23-AESSR-2285-500

Academy of
Education and Social Sciences Review
Vol. 3 No. 2 (May, 2023), 203-212
ISSN (p): 2790-8348 | ISSN (e): 2789-6781
DOI: https://doi.org/10.48112/aessr.v3i2.500

Original Article

Impact of Enactment of 'The Prevention of Electronic Crimes Act, 2016' as Legal Support in Pakistan

Article history:

Received	April 09, 2023
Revised	April 17, 2023
Accepted	April 18, 2023
Published	May 31, 2023

Chen Yongmei
School of International Law, Southwest University of Political Science and Law - China
chenym226@126.com

Jamil Afzal
School of International Law, Southwest University of Political Science and Law - China
sirjamilafzal@gmail.com
https://orcid.org/0000-0002-5640-0578

How to Cite:
Yongmei, C., & Afzal, J. (2023). Impact of enactment of 'The Prevention of Electronic Crimes Act, 2016' as legal support in Pakistan. *Academy of Education and Social Sciences Review, 3*(2), 203-212.
https://doi.org/10.48112/aessr.v3i2.500

Publisher's Note:
International Research and Publishing Academy (*i*RAPA) stands neutral with regard to jurisdictional claims in the published maps and institutional affiliations.

Abstract

This work is based on impact of implementation of digital laws in Pakistan. The focus of this study was on implementation of Digital Laws as Legal support for digital operations in Pakistan. The theoretical conclusions resulting from the work carried out can be used in the development of conceptual concepts of digital laws and its implementation as legal support. The data of three years 2019, 2020 and 2021 is compiled for the analysis, after the implementation of Electronic Crimes Act, 2016. The implementation of Electronic Crimes Act of Pakistan provided positive results. There was a positive change in the number of cases dealt under this law after its implementation. This act is being used as legal tool to solve digital crimes. The analytical results of this research report outcome will stand unlimited influence further study of digital law.

Keywords: digital law, cyber crime, federal investigation agency, cyber bullying law, electronic law

INTRODUCTION

The law which controls the deeds of human beings while doing work on internet is called Digital Law. It means Digital Law prohibits and allows users activities regarding the use of Internet and digital operations (Kerr, 2003). Ethical use of digital law encompasses all the activities which remain in the domain of social laws and unethical use of digital law encompasses all the activities which do not abide by the society law while using internet services (Marwan & Bonfigli, 2022). The main objective of the Digital Law is to educate the people about the theoretical thoughts relating to the Law and Economics issues in the Digital Environment (Smith, 2007). The implementation of proper laws also creates harmony and coexistence among citizens (Afzal, et al., 2022). The violation of Digital law leads to levy of hefty fine and jail. Illegal file sharing sites, pirating software, creating viruses, hacking into systems or networks, stealing someone's identity, and copyright infringement are also included in violations of Digital Law (Rudyk, et al., 2022).

According to Kundi, et al., (2014), the Digital Laws are also called Cyber Laws. The legal rules and regulations that formulate and monitor the use of internet are called Cyber Laws. In the digital economy, the organization aware of digital ethics (trust, honesty, fairness, reliability, credibility, confidentiality and accountability) but also actively implements them is the digital successful organization. The vital role of the digital successful organization is to make decisions that are above the criticisms. We can manage and monitor our digital presence, identity and personal information through Internet Privacy (Afzal, et al., 2023). Without Internet Privacy, anybody can manipulate your information, steal your savings and damage your personality (Fahey, 2022). Cybercrime is a criminal activity that is carried out by using computers and different modern digital gadgets. Cyber criminals use modern internet devices to commit various white-collar crimes such as cyber terrorism, electronic forgery, pornography, personal data leakage, and cyber harassment. In addition, cybercrimes are also involved hacking of government data, financial embezzlement in banking systems, email bombing, and theft of mobile information. These attacks are made without asking permission of their owners (Mazhorina, 2019).

