SYMBIOSIS
INSTITUTE OF GEOINFORMATICS
॥वसुधैव कुटुम्बकम्॥

Project Report

On

"Cyber Crimes in India: A Crime Head-wise and State/UT-wise Analysis of Incidences during 2020"

Submitted

By

Name: ***Kinjal Bandopadhyay***

PRN: ***22070243028***

Department: ***Data Science***

Course: M.Sc. ***Data Science and Spatial Analytics***

Subject: ***Data Driven Governance***

Date of Submission: **31st January, 2023**

Declaration:

I**, Mr. Kinjal Bandopadhyay**, declare that this project report entitled **"Cyber Crimes in India: A Crime Head-wise and State/UT-wise Analysis of Incidences during 2020"** is a result of my own work and is submitted in partial fulfilment of the requirements for the award of **Masters of Data Science & Spatial Analytics**. I have followed all academic and ethical guidelines in the preparation of this report and have not plagiarized any material from any sources. I have also acknowledged all sources used in the preparation of this report.

This report is being submitted to **Mrs. Moushmi Dasgupta**, **Data Science**, **Symbiosis Institute of Geoinformatics, Pune**.

Kinjal Bandopadhyay

[22070243028]

ABSTRACT

This study aims to analyse the trend of cybercrime in 2021 across different states in the country. Data was collected from various sources, including law enforcement agencies, to provide an overview of the type and frequency of cybercrime in each state. The findings of the study showed that cybercrime incidents varied widely between states, with some states experiencing higher levels of cybercrime compared to others. Additionally, certain types of cybercrime were found to be more prevalent in specific states. The study highlights the need for state-specific policies and strategies to tackle cybercrime and provides valuable insights for law enforcement agencies and policy makers in their efforts to prevent and combat cybercrime.

INTRODUCTION

The digital age has brought about numerous advancements and conveniences, but it has also given rise to new forms of crime, one of which is cybercrime. With the increasing use of technology, the threat of cybercrime is also increasing. India is no exception to this growing concern, as the country has seen a surge in the number of cybercrime cases in recent years.

In light of this growing concern, the present analysis report focuses on the " Crime Head-wise and State/UT-wise cyber-crimes during 2020". The report aims to provide a comprehensive picture of the extent and nature of cybercrime in India, with a specific focus on the number of reported cases in each state/union territory in 2020. The report will provide valuable insights into the trend of cybercrime across the country and highlight areas that may require increased attention and resources.

The report is based on the official data on cybercrime in India and provides an in-depth analysis of the data to draw meaningful conclusions. The findings of this report will be useful for policy makers, law enforcement agencies, and individuals alike in taking steps to prevent and mitigate the impact of cybercrime in India.

Data Source:

The data is collected from website of Indian Government: https://data.gov.in/

Link to the data sets used:

https://data.gov.in/resource/crime-head-wise-stateut-wise-cyber-crimes-during-2020.

Why I have selected this dataset:

With the increasing use of technology and the rise of cybercrime, understanding the state of cybercrime in India is of utmost importance. This dataset provides a detailed picture of the extent and nature of cybercrime in India, with a specific focus on the number of reported cases in each state/union territory in 2020.This dataset is up-to-date and relevant, as it covers the year 2020, a time when the use of technology was greatly impacted by the COVID-19 pandemic. The dataset provides data on the number of reported cybercrime cases in each state/union territory of India, allowing for a comprehensive analysis of the trend of cybercrime across the country. The insights from this analysis can be used by policy makers and law enforcement agencies to develop strategies to prevent and mitigate the impact of cybercrime in India. This report will raise awareness among individuals about the types of cybercrime that are prevalent in their state/union territory and provide them with information on how to protect themselves.

Overall, the " Crime Head-wise and State/UT-wise cyber-crimes during 2020" dataset is a valuable resource for understanding the state of cybercrime in India and taking steps to prevent and mitigate its impact.

