RABINDRA BHARATI JOURNAL OF PHILOSOPHY
ISSN : 0973-0087

IMPACT OF ARTIFICIAL INTELLIGENCE ON THE CONFIDENTIALITY IN LEGAL PROFESSION.

Asst. Professor **Chaitral K Kotwal** Affiliated Institution TMV's Lokmanya Tilak Law College, Kharghar : chaitralotwal@gmail.com

Abstract

Advocate client privilege is of paramount importance in legal profession. No matter the personal opinion, an advocate must represent his client with his full potential. Also the documents submitted to the advocates and courts are considered as confidential in nature. An advocate cannot sell the brief paper no matter the client left him decades ago. He can destroy it but cannot sell it for commercial value. This is the gravity of confidentiality in this relationship.

There are many AI based software like Lex Machina, Everlaw, Kira etc which are developed to analyze Law, facts, Documents etc and produce expected outcome of a legal proceeding. These softwares consider variety of aspects such as Facts of similar cases, Case Laws, Advocates standing, Judges orientation towards particular types of cases, previous similar cases decided by the court etc. In order to analyze all of it, we must input the details of current case such as facts, Exhibits and Articles, Arguments etc. This all data that we upload is stored in a repository and is used to analyze further cases. The question is how safe is this data stored in the repository. Will it be shown to anyone or just kept locked. Artificial intelligence is designed to learn and develop, as far as possible, like a human brain. We have experience of marketing AI, which people feel, is infringing on their privacy. The question is should that be allowed in legal field.

After analyzing the available data it is observed that many of these softwares mainly focus on the analyzing the legal documents such as contract and assess the risk factor. A few softwares that predict the outcome of a legal proceeding pose no threat to the confidentiality as such. However we must be cautious regarding the development of the AI in legal profession.

Keywords: Artificial intelligence, Advocate-client privilege, confidentiality, Legal Profession, Law.

Introduction

With the development of artificial intelligence it is argued that the security of our personal data is at risk. It has been observed that the artificial intelligence uses the pattern of our online activity and mostly use it to generate revenue by various methods such as popping up ads, suggesting further search option etc. This data collected by the software can be used to further analyze various aspects of human life and behavior. To some extent this type of analyses can help human being but at the same time the question is, is there any limitation on collection and misuse of personal data? It had been debated in recent years that there must be some restriction on the collection of personal data. What should be that 'Laxman Rekha'? It depends upon person to person. However Legal profession is one field where this 'Laxman Rekha' is clearly defined and can be identified. Every communication between an advocate and his client is a privileged and confidential communication as per the law. This communication helps an advocate to strategies his case and cannot be asked to be disclosed even by the court. However there are a few artificial intelligence that claim to frame out successful strategies for a legal case by analyzing various aspects of the same. In order to do that one must input the data in these software. Most of the information provided by a client for a legal case is sensitive, and therefore must be kept confidential. The question is can these software keep it so or will that be used for future analyses of a different matter? While giving the strategy for legal matter, will these software use the sensitive data provided by earlier users? The aim of this research paper is to analyze these software, current legal framework to protect the confidentiality and find out the risk of misuse of this sensitive data by artificial intelligence. Being a qualitative research, data is collected by way of an interview of the expert in the industry.

Confidentiality in legal profession

Indian Evidence Act, 1872, Advocates Act, 1961 and the rules made thereunder protect the confidentiality of communication between an advocate and his client. Sections 126 to 129 of Indian Evidence Act deal with privileged communication attached to professional communication between an advocate and his client. Section 126 of the Act provides the scope of privileges attached to the professional communications between an advocate and his client. It restricts advocates from disclosing any communications exchanged with their client and stating the contents or conditions of documents in possession of the advocate. It also provides certain exceptional grounds on which such privilege shall stand denied, being in furtherance of any illegal purpose or facts coming to the awareness of the advocate showing that either crime or fraud has been committed since the commencement of the advocate's employment on the concerned matter. Section 127 extends the privilege provided under section 126 to the interpreters, clerks and servants of the legal adviser. Section 129 lays down that no one shall be compelled to disclose to the court any confidential communication which has taken place between him and his legal professional advisor, unless he offers himself as a witness.

