
INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

LEGAL ISSUES IN MARKETING THROUGH SOCIAL MEDIA**- Prishita Chadha¹****ABSTRACT**

With the presence of social media transcending and percolating through all possible avenues of an individual's lifestyle, its importance in every other field cannot be overlooked. Marketing, being one of the most dynamic and ever-evolving discipline known to human kind, seems to flourish with the incorporation of social media within its spectrum. The advantages of these two brilliant domains amalgamating is boundless. However, these also lead to generation of multiple legal complications.

In this essay, the author attempts to identify the legal issues that can be found in the interplay between Social Media and Marketing. The expanses of both disciplines converge to form a new sphere of Social Media Marketing, proving to be a viable option for all possible business entities. But the ambiguity accompanying social media, given the lack of uniform provisions, globally, creates new challenges in the wake of effective marketing.

With the identification of distinct but partially overlapping legal issues and summarizing them constructively, the author then tries to identify applicable legal provisions covering the same, within India. Further, the global perspective with respect to the growth in legislation, to contain the functionality and effect of social media marketing is undertaken. The essay ends with offering a possible but in-exhaustive list of measures that can be undertaken by business entities, to avoid any and all lacunae within Social Media Marketing.

The prime objective behind the essay is to attempt and understand the function and lapses in legality within Social Media Marketing.

INTRODUCTION

Social media marketing is an upcoming phenomenon where businesses, small or large, physical

¹ Student of Symbiosis Law School, Noida

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

or online, aspire to seek novel methods to create value for their products or services, or both. With the advent of time and changing patterns of growth of social media, the functionality of social media marketing has changed along with the consumers' behavior. The introduction of multiple technologies in this field, making it a unique platform, has made the participation of consumers much easier and with minimal cost, with its outreach increasing rapidly. Engaging with consumers, promotion of business products and formulation of brands, all using word-of-mouth promotion and collection of real, current but actionable data, has enhanced the utility of social media in the marketing, within a limited period of time, across borders.

Along with creating unprecedented opportunities, social media marketing also leads to the propagation of risks along the way. As a principle, the collection, usage and storage of personal data by the companies must be consented to by the user, in order to avoid violation of privacy in many countries, irrespective of explicit provisions regarding this or not. With the availability of data, the businesses wish to facilitate various promotional activities to suit the attraction of the customers. However, said promotional activities sometimes border on falsity, misleading acts or deception, in furtherance of the analysis of the data acquired by virtue of social media, which surpass the claims of quality and authenticity and instead channel all the resources into merely satisfying the needs of the consumers, superficially. In this process, a number of legal liabilities, issuing from privacy violations and/or breaches on promotion laws, arise, knowingly or unknowingly.

LEGAL ISSUES FACED

Usually, organizations fail to consider the legal ramifications and neglect legal due diligence before they start using social media, because of one of these reasons:

- Lack of awareness regarding the legal complexities of advertising and marketing law.
- Assumed validity of action due to competitor's ignorance.
- Inadequate budget or time for legal check-up by firms.
- Lack of authenticity in establishing online database/lack of authenticity in testimonials.
- Absence of policies and sufficient recourse for such risks.
- Overlooking the need to insure data (cyber insurance)

Due to these reasons for lapse in necessary action, multiple legal issues arise.

The legal risks with social media can be effectively grouped into some overlapping categories:

- Intellectual Property Issues

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

<https://www.ijalr.in/>

- Employment- related Issues
- Marketing Activity Issues

According to the perception of 150 top senior marketing executives in UK, having convened at the IDM (The Institute of Direct Marketing), social media is “more of a risk rather than an opportunity, in marketing”.

Since marketing- related activities can be conveniently carried out with social media tools, using multiple technologies, there is a presence of acute concentration of legal issues. The issues are hence, understood in detail.