Uniqueness of this dataset:

This dataset provides a comprehensive overview of cybercrime in India in the year 2020, broken down by state/union territory. It includes different categories of cybercrime such as computer-related offences, cybercrime offences under the Information Technology (IT) Act, crimes under the Indian Penal Code (IPC) involving communication devices, and cybercrime offences under the Special Laws (SLL) involving communication devices. This dataset is unique in that it provides a state/UT-wise analysis of cybercrime, which allows for a deeper understanding of the distribution of cybercrime across India and helps identify areas that may require additional resources or attention to tackle the issue. Additionally, the inclusion of different categories of cybercrime provides a comprehensive understanding of the nature and types of cybercrime incidents in India.

Libraries used for the Analysis:

```
import numpy as np
import pandas as pd
import matplotlib.pyplot as plt
import plotly.express as px
import json
```

Importing the data and storing it into a data frame:

```
df=pd.read_csv("NCRB_CII-2020_Table.No-9A.2.csv")
df.head()
```

	Si. No (Col. 1)	Category	State/UT (Col. 2)	A. Offences under I.T. Act - Tampering Computer Source documents (Sec.65) - (Col. 3)	A. Offences under I.T. Act - Computer Related Offences - Computer Related Offences (Total) - (Col. 4)	A. Offences under I.T. Act - Computer Related Offences - Computer Related Offences (Sec.66) - a1) Ransom-ware - (Col. 6)	A. Offences under I.T. Act - Computer Related Offences - Computer Related Offences (Sec.66) - a2) Offences other than Ransom-ware - (Col. 7)	A. Offences under I.T. Act - Computer Related Offences - B) Dishonesty receiving stolen computer resource or communication device (Sec.66B) - (Col. 8)	A. Offences under I.T. Act - Computer Related Offences - C) Identity Theft (Sec.66C) - (Col. 9)	A. Offences under I.T. Act - Computer Related Offences - D) Cheating by personation by using computer resource (Sec.66D) - (Col. 10)	...	B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Fake News on Social Media (Sec.505) - (Col. 42)	B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Other Offences (r/w IT Act) - (Col. 43)
0	1	State	Andhra Pradesh	3	224	0	3	1	48	164	...	106	152
1	2	State	Arunachal Pradesh	0	23	0	0	0	21	1	...	0	0
2	3	State	Assam	10	1500	0	126	14	154	1160	...	0	197
3	4	State	Bihar	0	16	0	4	0	4	8	...	5	23
4	5	State	Chhattisgarh	0	20	0	3	1	8	8	...	1	80

Total Offences under IPC - (Col. 44)	C. Offences under SLL (Involving Communication Devices as Medium/ Target) r/w IT - Gambling Act (Online Gambling) - (Col. 45)	C. Offences under SLL (Involving Communication Devices as Medium/ Target) r/w IT - Lotteries Act (Online Lotteries) - (Col. 46)	C. Offences under SLL (Involving Communication Devices as Medium/ Target) r/w IT - Copy Right Act, 1957 - (Col. 47)	C. Offences under SLL (Involving Communication Devices as Medium/ Target) r/w IT - Trade Marks Act, 1999 - (Col. 48)	C. Offences under SLL (Involving Communication Devices as Medium/ Target) r/w IT - Other SLL Crimes - (Col. 49)	- Total Offences under SLL - (Col. 50)	Total Cyber Crimes (IT Act + IPC r/w IT Act + SLL r/w IT Act) - (Col. 51)
1572	0	4	0	0	0	4	1899
3	0	0	0	0	0	0	30
693	0	0	0	0	0	0	3530
1416	0	0	4	0	1	5	1512
166	0	0	0	0	0	0	297

We have employed a method for our own convenience in order to determine the correlation and carry out additional operations on the dataset. Because we have 52 columns, it is not possible to find the correlation of the original dataset, so this is what we have done, we have accumulated all the different types of offences that comes under computer related offences into one column and the same thing is done for the offences under SLL (Involving Communication Devices as Medium/Target) related to IT Act, Offences under I.T. Act, IPC Crimes (Involving Communication Devices as Medium/Target or r/w IT Act) in different states/UTs in India, where all the offences are accumulated and placed into the corresponding distinct columns and then the columns which were accumulated into one column are dropped from the dataset as shown below.

