 1–26. https://doi.org/10.2139/ssrn.2757236

21. Eslami M. et al. (2019) User Attitudes towards Algorithmic Opacity and Transparency in Online Reviewing Platforms. *Human Factors in Computing Systems Proceedings*, pp. 1–14. https://doi.org/10.1145/3290605.3300724

22. Floridi L. (2016) On Human Dignity as a Foundation for the Right to Privacy. *Philosophy and Technology*, no. 4, pp. 307–312. https://doi.org/10.1007/s13347-016-0220-8

23. Freidman B., Kahn H. (2002) Human values, ethics, and design. In: The human-computer interaction handbook: fundamentals, evolving technologies and emerging applications. Wash.: University of Washington, pp. 1177–1201.

24. Fried C. (1984) *Philosophical dimensions of privacy: an anthology*. Cambridge: University Press, 426 p.

26. Gillespie T. (2014) The Relevance of Algorithms. In: T. Gillespie et al. (eds.) Media Technologies: Essays on Communication, Materiality, and Society. Boston: MIT Press. pp. 167–194. https://doi.org/10.7551/MITPRESS/9780262525374.001.0001

26. Gillespie T. (2016) Algorithm. In: B. Peters (ed.) Digital Keywords: A Vocabulary of Information Society and Culture. Princeton: University Press, pp. 18–30.

27. Goffey A. (2008) Algorithms. In: M. Fuller (Ed.) *Software Studies. A Lexicon.* Boston: MIT Press, pp. 15–20. https://mitpress.mit.edu/books/software-studies

28. Goldberg I., Hill A., Shostack A. (2001). TRUST, ETHICS, AND PRIVACY. *Boston University Law Review*, no. 81, pp. 407–422.

29. Granka L.A. (2010) The politics of search: A decade retrospective. *Information Society*, no. 5, pp. 364–374. https://doi.org/10.1080/01972243.2010.511560

30. Haines N. (1955) Responsibility and Accountability. *Philosophy*, no. 30, pp. 141–163.

31. Hayes D. et al. (2017) Geolocation Tracking and Privacy Issues Associated with the Uber Mobile Application. Conference on the Information Systems Applied Research, vol. 10, no. 45, pp. 1–11.

32. Hildebrandt M. (2014) The Dawn of a Critical Transparency Right for the Profiling Era. In: *Digital Enlightenment Yearbook*, IOS Press, pp. 41–57.

33. Jensen T. E., Winthereik B. R. (2005) Book Review: The Body Multiple: Ontology in Medical Practice. *Acta Sociologica*, no. 3, pp. 266–268. https://doi.org/10.1177/000169930504800309

34. Karnow C. (1996) Liability for Distributed Artificial Intelligences. *Berkeley Technology Law Journal*, no. 11, 147 p. https://doi.org/10.15779/Z38ZD4W

35. Kearns M., Roth A. (2020) Ethical algorithm design should guide technology regulation. Available at: https://www.brookings.edu/research/ethical-algorithm-design-should-guide-technology-regulation

36. Koene A. (2017) Algorithmic Bias: Addressing Growing Concerns. *IEEE Technology and Society Magazine*, no. 2, pp. 31–32. https://doi.org/10.1109/MTS.2017.2697080

37. Kowalski R. (1979) Algorithm = logic + control. *Communications of the ACM*, no. *22*(7), pp. 424–436. https://doi.org/10.1145/359131.359136

38. Kranzberg M. (1986) Technology and History: Kranzberg's Laws; *Technology and Culture*, no. 3, p. 544. https://doi.org/10.2307/3105385

39. Lévy P. (2001) *Cyberculture*. Minneapolis: University of Minnesota Press. 280 p.

40. LoPucki, L. (2018) Algorithmic Entities. *Washington University Law Review*, no. 4, p. 887.

41. Lum K., Chowdhury R. (2021) What is an 'algorithm'? It depends whom you ask. *MIT Technology Review*. Available at: https://www.technologyreview.com/2021/02/26/1020007/what-is-an-algorithm/

42. Martin K. (2019) Designing ethical algorithms. *MIS Quarterly Executive*, no. 2, pp. 129–142. https://doi.org/10.17705/2msqe.00012

43. Mateas M., Montfort N. (2005) *A Darkly: Obfuscation, Weird Languages, and Code Aesthetics*.

44. Mol A. (2002) *The body multiple: ontology in medical practice*. Durham: Duke University Press. 216 p.

45. Nayak S. (2013) *Copyright Protection for Computer Software an Indian Prospective — Intellectual Property — India*. Available at: https://www.mondaq.com/india/copyright/262564/copyright-protection-for-computer-software-an-indian-prospective

46. Nieborg D.B., Poell T. (2018) The platformization of cultural production: Theorising the contingent cultural commodity. New Media and Society, vol. 11, pp. 4275–4292.