1. Trademark and Copyright Issue

The copyrights and trademarks are often nearly as valuable as the products or services offered by the companies and their protection is of utmost importance when using social media to promote brands.² The capacity of social media to facilitate informal, impromptu and often, real-time communication with the consumer base, aides’ companies to promote their brands while disseminating copyrighted material, which includes pictures, audios, videos, text and any virtual data that can be copied³. However, this also exposes the information of said business’ trademarks and copyrights, to an abuse by the third- party. Since there are clashing arenas due to blurred virtual lines in this universe of function, it is difficult to differentiate or stake claim for any piece of information or data given out into the media and therefore, makes this issue sensitive.

As a result, it is advisable to regularly supervise the use of trademarked and copyrighted information, while utilizing social media via third party outlet or company’s own social media platforms, in order to carry out marketing activities and propaganda. This should be done to ensure no misuse of the business’s intellectual property by any other content providing party on the same social media platform. The use of internet monitoring and screening services for checking the availability and use of marked and copyrighted information, being identical or substantially similar to the business’s name or brand, on third- party sites or media platforms provides protection from unsolicited impersonation. If left unchecked, it could lead to damage

² This is imperative, since copyrights and trademarks protect originality of the product/creation to be marketed.

³ All social media platforms facilitate the dissemination of data, in the form of pictures, audios, videos or content by using the copyright/trademark policies. Before agreeing to provide access to the portal, they take assent of the consumers to use, reproduce, modify and distribute their content on the site, for its operation and providing similar service to other users, while the consumers retain the legal rights to any and all information published. The legal disclaimer in the Terms of Service has a contractual obligation along these lines which bind the consumers to subjective limitations. Examples: Terms of Service of Facebook, Instagram, Twitter, Pinterest, etc.

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

of a business's brand and reputation and also serves as a negative indicator of business' success. Almost all the major social media platforms usually explicitly enlist the terms and conditions prohibiting trademark and copyright infringement, specific also to business or person impersonation. For instance, Twitter being involved in a case (*Anthony La Russa v. Twitter, Inc., Case Number CGC-09-488101*)⁴ for impersonation and defamation, going against the policy guidelines of the corporations involved. Procedures allowing reportage of trademark and/or copyright abuse to the outlet, are available on such platforms, which, in turn, are then obligated to take suitable action, sometimes legal, too. Businesses' policy docket, containing terms and conditions for own social media outlets, with specifications enlisting the usage of business' and/or third parties' intellectual property, must accompany the former. The marketing campaigns, especially promotions and user-generated content campaigns, should be guided by rules and prohibitions with respect to trademarks, copyright infringement and impersonation.

2. Privacy Violation

Privacy is a major and upcoming issue regarding data and information of businesses within its external and internal affairs, and is an imperative characteristic for the development of relationships and expanding network. It determines the level of transparency and the extent to which the information is to be retained, thus protecting the virtues of independence, dignity and integrity. While carrying out the research for marketing activities, sometimes entities infringe upon and transcend the privacy boundaries of the consumers, in order to collect the data and build consumer database out of social media activities generating private information. The concept of privacy remains to be a paradox with the consumers wanting their information to be private on one hand and on the other, the businesses wanting to maximize the use of it.

Most companies are subject to privacy laws when it comes to accessing private information of the consumers. In most cases, in case it is necessary to acquire such information, it is done with explicit consent of the consumers, as per the basic guidelines of privacy laid down by the organizations in their marketing manuals and code of conduct. Therefore, the collection, use and disclosure of private information by the public cannot be done by the businesses without complying to the comprehensive yet exhaustive guidelines of the organization regarding privacy, which run parallel to the basic laws related to privacy and upholding of liberty as per

⁴*CGC-09-488101 (state); 3:09-cv-02503-EMC*, Decided by the Superior Court of the State of California: City and County of San Francisco; United States District Court for the Northern District of California. The case highlighted and brought to the fore impersonation issues, which stemmed from a loophole of function in social media portals.

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

the basic elements of any legal structure in a country. Even the simplest forms of regulations concerning the accessing of private information requires consent and full disclosure of purpose by the entity to achieve the same. Apart from ensuring avoidance of unsolicited use of private information of the consumers, the businesses must also encourage privacy protection in its functions.