Code to add up all the columns that comes under computer related offences and place them into one column, then drop all other columns which comes under this category:

df['Computer Related Offences']=df['A. Offences under I.T. Act - Computer Related Offences - Computer Related Offences (Total) - (Col. 4)']+df['A. Offences under I.T. Act - Computer Related Offences - Computer Related Offences (Sec.66) - a1) Ransom-ware - (Col. 6)']+df['A. Offences under I.T. Act - Computer Related Offences - B) Dishonesty receiving stolen computer resource or

communication device (Sec.66B) - (Col. 8)']+df['A. Offences under I.T. Act - Computer Related Offences - Computer Related Offences (Sec.66) - a2) Offences other than Ransom-ware - (Col. 7)']+df['A. Offences under I.T. Act - Computer Related Offences - C) Identity Theft (Sec.66C) - (Col. 9)']+df['A. Offences under I.T. Act - Computer Related Offences - D) Cheating by personation by using computer resource (Sec.66D) - (Col. 10)']+df['A. Offences under I.T. Act - Computer Related Offences - E) Violation of Privacy (Sec.66E) - (Col. 11)']

df = df.drop(columns=['A. Offences under I.T. Act - Computer Related Offences - Computer Related Offences (Total) - (Col. 4)','A. Offences under I.T. Act - Computer Related Offences - Computer Related Offences (Sec.66) - a1) Ransom-ware - (Col. 6)','A. Offences under I.T. Act - Computer Related Offences - Computer Related Offences (Sec.66) - a2) Offences other than Ransom-ware - (Col. 7)','A. Offences under I.T. Act - Computer Related Offences - B) Dishonesty receiving stolen computer resource or communication device (Sec.66B) - (Col. 8)','A. Offences under I.T. Act - Computer Related Offences - C) Identity Theft (Sec.66C) - (Col. 9)','A. Offences under I.T. Act - Computer Related Offences - D) Cheating by personation by using computer resource (Sec.66D) - (Col. 10)','A. Offences under I.T. Act - Computer Related Offences - E) Violation of Privacy (Sec.66E) - (Col. 11)'])

Code to add up all the columns that comes under offences under I.T Act and place them into one column, then drop all other columns which comes under this category:

df['Offences under I.T. Act']=df['A. Offences under I.T. Act - Tampering Computer Source documents (Sec.65) - (Col. 3)']+df['A. Offences under I.T. Act - Cyber Terrorism (Sec.66 F) - (Col. 12)']+df['A. Offences under I.T. Act - Publication/ transmission of obscene / sexually explicit act in electronic form (Sec. 67) - Publication/ transmission of obscene / sexually explicit act in electronic form (Total) - (Col. 13)']+df['A. Offences under I.T. Act - Publication/ transmission of obscene / sexually explicit act in electronic form (Sec. 67) - A) Publishing or transmitting obscene material in Electronic Form - (Col. 14)']+df['A. Offences under I.T. Act - Publication/transmission of obscene / sexually explicit act in electronic form (Sec. 67) - B) Publishing or transmitting of material containing Sexually explicit act in electronic form (Sec.67A) - (Col. 15)']+df['A.

Offences under I.T. Act - Publication/transmission of obscene / sexually explicit act in electronic form (Sec. 67) - C) Publishing or transmitting of material depicting children in Sexually explicit act in electronic form (Sec.67B) - (Col. 16)']+df['A. Offences under I.T. Act - Publication/transmission of obscene / sexually explicit act in electronic form (Sec. 67) - D) Preservation and retention of information by intermediaries (Sec.67C) - (Col. 17)']+df['A. Offences under I.T. Act - Publication/transmission of obscene / sexually explicit act in electronic form (Sec. 67) - E) Other sub- sections of Sec. 67 IT Act - (Col. 18)']+df['A. Offences under I.T. Act - Publication/transmission of obscene / sexually explicit act in electronic form (Sec. 67) - (Col. 19)']+df['A. Offences under I.T. Act - Un-authorized access/attempt to access to protected computer system (Sec.70) - (Col. 20)']+df['A. Offences under I.T. Act - Abetment to Commit Offences (Sec.84 B) - (Col. 21)']+df['A. Offences under I.T. Act - Attempt to Commit Offences (Sec.84C) - (Col. 22)']+df['A. Offences under I.T. Act - Other Sections of IT Act - (Col. 23)']+df['Total Offences under I.T. Act - (Col. 24)']