This study has great significance, because this era is era of digitalization. The focus of this study is Implementation of Digital Law as Legal support for digital operations in Pakistan. The main theoretical conclusions resulting from the work carried out can be used in the development of conceptual concepts of digital law and its implementation as legal support. To complete this study, 2019 to 2021 three-year data obtained from official annul reports of Federal Investigation agency (FIA) of Pakistan under Right of Access to Information Act, 2017 of Islamic Republic of Pakistan was used. The work also attempts to understand the legal regulation of digital law from the point of view of digital operations as a legal tool in Pakistan. Significant literature is not yet available on this topic in context of Pakistan, so this study will be a good contribution in this regard. This research work open new research dynamic for further study.

LITERATURE REVIEW

Digital Crimes in Digital Operations

Digital law is used as a tool for E-government, now we are in age of digital operations (Doran, et al., 2023). Herewith, the booming digital era may be secured by the implementation of principles of good governance (Marwan & Bonfigli, 2022). For instance, how to enforce cybercrime laws based on the principles of properness, transparency, accountability, participation, effectiveness, and human rights (Leslie, et al., 2021).

This may apply to other fields, such as e-commerce, financial technology, crypto currency, online media, etc. (Nguyen, 2016). Cyber financial crimes include forgery of debit cards, manipulation of financial transactions, and fraudulent transactions. Cyber criminals use different channels to access the personal information of consumer (Chambers-Jones, 2013). Hacking is another kind of cyber-crime that operates in accessing the personal software and social media platforms to get of private data of banks, individuals, and multinational companies (McGuire & Dowling, 2013).

Cyber bulling is also called online harassment by using different social media means. At includes sharing of personal photos, videos, and other negative information in order to malign this character of someone else (Brenner & Rehberg, 2009). Over the last two years, there have two million exploitative photos of child abuse been uploaded on social media. At must be a sign of alarming concern for people sitting in helm of affairs (Eneman, 2020). Identify theft refers to stealing the personal and private information of any person and use that particular information for fraudulent activities (Grover, et al., 2011). Intellectual property rights are another form of cybercrimes. It refers stealing of ideas, creative materials, and inventions without prior permission of its genuine user. Hackers steal writing materials of books, trademarks of multinational companies and patents. They sell this information to other companies on cheap prices (Wexler, 2018). In Cyber stalking, people use different digital means such as instant messaging, emails, and social media to defame or libel the character of any person. Most of the people use this cheap method for fulfilling the personal and professional prejudice. They post the message or other group discussion on social media to defame the character of their opponents (Goodno, 2007). Without prior permission of his user stealing of personal information, pictures, videos, and any paper work is called data theft (Romanosky, et al., 2011).

Case Study of Pakistan

Cybercrime are considered illegal all over the world and Pakistan has no exception (Zhang, et al., 2012). Cybercrimes rate is very prevalent in Pakistan include illegal data crimes access, forgery of ATM cards, money laundering, the Trojan horse the salami techniques, awful cheques and child pornography. In this regard, the government of Pakistan has established federal investigation agency's cybercrimes in order to eradicate the menace of cybercrime in Pakistan. Federal Investigation Agency (FIA)'s cybercrimes aimed at controlling and investigation electronic crimes being committed by cyber criminals (Bashir & Shahzad, 2021). FIA's deals cybercrimes, such as hacking, cyber terrorism, credit card fraud, and data leakage, and online sex abuse, leakage of warrior's personal videos, online harassment and pornography. The government of Pakistan has passed various acts in order to control the cybercrimes. Such legislation includes prevention of electronic crimes ordinance, 2007, Pakistan telecommunication Act 1996, the prevention of electronic crimes Act 2016, and federal investigation agency act 1979 (Haq, 2019). Following Table 1 represents the division of FIA zone/ circle used in this study.

Table 1

Division of FIA Zone/Circle

Zone for Cyber Crime Reporting in Pakistan			
No.	***Name of Circle***	***Zone Number***	***Province***
1	Lahore	Zone-I	Punjab
2	Karachi	Zone-II	Sindh
3	Rawalpindi	Zone-III	Punjab
4	Peshawar	Zone-IV	KPK
5	Quetta	Zone-V	Balochistan
6	Islamabad	Zone-VI	Islamabad
7	Abbottabad	Zone-VII	KPK
8	D.I Khan	Zone-VIII	KPK
9	Gujranwala	Zone-IX	Punjab
10	Faisalabad	Zone-X	Punjab
11	Multan	Zone-XI	Punjab
12	Hyderabad	Zone-XII	Sindh
13	Sukkur	Zone-XIII	Sindh
14	Gawadar	Zone-XIV	Balochistan
15	Gilgit	Zone-XV	Balochistan

