



LawPublicus
The Legal Portal

Volume 1 : Issue 4
2021

February 2021

Email ID: Lawpublicusportal@gmail.com
Website: www.Lawpublicus.com
Address: A18 Dayanand Colony Lajpat Nagar - 4
New Delhi

Disclaimer

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of ***LawPublicus*** The Legal Portal. The Editorial Team of ***LawPublicus*** holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of ***LawPublicus***. Though all efforts are made to ensure the accuracy and correctness of the information published, ***LawPublicus*** shall not be responsible for any errors caused due to oversight or otherwise.

FOR ***LawPublicus*** The Legal Portal

Editorial Team

Editor-in-Chief

Mr. Nikhil Kumar Chawla

Partner - LawPublicus LLP
Principal Associate Advocate – DKC & Co.
Contact: +91-9654441680
+91-9654030411
Email ID: Nikhilchawla29@gmail.com
Lawpublicusportal@gmail.com

Senior Editor

Ms. Yantakshikaa Sharma

Partner - LawPublicus LLP
Career Counsellor
Email ID: Yantakshika@gmail.com

Senior Editor (Honorary)

Mr. KS Rana

Practising Advocate
Contact: +91-9810326424
Email ID: Jyotideepрана@gmail.com

Senior Editor (Honorary)

Mr. Sandeep Sharma

Practising Advocate

Legal Consultant – Ministry of Law and Justice

Contact: +91-9899009517

Email ID: Sandeepjanmat@gmail.com

Senior Editor (Honorary)

Ms. Khushboo Malik

Research Scholar – Faculty of Law (DU)

Email ID: Malikkhushilaw@gmail.com

About Us

LawPublicus The Legal Portal is a leading journal of multidisciplinary research. It is a free, peer-reviewed, open-access journal that provides insight into diverse and dynamic legal matters.

LawPublicus is a novel initiative by legal minds. As the its name suggests, it is platform for young minds to ignite their willingness and inventiveness in order to contribute to the field of law through new ideas, opinions and thereby contributing to an informed citizenry.

We hope to provide a forum for young and enthusiastic writers to voice their feelings and research on interdisciplinary approaches. We also have in view to evaluate, explore and deliberate, under the tutelage of seasoned editors and academic experts, on current trends and projections based thereon in legal studies. LawPublicus focuses not only on the scholarly writings but also on numerous other approaches such as discussions, interviews, and debates with experts and qualified & industrial professionals.

We are determined and excited to bring authentic, creative and individual ideas and socially-related problems into attention.

LawPublicus calls for research papers, articles, short notes, book reviews & case commentaries, that are distinctive and unpublished.

With this thought, we hereby present to you

LawPublicus The Legal Portal

Protection of Human Rights in a Digital Age: A Need to Overturn the Imminent Catastrophe

Authored By:

Ms. Kashvi Vachhani

Designation: Second Year Student

B.A. LL.B from Gujarat National Law University

E-mail ID: kashvivachhani24@gmail.com

Contact: +91-97695366**

Protection of Human rights in a Digital Age: A Need to overturn the Imminent Catastrophe

By: Kashvi Vachhani

It would be needless to say that we are being tracked every moment we spend on the internet. It is even more needless to state that only a few of us are consciously aware that the data acquired from our activities on the web is a source of financial and political gain that private organizations and governments around the globe benefit from. The discussion about digital privacy is cumbersome and daunting because there is an absence of effective regulations that govern and protect our privacy on the internet. Paradoxically, in this inevitable loop of austere supervision, our basic inalienable rights definitely lose their way.

Technology doesn't come with benefits alone. For the sake of our blooming society, we have to consider that technology has, in fact, has massively contributed to the whole of humanity. We cannot envisage a world where we don't have technology. The technology can be used for encrypted messages, satellite pictures and data sources may be used to explicitly protect and foster human rights. We can also use artificial intelligence to anticipate and prevent human rights abuses.¹

However there is more to this phenomenon- an axiomatic dark side. The digital world is an odious platform for human rights. In the past there have been grave human rights violations that more often than not have been overlooked. The basic premise of this discussion remains that the human rights which are inalienable not only exist in actuality but online too.