df = df.drop(columns=['A. Offences under I.T. Act - Tampering Computer Source documents (Sec.65) - (Col. 3)','A. Offences under I.T. Act - Cyber Terrorism (Sec.66 F) - (Col. 12)','A. Offences under I.T. Act - Publication/ transmission of obscene / sexually explicit act in electronic form (Sec. 67) - Publication/ transmission of obscene / sexually explicit act in electronic form (Total) - (Col. 13)','A. Offences under I.T. Act - Publication/ transmission of obscene / sexually explicit act in electronic form (Sec. 67) - A) Publishing or transmitting obscene material in Electronic Form - (Col. 14)','A. Offences under I.T. Act - Publication/transmission of obscene / sexually explicit act in electronic form (Sec. 67) - B) Publishing or transmitting of material containing Sexually explicit act in electronic form (Sec.67A) - (Col. 15)','A. Offences under I.T. Act - Publication/transmission of obscene / sexually explicit act in electronic form (Sec. 67) - C) Publishing or transmitting of material depicting children in Sexually explicit act in electronic form (Sec.67B) - (Col. 16)','A. Offences under I.T. Act - Publication/transmission of obscene / sexually explicit act in electronic form (Sec. 67) - D) Preservation and retention of information by intermediaries (Sec.67C) - (Col. 17)','A. Offences under I.T. Act - Publication/transmission of obscene / sexually explicit act in electronic form (Sec. 67) - E) Other sub- sections of Sec. 67 IT Act - (Col. 18)','A. Offences under I.T. Act - Publication/transmission of obscene / sexually explicit act in electronic form (Sec. 67) - (Col. 19)','A. Offences under I.T. Act - Un-authorized access/attempt to access to protected

computer system (Sec.70) - (Col. 20)','A. Offences under I.T. Act - Abetment to Commit Offences (Sec.84 B) - (Col. 21)','A. Offences under I.T. Act - Attempt to Commit Offences (Sec.84C) - (Col. 22)','A. Offences under I.T. Act - Other Sections of IT Act - (Col. 23)','Total Offences under I.T. Act - (Col. 24)'])

Code to add up all the columns that comes under IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) and place them into one column, then drop all other columns which comes under this category:

df['IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act)'] = df['B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Abetment of Suicide (Online) (Sec.305/306 IPC) - (Col. 25)']+df['B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Cyber Stalking/ Bullying of Women/ Children (Sec.354D IPC) - (Col. 26)']+df['B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Data theft (Sec.379 to 381) - (Col. 27)']+df['B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Fraud (Sec.420 r/w Sec.465, 468- 471 IPC) - Fraud (Sec.420 r/w Sec.465,468- 471 IPC) (Total) - (Col. 28)']+df['B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Fraud (Sec.420 r/w Sec.465, 468- 471 IPC) - A) Credit Card/Debit Card - (Col. 29)']+df['B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Fraud (Sec.420 r/w Sec.465, 468- 471 IPC) - B) ATMs - (Col. 30)']+df['B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Fraud (Sec.420 r/w Sec.465, 468- 471 IPC) - C) Online Banking Fraud - (Col. 31)']+df['B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Fraud (Sec.420 r/w Sec.465, 468- 471 IPC) - D) OTP Frauds - (Col. 32)']+df['B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Fraud (Sec.420 r/w Sec.465, 468- 471 IPC) - E) Others - (Col. 33)']+df['B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Cheating (Sec.420) - (Col. 34)']+df['B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Forgery (Sec.465, 468 & 471) - (Col. 35)']+df['B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Defamation/