47. NTSB. (2018) Collision Between a Sport Utility Vehicle Operating with Partial Driving Automation and a Crash Attenuator. Washington: NTSB, 74 p.

48. Panday, J. (2017) India's Supreme Court Upholds Right to Privacy as a Fundamental Right and it's about Time. Electronic Frontier Foundation. Available at: https://www.eff.org/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its-about-time

49. Parent W. A. (1983) A New Definition of Privacy for the Law. *Law and Philosophy*, no. 3, p. 305. https://doi.org/10.2307/3504563

50. Pasquale F. (2013) *The Emperor's New Codes*. P. 1–86.

51. Phillips J. W. (2011) Secrecy and Transparency: An Interview with Samuel Weber. *Theory, Culture & Society*, no. 8, pp. 158–172. https://doi.org/10.1177/0263276411428339

52. Puttaswamy v. India. Global Freedom of Expression (2017). Available at: https://inforrm.org/2017/09/04/case-law-india-puttaswamy-v-union-of-india-supreme-court-recognises-a-constitutional-right-to-privacy-in-a-landmark-judgment-hug

53. Rubel A. et al. (2018) Algorithms, bias, and the importance of agency. *CEUR Workshop Proceedings*, pp. 9–13.

54. Rushe D. (2020) Tesla driver who died in 'autopilot' crash was playing on phone, inquiry finds. The Guardian. Available at: https://www.theguardian.com/technology/2020/feb/25/tesla-driver-autopilot-crash

55. Seaver N. (2013) Knowing Algorithms. In: Digital STS Field Guide, pp. 412–422. https://doi.org/10.2307/j.ctvc77mp9.30

56. Seaver N. (2017) Algorithms as culture: Some tactics for the ethnography of algorithmic systems. *Big Data and Society*, no. 2, pp. 1–12. https://doi.org/10.1177/2053951717738104

57. Shabana N. (2015) An Indian Outline On Database Protection — Privacy — India. Available at: https://www.mondaq.com/india/data-protection/450526/an-indian-outline-on-database-protection

58. Siddiqui F. (2019). *Tesla sued by family of Apple engineer killed in Autopilot crash.* Available at: https://www.washingtonpost.com/technology/2019/05/01/tesla-sued-by-family-man-killed-autopilot-crash/

59. Striphas T. (2015) Algorithmic culture. *European Journal of Cultural Studies*, no. 4–5, pp. 395–412. https://doi.org/10.1177/1367549415577392

60. Teixeira A. C. et al. (2017) Complexities of Cyberculture in Pierre Lévy and Developments in Education. *Creative Education*, no 1, pp. 119–130. https://doi.org/10.4236/CE.2017.81010

61. Tene O. (2017) Taming the Golem: Challenges of Ethical Algorithmic Decision-Making. *North Carolina Journal of Law & Technology*, no. 19, 16 p.

62. Thomson J. J. (1975) The Right to Privacy. *Philosophy & Public Affairs*, no. 4, pp. 295–314.

63. Tjong Tjin Tai E. (2018a) Liability for (Semi)Autonomous Systems: Robots and Algorithms. *SSRN Electronic Journal*, pp. 55-82. https://doi.org/10.2139/ssrn.3161962

64. Tufekci Z. (2015) Algorithmic Harms beyond Facebook and Google: Emergent Challenges of Computational Agency. Journal on Telecommunications & High Tech Law, no. 23, pp. 203–216. https://doi.org/10.1525/sp.2007.54.1.23.

65. Tufekci Z., York J. C. et al. (2015) *The Ethics of Algorithms: from radical content to self-driving cars*. Available at: https://cihr.eu/publication-the-ethics-of-algorithms/

66. Verbeek P. P. (2008) Morality in Design, Design Ethics and the Morality. *Design*, pp. 91–103.

67. Williams R. (1983). *Keywords: A vocabulary of culture and society*. Oxford: University Press.

68. Wirth N. (1975) Algorithms Plus Data Structures Equals Programs. *Prentice Hall* (Issue August). (Prentice-Hall series in automatic computation)

---

**Information about the authors:**

Nabil Ahmad Afifi — PhD Scholar.

Reeta Sony A.L. — Assistant Professor.

The article was submitted 12.07.2021; approved after reviewing 11.10.2021; accepted for publication 01.11.2021.