Right now, cyber financial crimes are very deep rooted in Pakistan (Nawaz, et al., 2002). Over the last three years, cyber financial crimes have increased by 83 percent in Rawalpindi and Faisalabad. The federal investigation agency has registered 62,357 complaints regarding online financial embezzlement and access of data of criminals. Different social media companies and cellular companies do not cooperate with FIA's cyber need to establish a mutual legal assistance all out information for solving a case. In Pakistan, hacking is relatively new type of cybercrimes for the federal investigation agencies (Imran, et al., 2019). Cybercrimes wing has lodged 1576 complaints of banking sector in 2022. By using the persona information of ordinary citizens, hackers harass other citizens by asking them for money, emergency loans, and online transactions (Shad, 2019). Likewise Cyber bulling has become very common in teenagers of Pakistani society (Rafi, 2019). The federal investigation agency has established a separate cell to launch complains against online blackmailing have been registered under the prevention of electronic crimes Act (PECA) in Pakistan (Ahmad, 2019). In addition, FIA has received 4,441 cases of online blackmailing in 2021.

It is sad to learn that only five cases have been finalized against 343 cases of child pornography in Pakistan. Low consecutive rate is a main cause for rise in exponential rise in cybercrimes in Pakistan. Identify theft is a common practice; people use the personal information of renowned personalities in order to attract people's attention. Criminals use that information for asking money to people's near and dear ones (Rafiq, 2019). Cyber stalking is another form of cybercrime very prevalent in Pakistan. Pakistan has very strict legislation to counter the menace. Under the prevention of electronic crimes Act 2016, the court can order seven years imprisonment or fine up to 5 million. Data theft is also very common practice in Pakistani society. FIA's cybercrimes wing receives thousands of complaints annually. Criminal's steals information with the intent to get bank account information, and property information very recently, FIA has arrested eight officials of NADRA and phone franchises being involved in selling peoples vital information to cyber criminals. In addition, cyber criminals are also using Benazir income support programs platform to obtain personal information of ordinary citizens. Through a phone call, they ask people to share their information related to bank, property and workplace (Usman, 2017). This government should sensitize citizens to be vigilant regarding data theft fraud.

METHODOLOGY

The data used in this case study is obtained from official annul reports of Federal Investigation agency (FIA) of Pakistan under Right of Access to Information Act, 2017 of Islamic Republic of Pakistan. Table 2 represents the digital crimes cases reported and executed under the digital laws with effect from 1st January 2019 to 31st December 2021 in Pakistan.

