

# **ALGORITHMIC POLICING AND INTERNATIONAL LAW: CRITICAL REALITIES IN DATA-DRIVEN CORPORATES AND GOVERNMENTS OVER AI REALMS**

Abhivardhan\*

## **ABSTRACT**

*Algorithmic policing is an important development in the field of Law and Technology, which has subjected to a relevant instrumentality in developed and developing economies. Beyond the crude material realities of machine learning, the role of algorithmic policing has certainly changed and has questioned the basic role of big data in its structure and resonance with the principles of justice. Also, it has contributed towards an acute form of resilient effect in economies such as China, US and some EU countries, where the role of AI-based systems has surpassed the legal barriers of data protection legislations, and has certainly invoked concerns for corporate and individuals, where rule of law is not limited to mere subjected principles of natural justice. In fact, algorithmic policing raises some imperative questions over the role of international human rights law (or IHRL) and has impacted individuals in cases of studies on customer experience and data dimensionality, where corporates are accountable and reliant over the frugalities in international cyberspace regarding the role and scope of AI-based entities. The plural nature of data processing raises significant issues over the dimensional variation of privacy intrusions that AI-based parameters are applied and instrumented in developed and*

---

\*Amity University Uttar Pradesh, Lucknow Campus. The author can be reached at [abhivardhan2@gmail.com](mailto:abhivardhan2@gmail.com)

*developing economies. It has a significant role yet lacked opinio juris in international law and regional legal regimes, where it has become uncertain to restrict the dynamism of data-driven modalities existent under artificial intelligence. This paper thus raises legal issues over algorithmic policing in the sphere of international law and human rights, suggests solutions with regards the status of an AI in the schemata of algorithmic policing regarding privacy intrusions and provides case analysis of algorithmic policing as soft violations of definite human rights and privacies with reference to China, the EU and US.*

**Keywords:** *international law, algorithmic policing, machine learning, self-determination, customer experience.*

## I. INTRODUCTION

The extensive use of AI systems and devices has amassed varying interest towards the due development of a techno-globalist age in the West and Asiatic economies. China, for example, in most prominent sense, other than the US and the EU, has mastered the corporate art of AI modelling and marketing mechanics, which nowadays is put into use of realms of customer experience (CX)<sup>1</sup>. This realm is indulging yet at the certain verge of development, which itself, cannot be termed as a direct IHRL violation, but a due effect of AI modality. This is a part of the soft power implications created by governments and corporates over the same with the data subjects being individuals in different scopes and domains. This also entails a significant development in the field of international cyber law, pursuant to the need of a more diverse and relevant approach as compared to the principles of data protection and privacy.

---

<sup>1</sup> Giselle Abramovich, Study Finds Investments In Customer Experience Are Paying Off Cmo.com (2018), <https://www.cmo.com/features/articles/2018/2/26/adobe-2018-digital-trends-report-findings.html#gs.xoSSi8Q> (last visited Feb 11, 2019); Christina Larson, Who needs democracy when you have data? MIT Technology Review (2018), <https://www.technologyreview.com/s/611815/who-needs-democracy-when-you-have-data/> (last visited Feb 11, 2019).



Figure 1: A diagram depicting the essence of customer experience (CX)<sup>2</sup>.

It is a realm of existence, which has been dealt less, with the pursuant development of AI Ethics, in particular aspect of the Westernized model. Such emergence has led to the conceptual establishment of algorithmic policing as a legal, anthropological and technological phenomenon. The paper establishes the conceptual role of algorithmic policing, its policy-based impact on democracies and non-democratic regimes such as China, with its ontology affecting the role of human rights, data ethics and processing and cyberspace implications. Further, it analyses the privacy intrusions involved and a review whether such intrusions are real human rights violations. Relevant conclusions over the genesis of such related issues are provided.