At the outset, the human rights violation since the conception of a cyber space can be graded from minor to a global disaster of sorts, if measured on a spectrum. Cyber bullying, trolling, heinous cyber-crimes have been a part of this grave violation. Just when we think that there might be a light at the end of the tunnel, we are met with murk. In the year of 2020 in India's

¹ Human Rights and Technology, Visited at https://www.humanrights.gov.au/sites/default/files/2020-02/techrights_2019_discussionpaper.pdf (last visited May 17, 2020).

capital, the Internet was crowded with a grotesque event – “boys locker room talk” where a handful of high school boys created a chat room solely for degradation of women. They circulated obscene and private pictures of underage girls in addition to passing derogatory comments with a definite criminal intent. This enunciated how easy it is to attack and violate someone’s modesty with the click of a button.

The whole debate surges around the freedom of speech and expression against the right to privacy. However the pendulum shouldn’t swing in one direction where one right is availed at the cost of another.

In another grisly case, social media posts threatened the Rohingya community in Myanmar in the run-up to the 2017 mass murders and assaults.

There has been a gamut of notable instances. While we are on this topic, one cannot leave out the infamous Facebook fiasco. The Co-founder and the Chairman of Facebook, Mark Zuckerberg was called before the Congress for an alleged human rights violation. It turned out that Facebook had been clandestinely accumulating information about people who use Facebook or Facebook partner companies, such as Blockbuster and Fandango. Users of these services all around the world have been monitored to be able to present specific effective ads to people logged in and sometimes have published their online actions without their consent or approval. Facebook’s argument for this accusation was that this data was collected with the objective of presenting specific effective ads to people of the Internet and to people on their social networks.² It enraged the people around the world and rightly so. However, in this global web, corporations have been exploiting customers for years by collecting their confidential information. The difference with Facebook was that it was the first major enterprise to use this information for their economic benefit to be put under public scrutiny.³

Quite ironically, these corporations surely are accountable to the customers. However, they stand for their own personal gain.

² Linda Musthaler, FACEBOOK FIASCO HIGHLIGHTS PRIVACY CONCERNS NETWORK WORLD (2008), Visited at <https://www.networkworld.com/article/2281934/facebook-fiasco-highlights-privacy-concerns.html> (last visited May 17, 2020).

³ *Id*

On the other side of the court, governments have caught up well to this occurrence too. The government of a country holds cent percent accountability and responsibility towards the citizens and naturally the people of the nation, overtime that is, do learn to trust the regime. Unfortunately, the situation is not as simple as it seems.

The lack of transparency in certain governmental activities around the globe has raised eyebrows. The government of China has been inoculated for tracking the users' information for a long time now. The Chinese government has employed millions of people to track down the Internet activity of the users. The data is then collected and compiled into reports, which aims at diffusing any incoming political unrest.⁴

Another example of this blood-curdling happening is The UK's Investigative Power Bill, which legalizes and authorizes mass surveillance by UK security agencies and enables extrajudicial hacking of computers and networks. Respect for rights and upholding the rule of law, is a cornerstone of the strength of democratic systems.⁵

Amongst the known controversial occurrences, is Donald Trump's 2016 presidential campaign. It was suspected that Russians were allegedly involved with the 2016 presidential elections of The United States of America. Certain Russian hackers attacked voter registration systems or state websites in at least 21 states before the big day, entirely breached certain state databases, and stole hundreds of thousands of voters' confidential details. The main motive of this breach was to weaken the democratic campaign and ensure the election of Donald trump.⁶

The unsettling part in all of this is that these governments are perceived to be pioneers of dignified authorities who stand for the well-being of their citizens.