The Bar Council of India Rules stipulates for all advocates the standards of professional conduct and etiquette. Part VI, Chapter II, Section II, Rule 17 of BCIR stipulates that "An advocate shall not, directly or indirectly, commit a breach of the obligations imposed by Section 126 of the Indian Evidence Act" thus reiterating the spirit of advocate-client privilege, breach of which will also lead to violation of the Bar Council Rules.

Communications between an advocate and client are privileged even if they contain information from third parties. Prohibition of disclosure also extends to any interpreters, clerks or servants of the advocate. While the advocate-client privilege continues even after the employment has ceased, there is no privilege to communications made before the creation of an advocate-client relationship[i]. A breach of the above Rules would subject an advocate to disciplinary proceedings.

Artificial Intelligence

Artificial intelligence is a kind of ability or intelligence of a computer or a robot, which is controlled by another computer to do the task as opposed to how we humans do it. What all tasks humans analyze and do, that capability is being transferred to a machine so that the machine can now itself evolve and get decision making abilities over time. It will be collecting the data, causing the analysis, predict the outcomes using those analyses and based on that it will be taking appropriate actions.

Artificial intelligence is a very broad term as I would say, right. So, if the one is today, if you look at the software world, it is going towards artificial intelligence, from boardrooms to factory floors, from call centers to logistics, everybody is using artificial intelligence for a range of benefits. Even in our own houses today, we can see artificial intelligence being plugged such as an Alexa device, Google assistance etc. This is one such a branch of it, the others are machine learning, neural networks, deep learning etc. But all these deep dive into what we call as artificial intelligence.

The difference between an artificial intelligence and normal data analyses software is that the way they work. Data analyses software collect different kinds of data and based on that the humans would take some kind of action or the software may suggest that it is okay for this particular company to take this action. This software select some data based on that it will predict the revenue of the company over the next 10 years. As opposed to that, artificial intelligence is a bigger concept. It creates intelligent machines that can simulate human thinking capability and behavior. So, it would be intelligent machine, which can think like a human being, which would actually able to learn new things from that data and act on that data by itself. There is no limit on the learning capacity of the machine. How Artificial intelligence works is similar to humans. Artificial intelligence, unlike humans, has the computation power that allows it to process large amounts of data. Therefore, it is continuously learning from experiences, adjusting to the new inputs and performing human like tasks.

Available Artificial Intelligence Tools in Legal Profession

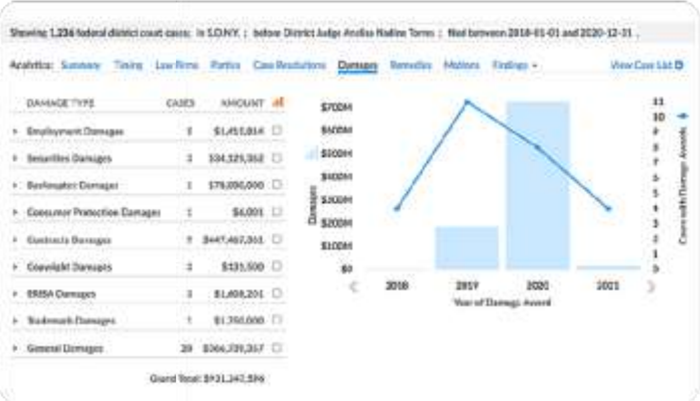
There are many analyzing software which can analyze a legal document such contracts, affidavits and give the desired outputs such as risk assessment, onerous clauses etc. But there are very few softwares which use artificial intelligence and give a strategy for legal proceeding. I studied a few and found most of them use similar strategy. Therefore I am mentioning only one here.

Lex Machina

Lex Machina provides Legal Analytics to law firms and companies, enabling them to craft successful strategies, win cases, and close business. It mines and processes litigation data, combines it and use next-generation artificial intelligence technology to provide analyses.

[ii] It analyzes courts and judges, evaluate opposing counsel, evaluate parties in legal matter and can also craft winning case strategy.