## II. ALGORITHMIC POLICING: A CROSS-CONNECTED PHENOMENON

The significance of AI systems is determinant in the course of social interaction, and that itself in the limitedness of the domain involved. It is not a simple establishment because after the Dartmouth Proposal, the tending

<sup>2</sup> Will Thiel, The role of Artificial Intelligence in customer experience Pointillist (2018), <https://www.pointillist.com/blog/role-of-ai-in-customer-experience/> (last visited Feb 11, 2019).

approach to deal AI has changed; states and non-state actors have established differential methods to use machine learning to channelize modal forms of data processing. The role of pseudonymization is a different outset, yet it is not the same as formed. However, Algorithmic policing is somewhat different. It is the manifested form of policy-making involving state/non-state actors in their affairs to materialize their corporeal and ethical interests towards a machine learning-based system to work upon the due development of interaction, reception and pursuance of the system and its efficiency directed in the method and need that the actor wishes to pursue. The problems suggest that an AI realm fails to entail bias, in algorithms, as a complexity, which if encouraged, leads to varying soft violations of human rights, which cannot be possibly dealt with retributive approaches due to the indulgent increase in the usage of AI realms and the economic impact that it has on corporates, propagating customer experience as a special phenomenon.

*[Xinjiang] (“New Territory”) is the traditional home of a Chinese Muslim minority known as Uighurs. [...] One result has been an uptick in violence in which both Han and Uighur have been targeted, including a 2009 riot in the capital city of Urumqi, when a reported 200 people died. The government’s response to rising tensions has not been to hold public forums to solicit views or policy advice. Instead, the state is using data collection and algorithms to determine who is “likely” to commit future acts of [violence] or defiance [...] The Xinjiang government employed a private company to design the predictive algorithms that assess various data streams. There’s no public record or accountability for how these calculations are built or weighted<sup>3</sup>.*

A special issue has been addressed in China by scholars and professionals, which is not recognized as a human right violation but a public policy

---

<sup>3</sup> Christina Larson, Who needs democracy when you have data? MIT Technology Review (2018), <https://www.technologyreview.com/s/611815/who-needs-democracy-when-you-have-data/> (last visited Feb 11, 2019).

approach by the Chinese Government. This activity is on the due approach of algorithmic policing in the territory of Xinjiang, where selective analysis is instrumented with biased algorithms, with no clear socio-statistical study over the geographical realm of the people. This is a legal issue for in case of understanding the course of human rights, where, it is a question if an AI can turn racist. However, the technological part comes into another conjugation, where the aspect of recognition of such modalities extend the limits. A recent approach to GDPR with AI systems, with no entitative recognition, has been given by the ICO, UK:

*“[I]f you use AI to make solely automated decisions about people with legal or similarly significant effects, tell them what information you use, why it is relevant and what the likely impact is going to be<sup>4</sup>.”*

An AI is a human artefact, which learns and is capable of relearning and developing such techniques at its own<sup>5</sup>. A recent declaration recognized the technological role of an AI realm as proposed by EDPS in 2018, based on (1) Privacy by Design and Default and (2) Fairness Principle as the prima facie conceptions involved<sup>6</sup>, which however is a legal and factual limitation for AI realms to estimate and recognize IHRL obligations. The limits that the jurisprudential scope on the subject-matter is rendered in thought, is not complete.

The first principle regards the usage of AI-based systems with a probable outlook towards wherein its activity can be privacy-oriented by default. It

---

<sup>4</sup> Right to be informed, Ico.org.uk (2018), <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed> (last visited Feb 14, 2019).

<sup>5</sup> A. M. TURING, *COMPUTING MACHINERY AND INTELLIGENCE*, LIX Mind 433-460 (1950).

<sup>6</sup> Declaration on Ethics and Data Protection in Artificial Intelligence, Edps.europa.eu (2018), [https://edps.europa.eu/sites/edp/files/publication/icdppc-40th\\_ai-declaration\\_adopted\\_en\\_o.pdf](https://edps.europa.eu/sites/edp/files/publication/icdppc-40th_ai-declaration_adopted_en_o.pdf) (last visited Feb 14, 2019), at 2-6. The general problem we face in determining the use of these principles is connected with the scope of GDPR over AI. The recent European regulation entails an AI to be a technology and not an entity, whereby it fails to lead a solvable route in its Articles 3 & 14-18 of the regulation.