Morphing (Sec.469 IPC r/w IPC and Indecent representation of women Act) - (Col. 36)']+df['B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Fake Profile (r/w IPC/SLL) - (Col. 37)']+df['B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Counterfeiting - Counterfeiting (Total) - (Col. 38)']+df['B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Counterfeiting - A) Currency (Sec.489A to 489E) - (Col. 39)']+df['B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Counterfeiting - B) Stamps (Sec.255) - (Col. 40)']+df['B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Cyber Blackmailing/ Threat ening (Sec.506,503,384 IPC) - (Col. 41)']+df['B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Fake News on Social Media (Sec.505) - (Col. 42)']+df['B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Other Offences (r/w IT Act) - (Col. 43)']+df['Total Offences under IPC - (Col. 44)']

df = df.drop(columns=['B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Abetment of Suicide (Online) (Sec.305/306 IPC) - (Col. 25)','B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Cyber Stalking/ Bullying of Women/ Children (Sec.354D IPC) - (Col. 26)','B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Data theft (Sec.379 to 381) - (Col. 27)','B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Fraud (Sec.420 r/w Sec.465, 468- 471 IPC) - Fraud (Sec.420 r/w Sec.465,468- 471 IPC) (Total) - (Col. 28)','B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Fraud (Sec.420 r/w Sec.465, 468- 471 IPC) - A) Credit Card/Debit Card - (Col. 29)','B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Fraud (Sec.420 r/w Sec.465, 468- 471 IPC) - B) ATMs - (Col. 30)','B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Fraud (Sec.420 r/w Sec.465, 468- 471 IPC) - C) Online Banking Fraud - (Col. 31)','B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Fraud (Sec.420 r/w Sec.465, 468- 471 IPC) - D) OTP Frauds - (Col. 32)','B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Fraud (Sec.420 r/w Sec.465, 468- 471 IPC) - E) Others - (Col. 33)','B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Cheating (Sec.420) - (Col. 34)','B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Forgery (Sec.465, 468 & 471) - (Col. 35)','B.

IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Defamation/ Morphing (Sec.469 IPC r/w IPC and Indecent representation of women Act) - (Col. 36)','B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Fake Profile (r/w IPC/SLL) - (Col. 37)','B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Counterfeiting - Counterfeiting (Total) - (Col. 38)','B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Counterfeiting - A) Currency (Sec.489A to 489E) - (Col. 39)','B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Counterfeiting - B) Stamps (Sec.255) - (Col. 40)','B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Cyber Blackmailing/ Threat ening (Sec.506,503,384 IPC) - (Col. 41)','B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Fake News on Social Media (Sec.505) - (Col. 42)','B. IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act) - Other Offences (r/w IT Act) - (Col. 43)','Total Offences under IPC - (Col. 44)'])

Code to add up all the columns that comes under Offences under SLL (Involving Communication Devices as Medium/ Target) r/w IT and place them into one column, then drop all other columns which comes under this category:

df['Offences under SLL (Involving Communication Devices as Medium/ Target) r/w IT']=df['C. Offences under SLL (Involving Communication Devices as Medium/ Target) r/w IT - Gambling Act (Online Gambling) - (Col. 45)']+df['C. Offences under SLL (Involving Communication Devices as Medium/ Target) r/w IT - Lotteries Act (Online Lotteries) - (Col. 46)']+df['C. Offences under SLL (Involving Communication Devices as Medium/ Target) r/w IT - Copy Right Act, 1957 - (Col. 47)']+df['C. Offences under SLL (Involving Communication Devices as Medium/ Target) r/w IT - Trade Marks Act, 1999 - (Col. 48)']+df['C. Offences under SLL (Involving Communication Devices as Medium/ Target) r/w IT - Other SLL Crimes - (Col. 49)']+df['- Total Offences under SLL - (Col. 50)']

df = df.drop(columns=['C. Offences under SLL (Involving Communication Devices as Medium/ Target) r/w IT - Gambling Act (Online Gambling) - (Col. 45)','C. Offences under SLL (Involving Communication Devices as Medium/ Target) r/w

IT - Lotteries Act (Online Lotteries) - (Col. 46)','C. Offences under SLL (Involving Communication Devices as Medium/ Target) r/w IT - Copy Right Act, 1957 - (Col. 47)','C. Offences under SLL (Involving Communication Devices as Medium/ Target) r/w IT - Trade Marks Act, 1999 - (Col. 48)','C. Offences under SLL (Involving Communication Devices as Medium/ Target) r/w IT - Other SLL Crimes - (Col. 49)','- Total Offences under SLL - (Col. 50)'])