Unsolicited extraction of information to fulfil the purpose of marketing by businesses not only violates the ethical professional code but, in that spirit, but also goes against the legal sanctions on the upholding of privacy of each and every citizen of a country. The stark violation of privacy guidelines by major social networking platforms, raised with the case of *Max Schrems v. Data Protection Commissioner, CJEU*,⁵ pointed out the information transfer to another country by Facebook for illicit purposes, going beyond the policy. Transfer of user generated content, gathered by social media platforms by evaluating the digital footprint of users and compiling the same to be used for marketing purposes by businesses in partnership with said social media platform goes against the privacy policy of the platform itself. This raises a major privacy concern which should be safeguarded within strict policy formulations by the business itself since this blatantly goes against the concept of consent to access of information so mentioned.

3. Advertising Standards

In the spirit of the ongoing discussion, it is safe to assume that businesses utilize social media to propagate their business activities and marketing strategies. In the global age, due to ever expanding scope of social media and its outreach, businesses focus mostly on using the virtual world for the marketing of their services or products or both, with a guarantee of maximum outreach. From branding to profile building to catching attention of the consumer base, the content posted on social media platforms by any business will usually be considered to be advertising material. Whatever brings to notice the brand of the business facilitates in its marketing or advertising. Therefore, as reliable and convenient as this is, it is also vulnerable to multiple risks which need to be mitigated by the business undertaking such activities.⁶

⁵ Case C-362/14; Decided by Court of Justice of the European Union. The case garnered a lot of attention with regard to the privacy of information and sharing it with third party vendors by the secondary organisation, being the social media interface, for whatever purpose.

⁶In multiple rulings by the Delhi High Court [as in *Horlicks Ltd. v. Heinz India* (2018), *Colgate Palmolive India Ltd v. Hindustan Unilever Ltd.*(2013), *MRF v. Metro Tyres* (2015) and *Dabur India v. Emami* (2015)], concerning comparative and competitive advertisement, albeit resulting in differing conclusions, the ground rule that was the

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

First, the regulation regarding the promotional activities of businesses on social media platforms comes under scrutiny. The most basic way of advertising or promoting any business is to offer sweepstakes or organize contests to allow consumers to avail the products or services without any consideration. For such activities, mostly, the regulations governing them are either overlooked completely or not adequately covered under them, which result in the businesses getting carried away with their promotional activities, like “Refer a friend, text to enter, public judging’, and bordering on violation of cyber laws or gambling laws or both (the elements of ‘chance’ and ‘consideration’). The information or claims made are also sometimes misleading, the need for businesses to formulate proper, strict guidelines by crafting disclosures in safe-constrained posts for undertaking such activities is necessary for a safe implementation of the marketing strategies. Pre- approval of content by the appropriate legal authority also is advisable.

Secondly, the unsolicited promotion by employees on social media, intentional or inadvertent, is also subject to multiple legal sanctions and is a concern for businesses planning to advertise on social media. The pressure on employees to promote their employer business on private social media goes against the basic Labor laws governing the trade employees of any country. The act of publishing content especially for the employees to post on their social media platforms, although pre- approved, facilitated with sanction in case of non- compliance violate multiple privacy clauses and goes against the spirit of employment as per the Labor Laws. On the other hand, unauthorized publishing of vital information of the business on social media by the employees violates the confidentiality clause of employment. The intellectual property of any business is the data or information released into the virtual strata, merely for outreach among the public. This does not have any physical characteristics, since its existence is merely virtual and therefore, the regulations and sanctions on its function are vulnerable to ambiguity. There sometimes arise instances where employees tend to slip confidential information on social media, which might sabotage the brand equity of the business as it is accessible without restriction, thus damaging the intellectual property of the organization.

Thirdly, the content published by businesses on their social media platforms is also subject to regulations. Almost all the social networking platforms allow businesses to furnish information

advertisements must be ‘comparison positive’, which allows the propagation of a basic element of distinguishing factor between products, with the help of advertisements.