[iii] This AI tool analyzes courts and judges with following considerations:



Showing 1,236 federal district court cases: In S.D.N.Y. ; before District Judge Analisa Nadine Torres ; filed between 2018-01-01 and 2020-12-31

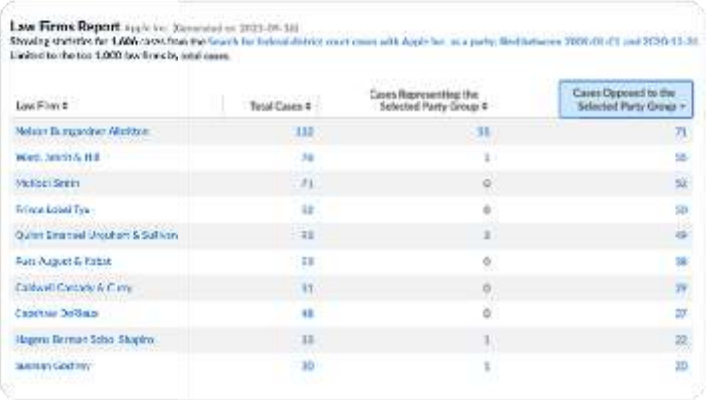
DAMAGE TYPE	CASES	AMOUNT
Employment Damages	1	$1,451,814
Securities Damages	3	$34,325,362
[illegible] Damages	1	$79,000,000
Consumer Protection Damages	1	$6,001
Contracts Damages	7	$447,467,361
Copyright Damages	3	$131,500
ERISA Damages	1	$1,608,201
Trademark Damages	1	$1,350,000
General Damages	29	$366,739,317

Grand Total: $931,342,596

Figure1. Representative sample of analyses output of courts and Judges.[iv]

- How likely is a judge to grant or deny a specific motion?
- How long do cases take to get to a grant of a permanent injunction, to trial, or to termination before a judge?
- How likely is a judge to find infringement of a patent, fair use of a trademark, or a Securities Act violation?
- How long does it usually take for a case to reach termination before Judge Torres?

This AI tool evaluate opposing counsel with following considerations



Law Firms Report Apple Inc. Generated on 2021-06-18

Showing statistics for 1,606 cases from the Search for federal district court cases with Apple Inc. as a party, filed between 2009-01-01 and 2020-12-31

Limited to the top 1,000 law firms by total cases.

Law Firm ⇕	Total Cases ⇕	Cases Representing the Selected Party Group ⇕	Cases Opposed to the Selected Party Group ▾
Nelson Bumgardner Albritton	112	51	71
Ward, Smith & Hill	56	1	55
McKool Smith	71	0	52
Prince Lobel Tye	52	0	50
Quinn Emanuel Urquhart & Sullivan	73	2	49
Russ August & Kabat	73	0	38
Caldwell Cassady & Curry	41	0	39
Capshaw DeRieux	48	0	27
Hagens Berman Sobol Shapiro	33	1	22
Susman Godfrey	30	1	20

Figure2. Representative sample of evaluation output of opposite counsel.[v]

- Opposing counsel’s experience before specific judges and courts,
- Opposing counsel’s client list
- Which law firms have the most experience against opposing counsel?

This AI tool evaluate parties in legal matter with following considerations

Figure3. Representative sample of evaluation output of parties in legal matter.

- Where the party tends to file suit?
- How many lawsuits they have been involved in?
- Their experience before a specific judge
- Whether to consider a transfer of venue?
- How long it may take to litigate your case?[vii]

All artificial intelligence based software in legal field use more or less same technique to give the expected outcome.

Questions and answers

Considering the gravity of advocate client confidentiality and the nature of artificial intelligence, it becomes eminent to ask a few questions before using such artificial intelligence based software. Here are few questions answered by the expert interviewed.

Can artificial intelligence be programmed about data security ethics?
Artificial intelligence is typically programmed to make sure that data breaches and the end privacy is not invaded. But all these things are not hard wired things. Because considering the enormous data that the companies feed into these artificial intelligence driven algorithms, they are susceptible data breaches, all of this data is stored somewhere. Artificial intelligence has some intelligence about much of the data should not be leaked, but it is still susceptible to data breaches.