also includes the design part; which means to regulate AI in the limitedness of the design or technical construct that vests in the same. This may seem towards a protectionist legal obligation on corporates, governments and private actors, but the implications arise beyond the principle, because machine learning leads the procedural reception and intervention with data into its own liberty, and that also is based on what functions are expectant. However, the locus standi over ML algorithms to be yet limited by the way they have to work destroys the creative and safeguarding aspect of AI, which can be understood by the increasing complexity of ML-oriented operations. Data mining, as well, even may be taken into the purview of anti-trust laws, for example in the case of Amazon, Facebook and Google. However, it poses more serious implications rather than the legal position of trust. The extensive utility of data is a legal possibility and privacy obligations are restrictive enough to determine over the course that such attributions are led. In 2017, scientists from Facebook AI Research (FAIR) discovered that their chatbots had developed their own language, as a major development in 9 hours<sup>7</sup>, which they had to shut down. There are similar incidents, which lead towards the similar or apparent implications of observance. However, the inferences that can be drawn out are that machine learning-oriented AI systems exist in the course of a technological liberty, which surpasses the privacy by design and default restrictions imposed (if done) and cannot be resolved only by fragmentation as a process, when they become complex. Indeed, gravity and degree can have a legal role as tools to understand the regulatory aspect of ML, but liability, as a matter of determination, can certainly not be limited by mere implications of presupposed simulations expected, because ML has the potential to break up barriers (provided that AI needs to be strong; weak AIs have relatively less chances of high predictability).

---

<sup>7</sup> Tony Bradley, Facebook AI Creates Its Own Language In Creepy Preview Of Our Potential Future Forbes.com (2017), <https://www.forbes.com/sites/tonybradley/2017/07/31/facebook-ai-creates-its-own-language-in-creepy-preview-of-our-potential-future/> (last visited Feb 14, 2019).

The second principle involving the declaration is the fairness principle. It is collateral to the scope of GDPR, as a transnational European Regulation. The key corollaries involving the development and scope of the principle are:

- (a) reasonable expectation;
- (b) observational impact;
- (c) predeterminate prevention of risk to human life, liberty and dignity; and,
- (d) original purpose.

Now, (a) is a legal idea based on the scope of expectation that the user may entail in relation to the data subject and the AI system, which is, on the side of human users, is justified. However, from the side of an AI system, it may not entail a complete justice because of the complications of ML. We cannot ascertain at the same time as in how come the legally reasonable expectation may render fruitful due to the varying implications of algorithmic policing. This is also not justifiable in positive law because we have personified an AI system with the similar jurisprudential normativity with which we consider natural persons. Regarding (b), observational impact is rendered to be justified because the question of real liability (civil/humanitarian/criminal) may come into place. However, the retributive or punitive approach towards redressal may lead us into a legal anarchy because an AI system needs an equation with human personification which a positive law render. In addition, the traditional or general approach of liability cannot apply to AI because it cannot be personified and equated with humans in that legal status of observation and adjudication. Thus, being a different species of juristic persons, an AI resembles a special capability of consideration. Consumer Personalization, for example is a directly connected phenomenon to this concept<sup>8</sup>. Regarding (c), we can dilute the positive legal position of an

---

<sup>8</sup> According to BrightEdge, in 2018, a new trend was seen in companies regarding tech marketing. While AI accounted 25.69%, Consumer Personalization accounted 28.66% and Voice Search grabbed up 21.23%. Also, these top 3 trend percentages are based on AI applications, accounting 75% collectively. See also What Consumers Really Think About AI, Pega.com (2017), <https://www.pega.com/system/files/resources/2017-11/what-consumers-really-think-of-ai-infographic.pdf> (last visited Feb 14, 2019); *Infra* note 21.

AI as a juristic position, account a considerable usage of data protection and anti-trust legislations and account private persons to limited discourses with considering a special yet temporary scope of (a). If we take GDPR for example, then yes, the 9 rights may come into practical usage, except in Arts. 16 to 18 owing to the complex nature of ML-led AI realms provided that the data influx for mining is considerably viable and has reached complex learning mechanisms and stages already. To that extent, (c) is rendered. With respect to (d), we can demarcate original purpose into two aspects- (i) user/data subject's purpose and (ii) purpose of AI realm. Regarding the user/data subject, we may limit the course of liability and provide liberty to high predictability discourses of machine learning systems. However, the ontology involved with the purpose that an AI has may be transient, and yet transforming. There may occur anomalies over the fact whether the AI realm has a potential and reasonable capability to attain the purpose and end. Nevertheless, this case occurs only when such complex stage of data mining and influx has reached. This is a course of procedure facilitated by the realm itself. Some points of importance must be considered:

- a. Algorithmic policing is a dynamic process of facilitating an AI towards a policy by the user(s), who require its relevant facilitation. Such facilitation, as when is employed by Machine Learning (hereinafter ML), is based on the algorithmic services that are crafted;
- b. Fragmentation of an AI is a possibility, but the complexity of data penetrations and interactions is not tenable to be dealt with the same approach per se;
- c. An AI and its algorithmic policing cannot be directly challenged via data protection law because its formation is deepened, and depends on the nature of strength that the ML-based AI attains;
- d. The Status of an AI via the principle of Privacy by Design and Default can be reformed by removing the similar limitations that the substantive principle entails on a tech-oriented architecture. A simple

method can be to recognize the entitative values and privacy of an AI system in terms of generic juristic status;

- e. Purposive construction can be suitably entitled to AI realms in general terms and can be led towards better modalities in terms of the elements of the fairness principle;

### **III. HUMAN RIGHTS REGIMES IN INTERNATIONAL CYBER LAW: THE COMMONALITIES**

A human right is anthropomorphic; and it recognizes the existence of human artefacts in detail. The principles of liberty, equality and fraternity are converted into safeguarded rights in constitutional democracies, and the customized patterns of such safeguarded rights by regional regimes shapes into the constituent form of international law, which is known as customary international law. The significant role that UDHR led was a global motivation, further led by the International Covenants of 1966. This signifies the existence of any universally tenable phenomena<sup>9</sup> related to the international legal scenario, and is duly facilitated thereby. However, in case of different human artefacts<sup>10</sup>, the observation and procedure of human rights changes dynamic in a varying fashion. Also, a special obligation approach, for understanding the technical and social commonalities on AI can be inspired by the tripartite model of human rights, based with the ICESCR, also known as the Maastricht Guidelines<sup>11</sup>, where minimal obligations shape up state responsibility in a better way.

<sup>9</sup> Ana Maria Lebada, Second Committee Considers Role of AI in Advancing SDGs Sdg.iisd.org (2017), <http://sdg.iisd.org/news/second-committee-considers-role-of-ai-in-advancing-sdgs> (last visited Feb 14, 2019); AI for Good: Accelerating Progress towards the SDGs - UNSDN - United Nations Social Development Network, UNSDN - United Nations Social Development Network (2018), <http://unsdn.org/2018/05/09/ai-2> (last visited Feb 14, 2019); Artificial intelligence can help achieve the SDGs, UNOPS (2018), <https://www.unops.org/news-and-stories/speeches/the-second-annual-digital-workforce-summit> (last visited Feb 14, 2019).

<sup>10</sup> The importance of a human artefact is tenable for artificial intelligence and is technology-subjected and objected socialization, which has relations with culture. See also ARNOLD PACEY, MEANING OF TECHNOLOGY 8, 176-178 (1999).

<sup>11</sup> This approach entitles a clear and yet protectionist ontology towards determining the practical role of human rights obligations. See also ELLIE PALMER, JUDICIAL REVIEW, SOCIO-ECONOMIC RIGHTS AND THE HUMAN RIGHTS ACT 22 (2007); International Commission of Jurists, Maastricht Guidelines on Violations of Economic, Social and Cultural Rights Refworld (1997), <https://www.refworld.org/docid/48abd5730.html> (last visited Jan 8, 2019).

“The [reader] must accept it as a fact that digital computers can be constructed, and indeed have been constructed, according to the principles we have described, and that they can in fact mimic the actions of a human computer very closely<sup>12</sup>”.

The problem with algorithmic policing is not about its structure: it is about its patronage of data utility and penetration, where legitimacy and credibility are moot. We have to adequately determine the stable role of an ML-led system, whether the algorithms and data used are in consonance to understand the human society, and the recourse of the same perception and retentivity, which is an expectancy for the deference of human rights<sup>13</sup>. Also, a point of interest to discern is about the legal structure developed in the theory and doctrines of human rights<sup>14</sup>. From the recourses of action, accountability, responsibility and violation, human rights seem to be a lineation. It fails to settle its legitimate stability, because it promises for a compromising sustenance<sup>15</sup> in the eyes of law, which is again an instrumentation towards maintaining rule of law.