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

<https://www.ijalr.in/>

adequate for healthy advertising by implementing standards for information publishing. Age restrictions, user friendly information, target consumer base, etc. are to be kept in mind while accessing social media platforms to advertise the brand in order to avoid any legal issues. These platforms are frequently monitored, not only by the platforms themselves, but also by the businesses themselves, in order to avoid any negative outlook for their business to propagate on the platform. They have the prerogative to control the user base feedback to ensure maximum positive outreach as well.

4. Defamation Issues

While carrying out promotional activities, a horde of information is published, which could attest to any principle of advertisement strategy undertaken by the business. In that process, sometimes businesses undertake to express certain information in a certain way which might mar the reputation of any competitive organization or any other organization carrying out a business. In legal terms, this constitutes as the issue of Defamation. Knowingly or unknowingly, defamation is undertaken when any business validates, in any way, anything negative against any person or group of persons or organization, which could tarnish the reputation or the legal standing/branding of that particular entity.

Under the Indian legal system, Defamation is punishable as a civil or criminal offence. It has multiple complexities, in that regard. Essentially, anything spoken, written or published is considered to be defamation in the legal sense, when it is proved to be damaging and untrue.⁷

Within the ambit of social media, defamation can occur with the slightest of validation, in any form. Apart from publishing comments or data virtually, even the act of sharing a negative expression, originally given by someone else or propagating anything negative in any form and attaching the organization's name to it, thus validating the support of that questionable comment or data, even constitutes as defamation.

The employees of particular organizations are majorly vulnerable to the legal sanctions arising out of this issue. Any form of digital footprint in the form of a picture, text (including texts and E-mails), audio/video, activity or testimony on any social media can face defamation claims. For this, apart from proper scrutiny towards data or information published, the employees need to be made aware of the repercussions in order to avoid such sanctions.

⁷ Section 499 of the IPC criminalise the act of defamation, if it proves to be an imputation of the truth and not done for public good. Section 500 of the IPC provides for a punishment of defamatory acts committed.

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

5. Cheating and Related Fraudulent Activities

Frauds or scams are illegal practices that involve the creation and propagation of fallacious or misleading claims for fueling any financial gain. These activities include exaggeration of the article/product or the qualities that it is sold for, initiating sale of imitation goods by means of advertising for any genuine product or concealing material information about a product. The primary objective of these activities is to get in contact with individuals in order to solicit money or some other item from them, in exchange for something that has little to no value. The essence of a fraud usually involves the promise of delivering a monetary gain, a return on investments, or anything so promised and going back on the same, to create a deficit/lack of fulfilment of the transaction.

Under the Indian legal system, cheating is considered as an activity which was done with explicit intention to deceive⁸. Although, there are multiple technicalities attached to the concept of cheating, essentially, it functions on the intent to carry out wrongful damage to someone, by the means of deception.

There are multiple ways with which frauds are carried out, especially over social media, considering the angle of ambiguity, which provides respite to the fraudsters to execute the act with more precision. Frauds committed using mass media tools are known as mass marketing frauds. These involve disseminating information with the help of media portals, like internet, radio, television broadcasting, print media, etc., in order to trick the people. Under this ambit, social media frauds are also recognized, which involve using the social media platforms to spread false claims in order to facilitate planned fraudulent activities. A rather simple way of online fraud is cheating or misrepresentation, which involves false advertisement claims, false endorsements, using unoriginal/copyrighted photographs or material for furthering own cause and finally, false impersonation. These can be executed in multiple ways, for instance: posting an advertisement of a sale without ensuring sufficient quantity of goods, ensuring a particular percentage of returns on security investments and/or false claims about guarantees of safety, claiming to sell a particular brand of shoes on an online portal which do not match the description on receipt and tricking as an impostor by asking for funding (also includes catfishing⁹ and clickbait scams¹⁰). Cybersquatting, being another one of the many twisted

⁸Sections 415 of the IPC deals with the provision of Cheating and various interpretations attached to it. Although, fraud is not explicitly enlisted within the IPC, its implications are found in Sections 421, 422, 423 and 424 of the IPC.