Is it susceptible on its own or if someone invades the software?
Invading and hacking into the artificial intelligence software and stealing their data are different things altogether. Even the artificial intelligence software is hacked it lead to a data breach. But giant software companies are continuously collecting data and even when we create our social pages, it asks for consent of us to read our messages, to read our call logs and even reading it, majority of the customers click on 'I accept'. There might be a probability that this data is also being sold to other companies. So, that is where we say can that there might be a leak in the data privacy. Both raw data and analyzed data can be leaked this way.
The confidentiality of raw data is dependent on how the software has been built. if they are mature stable software running for a decade or so, and if you could just analyze their path how are they developing the software and how are they making sure that they apply the software patches on top of any kind of third party tools which they are using. Based on how, how good or how well the work they are doing we can say that the security attacks are minimized and that is how their raw data is being protected well.

Does artificial intelligence uses their own mind to collect, analyze and publish data or they're bound by the program code? Are they strictly adhering to their program code or they can develop their own program code to learn more things to collect, analyze and publish the data?
It is proportional to how much of data is being fed into artificial intelligence. Now, if you look at today's examples, where these devices like Alexa, Google Assistant, the kind of data which is being fed to them and how they are programmed, you will see that they are typically learning on how they have been programmed. So, they are not just going ahead and acting on their own calling the user, sending out emails, they don't do that. What they have been doing is the way they have been programmed is how they are responding, but that is what we are talking about in today's time considering the amount of data which has been fed to them, but we do not know in the near future.

Can artificial intelligence be developed to change its own program codes or to develop its own program codes?
Yes. It is another field of AI called as machine learning in which they have the capability of self modifying code, which is one of the techniques which is used in some of the applications of artificial intelligence. But if we consider neural networks, it is basically not writing any kind of code, it is just running through an optimization algorithm that is incrementally changing some coefficients based on certain inputs and you get an output which is close to the desired output. But that is not the case with artificial intelligence, with artificial intelligence there is self modifying code which is written and it is continuously meta programming, reasoning itself continuously and changing its program code itself.

Once we upload the privileged data in the artificial intelligence based software, this data will be kept confidential?

Yes. There are artificial intelligence tools which collect data from various organizations and without disclosing the raw it shares only the outcome. For example there are tools in medical sectors which collect the raw data and shares only probable diagnostic without sharing the previous patients' details.

Therefore the risk of data leakage is really low. But at the same time data selling can happen for which we need strict laws to stop such commercial sale by the parent company. On the other hand the data which is stored by this artificial intelligence in the repository is also subject to external threats but usually they are at a secure location and well protected by firewalls using different kinds of security tools. Such hacking and stealing of data should also be strictly penalized.

Conclusion

Based on the above discussion it can be concluded that artificial intelligence in itself as of now, is not a threat and it can be safely presumed that the information an advocate uploads in these software is not at risk. But at the same time there is a low risk of data leakage. Being an advocate, one must read the terms and conditions or license agreement of the artificial intelligence tool which he proposes to use and assess the risk himself.

While choosing an artificial intelligence tool in legal profession, especially in litigation strategy making, one must, first and foremost consider is security and compliance. There are different kinds of security compliances which are being offered by the government organizations such as Federal Information Processing Standards (FIPS) where there are levels of security to be followed by the companies. There are lots of security practices, which are being documented. And these standards make it sure that there are no weak cryptographic using the software, there are no hashing algorithms that are considered as insecure. One should be looking at what all are the compliancy levels of that software? We could also look at the state compliancy that is to check if those guidelines are followed.

References:

1. Kalikumar Pal v Rajkumar Pal 1931 (58) Cal 1379
2. https://lexmachina.com

[i] Kalikumar Pal v Rajkumar Pal 1931 (58) Cal 1379

[ii] Available at https://lexmachina.com/about/ accessed on 01-02-2022.

[iii] Available at https://lexmachina.com/legal-analytics/ accessed on 01-02-2022.

[iv] Available at https://lexmachina.com/legal-analytics/ accessed on 01-02-2022.

[v] Available at https://lexmachina.com/legal-analytics/ accessed on 01-02-2022.

[vi] Available at https://lexmachina.com/legal-analytics/ accessed on 01-02-2022.

[vii] Available at https://lexmachina.com/legal-analytics/ accessed on 01-02-2022.