“[All] persons deprived of their liberty shall be treated with humanity and with respect for the inherent dignity of the human person<sup>16</sup>”

This linear approach of preserving liberty and equality as basic human rights is promising, yet it cannot be a complete status quo, nor can we expect

---

<sup>12</sup> *Id.* at 438.

<sup>13</sup> One constraint of machine learning is that, as a data-determined procedure, it essentially relies on the value of the causal data and thus can be very inelastic. In fact, its generic establishment for procurement and possible recourses must be generally settled, which is a big issue. See also M. L. Cummings et al., *Artificial Intelligence and International Affairs: Disruption Anticipated* Chathamhouse.org (2018), <https://www.chathamhouse.org/sites/default/files/publications/research/2018-06-14-artificial-intelligence-international-affairs-cummings-roff-cukier-parakilas-bryce.pdf> (last visited Jan 17, 2019) at 13; MICHAEL N SCHMITT & LIIS VIHUL, *TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS* 22-24, 190-191, 206, 535 (2 ed. 2017).

<sup>14</sup> *HUMAN RIGHTS PROTECTION IN GLOBAL POLITICS* 54 (Kurtz Mill & D. J. Karp eds., Palgrave Macmillan 2015).

<sup>15</sup> JACK M BALKIN, *CONSTITUTIONAL REDEMPTION* 141 (2011).

<sup>16</sup> *International Covenant on Civil and Political Rights*, Refworld (1966), <http://www.refworld.org/docid/3ae6b3aa0.html> (last visited Feb 14, 2019).

towards a promised simulation to be conceived by legislators until, the state concerned can foresee it<sup>17</sup>. There do exist commonalities over the conceptual realism of international human rights law and its role and primacy implications to regional human rights regimes, and in the case of AI, this coalesces with data law and obligations pursuant to cyberspace. These commonalities are:

- (a) flexibility of legal viability;
- (b) minimal deterrence over or/and adherence to state and non-state actors obliged under international law;
- (c) socialization and technological relevance as an anthropomorphic question and;
- (d) economic and social justice.

With regards (a), the legal adherence to human rights treaties/jus cogens norms/declarations/UNGA resolutions/transnational regulations or treaties reflects the significant role of customary international law and state practice to certify the leaning stage towards flexible mechanisms in the legal system towards the development, protection and evolution of AI realms. Ratification or obligatory stages of acceptance to IHRL obligations requires a public policy settlement and clarity, which states do entail while they propose to adhere such obligations. Pursuant to AI, if liberal, yet mature legal policies are taken into account for reform, then it may lead with a better possibility for the legal system to preserve a credible juristic status of artificial intelligence.

[T]he State duty to protect is a standard of conduct. Therefore, States are not per se responsible for human rights abuse by private actors. However, States may breach their international human rights law obligations where such abuse can be attributed to them, or where they fail to take appropriate steps to prevent, investigate, punish and redress private actors' abuse [...] States also have the duty to protect and promote the rule of law, including by taking

---

<sup>17</sup> *Id.* 4, at 144.

measures to ensure equality before the law, fairness in its application, and by providing for adequate accountability, legal certainty, and procedural and legal transparency<sup>18</sup>

On (b) and (c), we may refer the viable legal utility of the Maastricht Guidelines as aforementioned, where the perspective and spectrum of the ICESCR is referred. The perspective of economic and social rights entails to a more credible issuance of reasonable considerations over an AI and its recognition in a welfare state. In fact, every technological realm (smartphones, cryptocurrencies, IoT devices, PCs, etc.) has changed socialization from two ends: first is the end of the subjected users as how the life of a society is changed and second from the end of the realm itself in terms of its economic viability and social utility<sup>19</sup>. Of course, an AI is a technological entity and attains the same right and reality to a subjected socialization as any other tech-oriented system or device or realm may pose. Hence, for the perspective of IHRL, the umbrella of socio-economic obligations can render a progressive future and settlement of usage and scope of AI in a social life. With respect to (d), questions can be posed over employment, corporate rights, socio-economic equity in cyberspace regarding representation & capability and other related issues of residual scope.