⁹ Fraudsters lure individuals into an online relationship of sorts, by creating fake online profiles. They attempt to extort money from people or demand personal details, after building trust with individuals.

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

devices, also witnesses the wrongful enrichment of those who use the goodwill of another to their own benefit, by incorporating the details or simply, taking up a well-established name/brand as their own.

Social media platforms are the easiest and therefore, more prone to be inflicted with fraudulent activities, since the scope it recognizes is wider and has open accessibility, therefore transcending global boundaries. Since the extent is larger, more people are likely to come across any piece of information posted online and if in case, said information stands to be illegitimate, the repercussions of the initiated fraud cannot be contained or zeroed down to a particular area. In addition to financial setbacks to consumers, these activities prove to be detrimental to the involved brands or businesses as well, since it taints the reputation and leaves a bad impression.

Recourse, in this case, proves to be difficult, considering the extent of its spread, as mentioned above. However, in many legal structures of countries, there exist provisions for official reporting of such activities, if found and consumer redressal. Otherwise, on behalf of the industry players, being businesses, the prevention can be in the form of disseminating timely and frequent information of such activities to their consumers. Alternatively, it is also a responsibility of the social media platforms to enforce proper measures and avoid these and similar activities to a great extent.

LEGAL RECOURSE

With the adoption of model laws in electronic commerce in 1996, by the United Nations Commission on International Trade Laws (UNCITRAL), the United Nations General Assembly gave recommendations to provide for favorable considerations for the protection of general public and businesses in Resolute No. 51/162, dated January 30, 1997. Considering the model necessary and urgent in 2000, the Government of India enacted the Information Technology Act, 2000.

In the Information Technology Act, 2000, various interfaces of social media can be understood under Section 2(w) as ‘intermediary’, with respect to any particular electronic record, which means “any person who, on behalf of another person, receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, web- hosting service providers, search engines, online payment sites, online

¹⁰ Clickbait scams involve encouraging consumers to pursue links or hidden URLs, camouflaged with prompts of ‘exciting celebrity news’ on social media posts. These lead to exposing the victim’s computer to malware, by taking them to an external site.

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

auction sites, online market places and cyber cafes.” In the capacity of this definition, the government includes social media websites such as Facebook, Twitter, LinkedIn, Instagram, etc. Although attempts have been made to camouflage the crimes undertaken on social media by taking unfair advantage of the ambiguity in the provisions, certain other provisions regulating cybercrimes¹¹ have been introduced in Information Technology Amendment Act, 2008.

The Intellectual Property Rights remained to be the most ambiguous area to be covered under this Act. This has seen years of evolution in the Indian legislature with its importance becoming evident with an uprising of cybercrime in the country. This arena is such that its technicalities and complexities evolve with time and the recognition for the same cannot be implemented in one go. Finally, in 2012, India introduced the Intellectual Property Act, to cover modern copyright issues such as rights management information and technical protection measures. The development of India’s technology sectors, in consonance with intellectual property, remains challenging, with multiple layers to be uncovered and dissected.

A comprehensive outline of certain offences covered under the ambit of social media marketing are:

- Posting of defamatory comments or material against someone- Offence under Section 66 of the IT Act, punishable with imprisonment, damages and/or injunction.¹²
- Posting defamatory material or comment- Criminal defamation under Section 499 of IPC.
- Posting or selling inappropriate material on the internet- Offence under Section 292, 292A, 293, 294 IPC punishable with imprisonment.
- Posting content online by impersonating someone else- Offence under Section 415 and 416 IPC, punishable with imprisonment and/or fine.
- Posting secret information, documents of Government, photographs of prohibited places- Punishable for the violation of Official Secrets Act.
- Posting copied material on the website- Offence under Copyright Act.