Now the tables of the dataset appear like this:

	Si. No (Col. 1)	Category	State/UT (Col. 2)	Computer Related Offences	Offences under I.T. Act	IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act)	Offences under SLL (Involving Communication Devices as Medium/ Target) r/w IT	Total Cyber Crimes (IT Act + IPC r/w IT Act + SLL r/w IT Act)
0	1	State	Andhra Pradesh	448	468	3908	8	1899
1	2	State	Arunachal Pradesh	46	34	9	0	30
2	3	State	Assam	3000	5306	1445	0	3530
3	4	State	Bihar	32	241	4130	10	1512
4	5	State	Chhattisgarh	40	349	403	0	297
5	6	State	Goa	10	23	59	0	40
6	7	State	Gujarat	404	534	2101	20	1283
7	8	State	Haryana	526	910	356	12	656
8	9	State	Himachal Pradesh	44	220	19	0	98
9	10	State	Jharkhand	1882	1011	461	96	1204
10	11	State	Karnataka	20218	11777	2	0	10741
11	12	State	Kerala	248	769	148	18	426
12	13	State	Madhya Pradesh	428	660	702	26	699
13	14	State	Maharashtra	788	1259	11609	18	5496
14	15	State	Manipur	0	16	146	0	79
15	16	State	Meghalaya	176	172	60	0	142
16	17	State	Mizoram	8	12	12	0	13
17	18	State	Nagaland	14	10	0	0	8
18	19	State	Odisha	276	1826	3495	6	1931
19	20	State	Punjab	122	480	337	18	378
20	21	State	Rajasthan	632	1023	1802	6	1354
21	22	State	Sikkim	0	0	0	0	0
22	23	State	Tamil Nadu	246	1346	471	28	782
23	24	State	Telangana	384	517	12743	10	5024
24	25	State	Tripura	34	68	0	0	34
25	26	State	Uttar Pradesh	13232	13766	4717	52	11097
26	27	State	Uttarakhand	376	337	9	0	243
27	28	State	West Bengal	52	149	1415	2	712

	Si. No (Col. 1)	Category	State/UT (Col. 2)	Computer Related Offences	Offences under I.T. Act	IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act)	Offences under SLL (Involving Communication Devices as Medium/ Target) r/w IT	Total Cyber Crimes (IT Act + IPC r/w IT Act + SLL r/w IT Act)
28	Total State(s)	Total State(s)	Total State(s)	43666	43283	50559	330	49708
29	29	Union Territories	A & N Islands	2	8	2	0	5
30	30	Union Territories	Chandigarh	2	16	22	0	17
31	31	Union Territories	D & N Haveli and Daman & Diu	4	5	0	0	3
32	32	Union Territories	Delhi	108	193	165	0	168
33	33	Union Territories	Jammu & Kashmir	50	147	56	50	120
34	34	Union Territories	Ladakh	0	0	0	2	1
35	35	Union Territories	Lakshadweep	0	6	2	0	3
36	36	Union Territories	Puducherry	20	10	0	0	10
37	Total UT(s)	Total UT(s)	Total UT(s)	186	385	247	52	327
38	Total All India	Total All India	Total All India	43852	43668	50806	382	50035

The dataset utilised in this analysis contains no null values, that is all of the rows and columns are filled with data; there are no missing values.

```
df.isnull().sum()
```

```
Si. No (Col. 1)                                                    0
Category                                                           0
State/UT (Col. 2)                                                  0
Computer Related Offences                                          0
Offences under I.T. Act                                            0
IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act)    0
Offences under SLL (Involving Communication Devices as Medium/ Target) r/w IT    0
Total Cyber Crimes (IT Act + IPC r/w IT Act + SLL r/w IT Act)      0
dtype: int64
```