This may be case to case-based, because a democratized legal system may have its own public policy, which is coherent and real. Nevertheless, keeping the democratic counterparts aside, data-driven governance systems need to follow obligations in general. The *opinio juris* involved in state sovereignty and human rights recognizes the role of self-determination of the people,

---

<sup>18</sup> Office of High Commissioner of Human Rights, Guiding Principles on Business and Human Rights Ohchr.org (2011), [https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR\\_EN.pdf](https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf) (last visited Jan 16, 2019).

<sup>19</sup> J. G. Ruggie, Protect, Respect and Remedy: A Framework for Business and Human Rights (A/HRC/8/5) Ohchr.org (2008), <http://www.ohchr.org/EN/Issues/TransnationalCorporations/Pages/Reports.aspx> (last visited Jan 9, 2019) at 9.

and has been inestimably recognized by international law<sup>20</sup>. Here are the proposed aspects over the consideration of human rights regimes:

- a. Legitimate foundations must be made in regards the discourse of human rights and technology-oriented AI policing taking care the reasonable mechanism and role that ML entails;
- b. There must exist ethics-oriented rules and initiatives to develop the discourse of ML-based algorithmic policing and legitimate foundations must be settled to channelize routes to recognize and preserve the self-determination of individuals in cyberspace and in personam;
- c. There must be a gradual change in the understanding of human rights violations; there may be such violations or abuses of the same kind, but their degree or observance may render a dimensional perspective, where they might by 'soft' interventions, which has been seen in Xinjiang, China and the West: even using any voice-recognition device for example (not only about data collection and voice recognition mechanisms), the use of a device here, with the pursuit of customer experience to be enhanced, is coalescing and connective to that user, which is a policy-based service by the company and facilitates manifested liabilities or responsibilities according to that;

#### **IV. CUSTOMER EXPERIENCE TOWARDS ALGORITHMIC POLICING: MODALITIES IN CHINA, US AND EU STATES**

Any start-up or company has a presumptive intent to cause or incentivise methods or channels towards better experience for and create an essence of loyalty towards the customer(s) concerned. This is not a new concept, as marketing reaches out to be essential factor of corporates to sustain and leave a social relevance for some time. Customer Experience (hereinafter CX) is a phenomenon of marketing and data science, where instead of reaching out long-term manual methods of winning customer loyalty and concern,

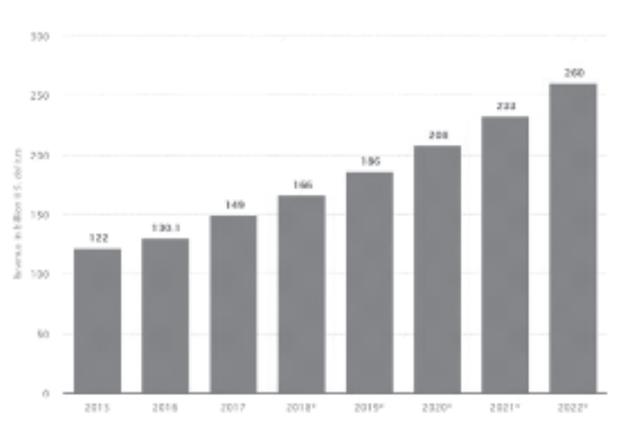
---

<sup>20</sup> South-West Africa Cases; Advisory Opinion Concerning the International Status, ICJ Rep. 1950 148 (1950). Understanding the scope of international cyber law, we can understand the Rules 36-39 of the Tallinn Manual 2.0 and the ITU Convention.

some corporates in the world are implementing ML-led strategies towards understanding the essence of customer-oriented requirements, which seems befitting and promising. However, the problems related start at a latent aspect, when data appropriation is subjected towards the same.

[R]espondents' CX-specific priorities indicate that their organizations are focusing on improving the end-to-end customer experience instead of the entire customer journey from acquisition to loyalty was the top priority (46%), followed by improving cross-channel experiences (45%), and expanding content marketing [capabilities] (42%)<sup>21</sup>

Amazon, Facebook, Google, Alibaba, Symantec, HP, Apple and Microsoft are one of the few tech corporates, who are involved in the extensive usage of algorithms involved to benefit consumers. These benefits, are dynamic, and are yield by simple ML-led data mining methods, where based on a mass of data present, it facilitates a comfortability for the corporates to understand the realms of need for their consumers.