¹¹ Further, cybercrime, in layman terms, is understood as something which is a crime committed not by the sole involvement of a person, but is specifically a combination with a computer, too. Simplifying, a cybercrime is any offence or crime in which a computer is used.

¹² Previously liable under Section 66A(c) of the Information Technology Amendment Act, 2008, which has now been adjudged unconstitutional, following the judgement, *Shreya Singhal v. Union of India*, (2013) 12 S.C.C. 73.

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

REPORTING CYBERCRIMES

Since the implications of these online activities mostly result in the commission of cybercrimes, individually or to a combined effect, as can be categorised on the basis of a known premise, the possible definitive legal recourse remains to be the reporting of any related activity, to the concerned authority, as per available provisions.

Section 70-B of the Information Technology Act, 2000 (the “IT Act”) gives the Central Government the power to appoint an agency of the government to be called the ‘Indian Computer Emergency Response Team’. In pursuance of the said provision the ‘Central Government issued the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013’ (the “CERT Rules”) which provide the location and manner of functioning of the ‘Indian Computer Emergency Response Team (CERT-In)’. For Example: Rule 12 (1) (a)¹³, read with Annexure¹⁴ of the CERT Rules gives every person, company or organisation the option to report cyber security incidents to the CERT-In, with an obligation to mandatorily report crimes of certain kind, specifically, as mentioned in the provision.¹⁵

STEPS TO MITIGATE LEGAL RISKS

The implementation of avoidance of legal issues in social media marketing will differ for every organization. However, some general outlines for this are given below:

- Formulation of proper company policy for digital communication and related social media function, both internal and external.
- Terms of usage for users who control and handle the social media platforms of organizations.
- Regular monitoring and moderation of online and social media sites to avoid publishing and perpetuation of inappropriate and unlawful content and removal thereof, in case it exists.

¹³ CERT-in Operations-

(1) Incident reporting, response and information dissemination- CERT – In shall operate an Incident Response Help Desk on 24-hour basis on all days including Government and other public holidays to facilitate reporting of cyber security incidents.

(a) Any individual, organization or corporate entity affected by cyber security incidents may report the incident to CERT-in. the type of cyber security incidents as identified in Annexure shall be mandatorily reported to CERT- In as early as possible to leave scope for action.

¹⁴ Types of incidents to be mandatorily reported to the CERT.

¹⁵ These specific situations, but not exclusive to, include:

- Defacement of website or intrusion into a website and unauthorized changes such as inserting malicious code, links to external websites, etc.;
- Malicious code attacks such as spreading of virus/worm/Trojan/botnets/spyware;
- Identity theft, spoofing and phishing attacks

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

- Allocation of site monitoring responsibilities to individual staff members with adequate answerability and proper reportage.
- Regular staff training on company policy and legal requirements.
- Internally secure digital security measures.
- Online filters to keep out restricted, inappropriate and non- useful data.
- Mandatory breach notification requirement and penalty imposition.
- Creation of properly drafted privacy policy, easily accessible to consumers, with clear outlines for the usage and collection of personal information by the company, unsolicited or not.
- Legal review of campaigns, including obtaining copyright clearances.
- Creation of proper legal team and marketing team and their function in proper tandem.

GLOBAL OPERATION

The internet is a humongous collection of data and related activities, with no visible boundaries to contain it within. It is an ambiguous spread of information, which is constantly expanding, due to an increase in the digital footprint, as digitization spreads across the globe. Personal data is an essential commodity for businesses to function, as it provides a projected ballpark for performance and growth. Since it is so valuable, it is equally, or more vulnerable to being misused. Considering that the regulation of something so vast can be tricky to execute, in the form of a lack of uniform provisions for functionality across borders, issues like those mentioned above, crop up in the simplest of transactions and situations. In that sense, the freedom of access and outreach becomes restricted in many ways.