Firstly such violating bills or legislations must not be passed or introduced for that matter before the legislature. Secondly, in the context of all the countries around the world, they

⁴Eileen Donahoe & Global Affairs, DIGITAL DISRUPTION OF HUMAN RIGHTS HUMAN RIGHTS WATCH (2016), Visited at <https://www.hrw.org/news/2016/03/25/digital-disruption-human-rights> (last visited May 17, 2020).

⁵ *Id*

⁶ Abigail Abrams, HERE'S WHAT WE KNOW SO FAR ABOUT RUSSIA'S 2016 MEDDLING TIME (2019), Visited at <https://time.com/5565991/russia-influence-2016-election/> (last visited May 17, 2020).

should be introspective and examine their policies which might be counterproductive to the basic democratic principles. The governments around the world should be advocates for adherence to the law because theoretically and in actuality, nobody is above the law.

CONCLUSION

Cyber resilience should be the aim of national security. The Internet is the backbone of all the sectors of the economy and thus it becomes imperative to protect it from the stinging grapevines and unsupervised activities. Governments and corporations all around the globe need to understand that human rights protection is in fact in alignment with their goals. They should at all points ensure their accountability towards the citizens. Acceleration to digital literacy should be given⁷. Citizens should be educated on how to respect the rights and boundaries of the individual while learning more about the tech world.

It will take a collaborative effort to formulate integrated policies, which foster both freedom and security.

Article 3 of Universal human rights declaration provides people the right to security⁸. This attributes to the fact the security of citizens and their rights is of paramount importance. With the introduction of technology, the dynamics of this relationship between the government and the citizens have surely shifted.

However, understanding that human rights protection and digital security should be a shared goal will not only work in their favor individually but help in the burgeoning of the civilization.

This case study is for information purpose only. Nothing contained herein shall be deemed or interpreted as providing legal or investment advice.

⁷ HUMAN RIGHTS IN THE DIGITAL AGE, Visited at <https://www.asser.nl/nnhrr/working-groups/human-rights-in-the-digital-age/> (last visited May 17, 2020).

⁸ Eileen Donahoe & Global Affairs, SO SOFTWARE HAS EATEN THE WORLD: WHAT DOES IT MEAN FOR HUMAN RIGHTS, SECURITY & GOVERNANCE? HUMAN RIGHTS WATCH (2016), Visited at <https://www.hrw.org/news/2016/03/22/so-software-has-eaten-world-what-does-it-mean-human-rights-security-governance> (last visited May 17, 2020).

REFERENCES

1. Abigail Abrams, HERE'S WHAT WE KNOW SO FAR ABOUT RUSSIA'S 2016 MEDDLING TIME (2019),
<https://time.com/5565991/russia-influence-2016-election/> (last visited May 17, 2020).
2. Eileen Donahoe & Global Affairs, DIGITAL DISRUPTION OF HUMAN RIGHTS HUMAN RIGHTS WATCH (2016),
<https://www.hrw.org/news/2016/03/22/so-software-has-eaten-world-what-does-it-mean-human-rights-security-governance> (last visited May 17, 2020).
3. Eileen Donahoe & Global Affairs, SO SOFTWARE HAS EATEN THE WORLD: WHAT DOES IT MEAN FOR HUMAN RIGHTS, SECURITY & GOVERNANCE? HUMAN RIGHTS WATCH (2016),
<https://www.hrw.org/news/2016/03/22/so-software-has-eaten-world-what-does-it-mean-human-rights-security-governance> (last visited May 17, 2020).
4. Human Rights and Technology,
https://www.humanrights.gov.au/sites/default/files/202002/techrights_2019_discussionpaper.pdf (last visited May 17, 2020).
5. HUMAN RIGHTS IN THE DIGITAL AGE,
<https://www.asser.nl/nnhrr/working-groups/human-rights-in-the-digital-age/> (last visited May 17, 2020).
6. Linda Musthaler, FACEBOOK FIASCO HIGHLIGHTS PRIVACY CONCERNS NETWORK WORLD (2008),
<https://www.networkworld.com/article/2281934/facebook-fiasco-highlights-privacy-concerns.html> (last visited May 17, 2020).