Table 2

Overview of Reported Cases

Year	Zone-Wise	Previous Cases	New Cases	Total Cases	Disposed off / Transferred	Pending Cases	% of cases increased
	Zone-I	***1394***	***2048***	***3442***	***721***	***2721***	***59.50***
Year 2019 (01.01.2019 to 31.12.2019)	Zone-II	668	515	1183	343	840	43.53
	Zone-III	505	723	1228	683	545	58.88
	Zone-IV	447	742	1189	360	829	62.41
	Zone-V	176	220	396	89	307	55.56
	Zone-VI	42	202	244	116	128	82.79
	Zone-VII	84	227	311	92	219	72.99
	Zone-VIII	47	193	240	46	194	80.42
	Zone-IX	366	637	1003	569	434	63.51
	Zone-X	306	620	926	170	756	66.95
	Zone-XI	218	575	793	86	707	72.51
	Zone-XII	0	47	47	8	39	100.00
	Zone-XIII	13	68	81	10	71	83.95
	Zone-XIV	0	0	0	0	0	0.00
	Zone-XV	0	2	2	0	2	100.00
	Total	***4266***	***6819***	***11085***	***3293***	***7792***	***61.52***
Year 2020 (01.01.2020 to 31.12.2020)	Zone-I	2721	2979	5700	2568	3132	52.26
	Zone-II	840	641	1481	697	784	43.28
	Zone-III	545	823	1368	1124	244	60.16
	Zone-IV	829	1285	2114	1221	893	60.79
	Zone-V	307	198	505	248	257	39.21
	Zone-VI	128	402	530	312	218	75.85
	Zone-VII	219	229	448	352	96	51.12
	Zone-VIII	194	191	385	214	171	49.61
	Zone-IX	434	946	1380	1052	328	68.55
	Zone-X	756	402	1158	923	235	34.72
	Zone-XI	707	675	1382	565	817	48.84
	Zone-XII	39	173	212	128	84	81.60
	Zone-XIII	72	106	178	136	42	59.55
	Zone-XIV	0	0	0	0	0	0.00
	Zone-XV	2	62	64	29	35	96.88
	Total	***7793***	***9112***	***16905***	***9569***	***7336***	***53.90***
Year 2021 (01.01.2021 to 31.12.2021)	Zone-I	3131	4701	7832	2535	5297	60.02
	Zone-II	784	801	1585	288	1297	50.54
	Zone-III	271	1591	1862	1030	832	85.45
	Zone-IV	893	1992	2885	700	2185	69.05
	Zone-V	257	299	556	440	296	53.78
	Zone-VI	215	1238	1453	646	807	85.20
	Zone-VII	96	249	345	215	130	72.17
	Zone-VIII	152	299	451	275	176	66.30
	Zone-IX	421	1210	1631	891	740	74.19
	Zone-X	235	1557	1792	1102	690	86.89
	Zone-XI	592	1350	1942	953	989	69.52
	Zone-XII	84	211	295	99	196	71.53
	Zone-XIII	42	125	167	52	115	74.85
	Zone-XIV	0	0	0	0	0	0.00
	Zone-XV	34	143	177	107	70	80.79
	Total	***7207***	***15766***	***22973***	***9333***	***13820***	***68.63***

After the enactment of new digital law in Pakistan which in known as 'Electronic Crimes Act, 2016 (The Gazette of Pakistan, August 22, 2016 Part. I)', the statistical data shows that there was positive change in the

cases dealt under this digital law. According to table number 2, number of cases was increased from 4266 to 11085 in year 2019 with effect from 1st January 2019 to 31st December 2019. There was the addition of 6819 registered cases by the virtue of digital law. Same situation was observed in the year 2020, the number of cases was increased from 7793 to 16905, and there was addition of 9112 new complain/ cases. Likewise, for the year 2021, the number of cases was also increased from 7207 to 22973. There was a notable increment of 15766 cases.

Figure 1 is the graphical representation of the cases dealt in 2019 under the Electronic Crimes Act, 2016 of Pakistan. Whereas Series1 stands for Pervious Cases, Series2 for New Cases, Series3 for Total Cases, Series4 for Disposed Off/ Transferred /Solved Cases, Series5 for Pending Cases and Series6 for Percentage of cases increased. The graphical representation shows the positive trend in registered cases after the enactment of digital law. The 61.51% increment in registered cases was recorded to control the digital operations all over the Pakistan.

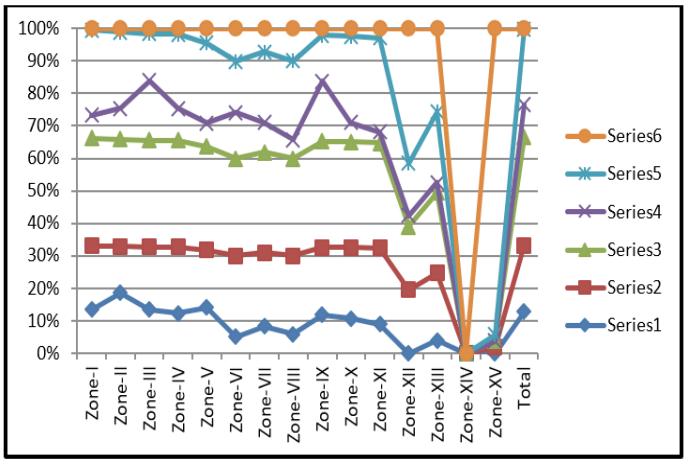

Figure. 1. Represents Data Analysis of Year 2019

Figure 2 is the graphical representation of the cases dealt in 2020; the graphical representation also shows the positive trend towards digital law. The sum of 53.90% was increment of registered cases dealt under digital law in the year 2020.