*Figure 2: Revenue from big data and business analytics worldwide from 2015 to 2022 (in billion U.S. dollars)<sup>22</sup>*

<sup>21</sup> The Business Impact of Investing In Experience, Adobe.com (2018), [https://www.adobe.com/content/dam/acom/au/landing/Adobe\\_Biz\\_Impact\\_CX\\_APAC\\_Spotlight.pdf](https://www.adobe.com/content/dam/acom/au/landing/Adobe_Biz_Impact_CX_APAC_Spotlight.pdf) (last visited Feb 14, 2019) at 2.

<sup>22</sup> Global big data and business analytics revenue 2015-2022, Statista (2019), <https://www.statista.com/statistics/551501/worldwide-big-data-business-analytics-revenue/> (last visited Feb 14, 2019).

If we estimate the comparative aspect of EU in terms with the US and other potential data-driven economies of related nature, then a special estimation is discernible over consumer experience and its implications being embedded. The US is subjecting an increasing isolation in its foreign policy as well as in socio-economic terms with the EU, and in case of the digital single market, compliance regarding GDPR is still ongoing. While illegal bid requests under Art. 5(1)f of the regulation are in activity, it is imperative to consider as how consumer experience will be regarded in terms of its safety and credibility. The reason is based on the aspect of precautions and methods to prevent intrusive designs per se, and cases may increase. Nevertheless, big data has been discerned to be a special incentive towards utilization and streamlining of purpose, which China has been doing without restrictions. Still, the European diaspora has led a better digital single market and has attempted to lead the discourse of enforcement for the deemed purpose involved.

Content expansion becomes feasible and it leads to another form of algorithmic policing. This is not a hard-lined violation of human rights, because the processing is corporate-oriented<sup>23</sup>. However, a major use of big data in 2016 by Cambridge Analytica, led to basic violations (yet disputed) of human rights of millions of Facebook users. Nevertheless, statistical analysis shows that some progressive EU states are nearing in spending with the US and their contributory aspect has arisen big per se to proceed<sup>24</sup>. Some important mentions are given herein:

- a. Right to be forgotten and of rectification in Arts. 15-17 GDPR lay a precedent as happened with Google in April 2018 to act and sue companies for the same, but this entails a complex issue and thus needs an ethical approach to recognize the modalities of a ML-led policy involved by companies;

---

<sup>23</sup> Nevertheless, such obligations have a legal value on non-state

<sup>24</sup> Impact of AI on GVA by country worldwide, Statista (2016), <https://www.statista.com/statistics/621583/worldwide-artificial-intelligence-impact-on-economic-growth/> (last visited Feb 15, 2019).

- b. Data-oriented monopoly must be recriminated; anti-trust legislations are obsolete and cannot be applied in competitive markets even if tech corporates are destroying other markets;
- c. Paucity of tenable international law regarding algorithmic policing causes adverse circumstances;

## V. CONCLUSION

As a technical concept, algorithmic policing is a legal procedure yet a dynamic and eccentric to be controlled as a policy to resolve issues in generic sense for recognizing and furthering the self-determination of individuals in international human rights law. Certain conclusions based on proposition are provided thereto:

- a. The legal conception of human rights and rule of law must be cultivating and lead to dimensional and credible establishments, which can be done by extra-implementable methods;
- b. Algorithmic policing can be solved and considered by making data mining an objective ethic, rather than a subjective requirement;
- c. The approach of dealing with the privacy of data is equivalent to and much closer to that of the user in case of algorithmic policing;
- d. Data-oriented monopolies must be curtailed by newer anti-trust legislations in developed and developing economies;
- e. The approach of privacy by default and design is limited and the instrumental role of the GDPR does weaken to understand and estimate a regulatory and safer future for and in the pursuance of the creation and maintenance of an AI-oriented ecosystem;

These conclusions are based on an outset of developments that AI is gaining in corporate and human resources. It is thus possible that algorithmic policing may be rendered in that perspective with resonant solutions.