Against a rising sensitivity among the masses with regard to their personal data and a need to curb the exploitation, a recent and highly commendable development in the digital regulations is the GDPR, or the General Data Protection Regulations¹⁶, which were implemented across the member states of European Union. This step was undertaken to protect the rights and privacy of the consumers, by ensuring standardization and creation of stricter regulations of data collection, processing and mining by the enterprises, to avoid misuse of the same. With the implementation of this across EU nations, their interactions with organizations of other countries was impacted in a sense that required them to be vigilant and attentive to the

¹⁶Came into force across the European Union on 25th May, 2018. The extent of effect of GDPR on the Indian legislation is limited to the transactions/dialogues carried out between Indian Companies and Companies in Countries that recognize GDPR, following certain amendments in the IT Act, in this regard. Although, no specific law to that effect exists in India, the Personal Data Protection Bill, 2019 strives to function along those lines.

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

provisions of this enforcement. Following suit, many non- EU countries¹⁷ have also taken up on the robust data privacy frameworks, offered by the differential implementation of GDPR across EU.

The effect of GDPR in social media marketing can be assessed along the following lines:

1. Availing Data Permissions from Customers

This requires all the consumers to physically assent to the dissemination of any and all personal data that they might be extending to the online entity, being a small-time business or an established organization, thus creating a legal obligation of compliance with the regulations of privacy.

2. Open Data Access to Customers

This shall entail an open access into related databases to customers, limited to the extent of what was provided by them. It also includes altering or removing data, including the consent of usage of the same, per preference.

3. Specific Focus on Data Required

This shall bind the online entities to retrieving only that amount of data as is necessarily required, with a legal justification accompanying the processing of any personal data collected. The only lacuna is that these restrictions are limited to those countries that have a strict implementation of GDPR or any similar regulations. In a country like India, where no proper regulations like these exist, it is very difficult to contain any legal complication flowing from the malpractices carried out over the internet, while even conducting business activities. The only possible expedience, considering the Indian scenario, is stricter legislations, along the lines of GDPR practices.

CONCLUSION

For advertising and marketing endeavors, social networking sites prove to be effective platforms, with marketers increasingly attempting to spread the word about a product or service through advertisements, promotions and other means, using these sites as modus operandi. However, such marketing campaigns unavoidably involve various third parties – including consumers, the social media outlets, marketing affiliates and potentially, other third parties. Therefore, it is imperative for the marketers to be sensitive to the legal issues raised following the involvement of these parties.

¹⁷ The countries whose data protection laws are considered adequate by the EU are Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US.

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

In the 21st Century, with the world functioning at the peak of globalization, people have become more aware of their rights and the exploitation of privacy that they undergo, continually, by virtue of enjoying the benefits and convenience of an open space, courtesy of the internet. However, data is being generated globally at an exponential rate and most countries are not prepared to tackle the issues that accompany the growth.

Specific to social media marketing, the lack of any proper regulation, in India leads to an increase in the propensity of occurrence of cybercrimes, with innocent people falling prey to the evils of internet. The need for a strict legislation arises from the lack of accountability and legitimacy, stemming from a deep and unregulated network functioning in India, in the name of social media interactions over the internet.

BIBLIOGRAPHY

1. Jawahitha Sarabdeen, *Legal Risks in Social Media Marketing*, 4, International Journal of e-Education, e-Business, e-Management and e-Learning,3, (2014).
2. Melissa Landau Steinman and Mikhia Hawkins, *When Marketing Through Social Media, Legal Risks Can Go Viral*, Venable LLP on Online Marketing Law, (2010).
3. Dhruv Gupta, *Cyber Crime and Social Media Marketing*, Bharati Law Review, (2016).
4. Joanna Belby, *Social Media: How to Avoid Trouble with The Law and the FTC*, August 17, 2017, 07:00 AM, www.forbes.com.
5. *Social Media Marketing: The 411 on Legal Risk and Liability*, Smith, Gambrell & Russell LLP, Issue 28, Winter 2010/2011.
6. Kris Ruby, *13 Social Media Mistakes Your Business Is Making That Could Result in Legal Trouble*, July 8, 2017, 6:10AM, www.observer.com.