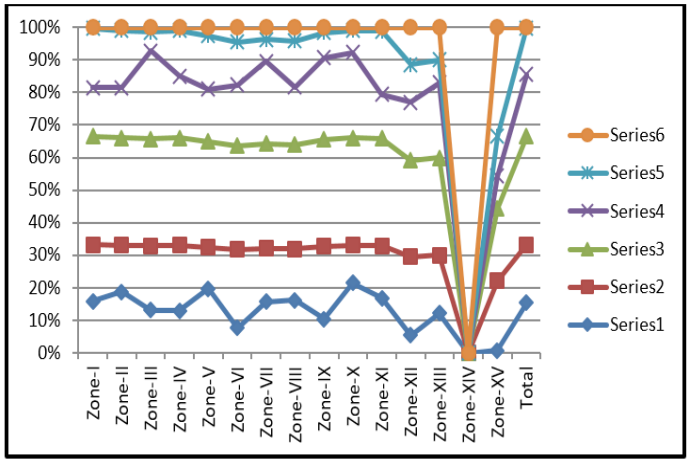

Figure. 2. Represents Data Analysis of Year 2020

Likewise, Figure 3 is the graphical representation of the cases dealt in 2021; the graphical representation also shows the positive trend towards this digital law. The sum of 68.62% was increment of registered cases under digital law in this year.

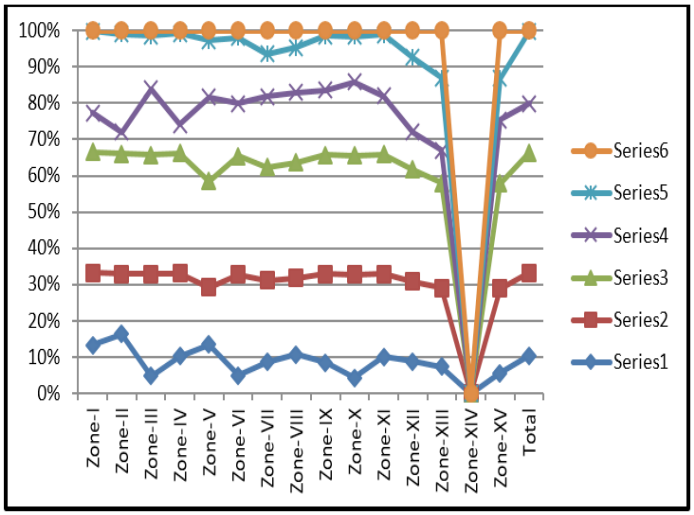

Figure. 3. Represents Data Analysis of Year 2021

Table 3 represents the statistical figures of cases disposed off/ transferred / solved by the virtue of digital law in Pakistan.

Table 3

Representation Percentage of Solved Cases

No.	Year	New Cases	Total Cases	Disposed off / Transferred / Solved	Percentage of solved cases
1	2019	6819	11085	3293	29.70
2	2020	9112	16905	9569	56.60
3	2021	15766	22973	9333	40.62

According to the data represented in table number 3, there was a remarkable increment in the solved cases percentage in 2020 as compare to 2019. The percentage in 2019 was 29.70, whereas in 2020 was 56.60. Nevertheless, in 2021 percentage were less than 2020; however, it was greater than 2019. The percentage of 2021 was 40.62, the COVID-19 and lockdown situation was the reason behind this decrease in percentage. It is clear from the Figure 4 that, there was handsome increment in registered cases after enactment of subject matter digital law in 2019, 2020 and 2021.

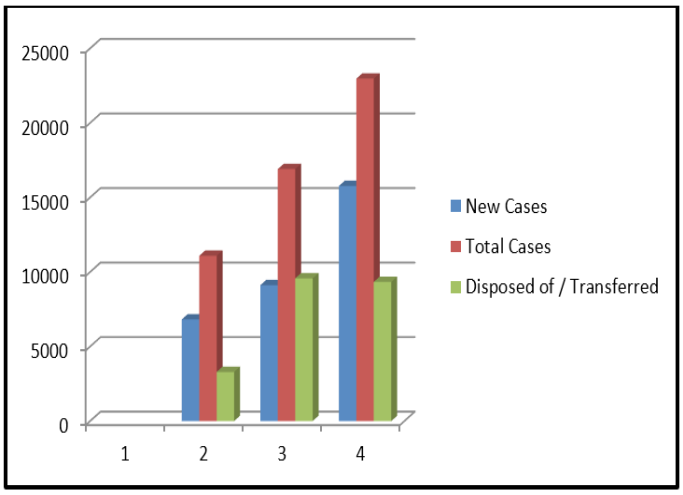

Figure. 4. Graphical representation of solved cases

CONCLUSION & RECOMMENDATIONS

Digital Law prohibits and allows users activities regarding the use of Internet and digital operations. Ethical use of digital law encompasses all the activities that remain in the domain of social laws and unethical use of digital law encompasses all the activities that do not abide by the society law while using internet services, the booming digital era may be secured by the implementation of principles of good governance by virtue

of digital laws' implementation.

To conclude we can say that the enactment of digital law provided positive results to register and solve the cybercrimes cases in Pakistan. The Electronic Crimes Act, 2016, was the digital law implemented in Pakistan to regulate the digital operations and deeds. By the virtue of this digital law, in 2019 the registered cases under this law was increased from 4266 to 11085 and in 2020 there was addition of 9112 new complain/ cases. Likewise, for the year 2021, the number of cases was also increased from 7207 to 22973. There was a notable increment in cases as 15766. The study also proves that by using digital law as a legal tool, there was a remarkable increment in the percentage of solved / disposed of cases in Pakistan. The analytical results of this research outcome will stand unlimited influence on further study of digital law.

Competing Interest

The authors have declared no competing interest.

References

Afzal, J., Lumeng, W., & Aslam, M. (2022). Assessment of tolerance, harmony and coexistence: A study on university students in Government College University, Faisalabad. *Siazga Research Journal, 1*(1), 06-10.
https://doi.org/10.58341/srj.v1i1.6

Afzal, J., Munir, M., Naz, S., Qayum, M., & Noman, M. (2023). Relationship between organizational silence and commitment of employees at university level. *Siazga Research Journal, 2*(1), 58-65.
https://doi.org/10.58341/srj.v1i2.9

Ahmad, A. A. M. D. A. (2019). Deficiencies In peca and proposed amendments to facilitate investigating agencies, courts and prosecution; proper use of electronic devices for effective implementation of law. *International Journal for Electronic Crime Investigation, 3*(3), 6-6.
https://doi.org/10.54692/ijeci.2020.030338

Bashir, S., & Shahzad, F. (2021). Federal investigation agency against the crime of book piracy in Pakistan. *Library Philosophy and Practice (e-journal*). 5034.

Brenner, S. W., & Rehberg, M. (2009). Kiddie crime-the utility of criminal law in controlling cyberbullying. *First Amend. L. Rev.,* 8, 1.
https://doi.org/10.2139/ssrn.1537873

Chambers-Jones, C. (2013). Cyber economic crime and commonwealth laws. *International Journal of Intellectual Property Management 7*, 6(1-2), 95-110.
https://doi.org/10.1504/ijipm.2013.053451

Doran, N. M., Puiu, S., Bădîrcea, R. M., Pirtea, M. G., Doran, M. D., Ciobanu, G., & Mihit, L. D. (2023). E-government development—A key factor in government administration effectiveness in the European Union. *Electronics, 12*(3), 641.
https://doi.org/10.3390/electronics12030641

Eneman, M. (2020). Crime investigations of 'child abuse material': Challenges and opportunities posed by digital technologies. *AoIR Selected Papers of Internet Research*.
https://doi.org/10.5210/spir.v2020i0.11210

Fahey, E. (2022). *Developing EU cybercrime and cybersecurity on legal challenges of EU institutionalisation of cyber law-making*. The Routledge Handbook of European Integrations, 270-284.
https://doi.org/10.4324/9780429262081-20

Goodno, N. H. (2007). Cyberstalking, a new crime: Evaluating the effectiveness of current state and federal laws. *Mo. L. Rev., 72,* 125.

Grover, A., Berghel, H., & Cobb, D. (2011). The state of the art in identity theft. *Advances in Computers, 83,* 1-50.
https://doi.org/10.1016/b978-0-12-385510-7.00001-1

Haq, Q. A. U. (2019). Cyber security and analysis of cyber-crime laws to restrict cyber crime in Pakistan. *International*

Journal of Computer Network and Information Security, 11(1), 62.
https://doi.org/10.5815/ijcnis.2019.01.06

Imran, M., Faisal, M., & Islam, N. (2019). Problems and vulnerabilities of ethical hacking in Pakistan. In *2019 Second International Conference on Latest trends in Electrical Engineering and Computing Technologies* (INTELLECT) (pp. 1-6). IEEE.
https://doi.org/10.1109/intellect47034.2019.8955459

Kerr, O. S. (2003). The problem of perspective in Internet law. *Georgetown Law Journal, 9*1(2), 357.

Kundi, G. M., Nawaz, A., Akhtar, R., & MPhil Student, I. E. R. (2014). Digital revolution, cyber-crimes and cyber legislation: A challenge to governments in developing countries. *Journal of Information Engineering and Applications, 4*(4), 61-71.

Leslie, D., Burr, C., Aitken, M., Cowls, J., Katell, M., & Briggs, M. (2021). Artificial intelligence, human rights, democracy, and the rule of law: a primer. *arXiv preprint arXiv:*2104.04147.
https://doi.org/10.2139/ssrn.3817999

Marwan, A., & Bonfigli, F. (2022). Detection of digital law issues and implication for good governance policy in Indonesia. *BESTUUR, 10*(1), 22-32.
https://doi.org/10.20961/bestuur.v10i1.59143

Mazhorina, M. V. (2019). Digital platforms and international private law, or is there a future for cyber law?. *Lex russica,* (2), 107-120.
https://doi.org/10.17803/1729-5920.2019.147.2.107-120

McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. Summary of key findings and implications. *Home Office Research report, 75,* 1-35.

Nawaz, S., McKinnon, R., & Webb, R. (2002). Informal and formal money transfer networks: Financial service or financial crime?. *Journal of Money Laundering Control, 5*(4), 330-337.
https://doi.org/10.1108/eb027315

Nguyen, Q. K. (2016). Blockchain-a financial technology for future sustainable development. In *2016 3rd International conference on green technology and sustainable development* (GTSD) (pp. 51-54). IEEE.
https://doi.org/10.1109/gtsd.2016.22

Rafi, M. S. (2019). Cyberbullying in Pakistan: Positioning the aggressor, victim, and bystander. *Pakistan Journal of Psychological Research, 34(*3), 601-620.
https://doi.org/10.33824/pjpr.2019.34.3.33

Rafiq, A. (2019). Challenges of securitising cyberspace in Pakistan. *Strategic Studies, 39*(1), 90-101.
https://doi.org/10.53532/ss.039.01.00126

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft?. *Journal of Policy Analysis and Management, 30*(2), 256-286.
https://doi.org/10.1002/pam.20567

Rudyk, N. V., Niyazbekova, S. U., Yessymkhanova, Z. K., & Toigambayev, S. K. (2022). Development and regulation of the digital economy in the context of competitiveness. In *Cooperation and Sustainable Development* (pp. 167-174). Springer International Publishing.
https://doi.org/10.1007/978-3-030-77000-6_20

Shad, M. R. (2019). Cyber threat landscape and readiness challenge of Pakistan. *Strategic Studies, 39*(1), 1-19.
https://doi.org/10.53532/ss.039.01.00115

Smith, G. J. (Ed.). (2007). *Internet law and regulation*. Sweet & Maxwell.

Usman, M. (2017). cyber crime: Pakistani perspective. *Islamabad Law Review, 1*(03), 18-40.

Wexler, R. (2018). Life, liberty, and trade secrets: Intellectual property in the criminal justice system. *Stanford Law*

Review, 70(5), 1343-1429.

https://doi.org/10.2139/ssrn.2920883

Zhang, Y., Xiao, Y., Ghaboosi, K., Zhang, J., & Deng, H. (2012). A survey of cyber crimes. *Security and Communication Networks, 5*(4), 422-437.

https://doi.org/10.1002/sec.331