<u>The correlation of the above mentioned table is given below :-</u>

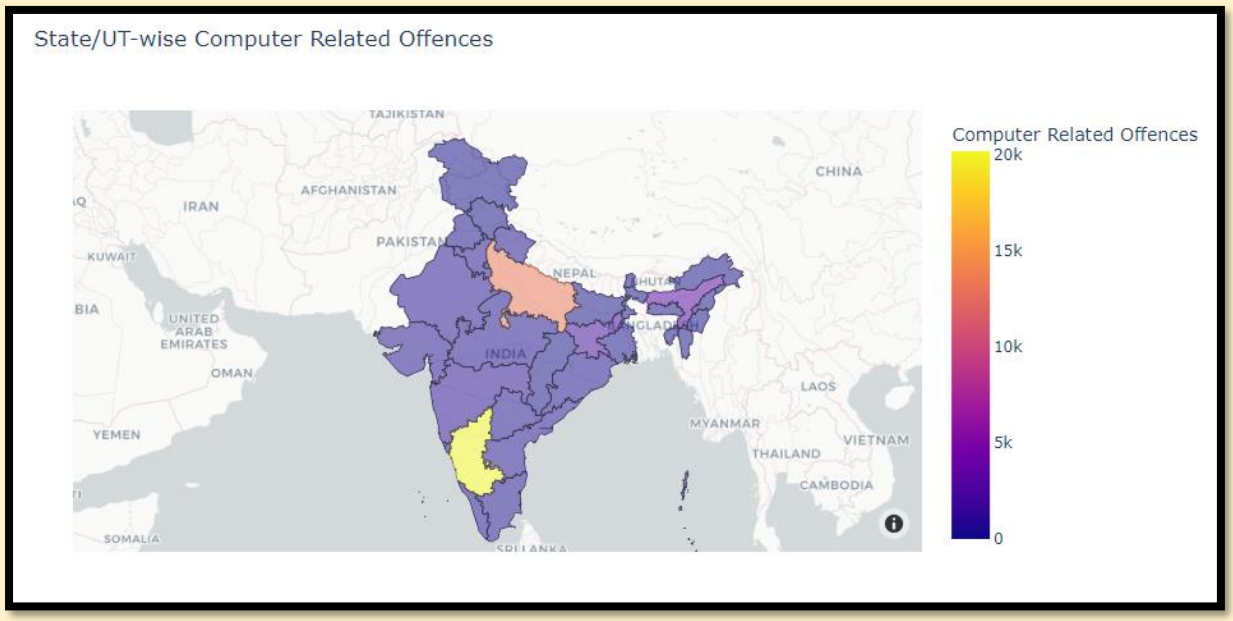
```
df.corr()
```

	Computer Related Offences	Offences under I.T. Act	IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act)	Offences under SLL (Involving Communication Devices as Medium/ Target) r/w IT	Total Cyber Crimes (IT Act + IPC r/w IT Act + SLL r/w IT Act)
Computer Related Offences	1.000000	0.989894	0.905496	0.910261	0.978908
Offences under I.T. Act	0.989894	1.000000	0.937337	0.938922	0.992062
IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act)	0.905496	0.937337	1.000000	0.941283	0.971768
Offences under SLL (Involving Communication Devices as Medium/ Target) r/w IT	0.910261	0.938922	0.941283	1.000000	0.950866
Total Cyber Crimes (IT Act + IPC r/w IT Act + SLL r/w IT Act)	0.978908	0.992062	0.971768	0.950866	1.000000

Performing data visualization:

For Computer Related offences:

```
fig = px.choropleth_mapbox(
    data,
    locations="id",
    geojson=india_states,
    color="Computer Related Offences",
    hover_name="State/UT (Col. 2)",
    hover_data=["Computer Related Offences"],
    title="MAP",
    mapbox_style="carto-positron",
    center={"lat": 24, "lon": 78},
    zoom=2.8,
    opacity=0.5,
)
fig.show()
```



Overview Analysis:

From the dataset we could see that the number of computer-related offenses reported in different states and Union Territories (UTs) of India as of 2021.Some insights that can be gathered from this dataset and also after visualising it, is that there is significant variation in the number of computer-related offenses across different states and UTs.

- For instance, the number of offenses in Uttar Pradesh (13232), Karnataka (20218) is much higher compared to other states and UTs such as Nagaland (14) or Lakshadweep (0). This could be because of certain factors such as:

- Uttar Pradesh has the largest population of approximately 19 crore and Karnataka is also gradually becoming more populous, so a high population density can lead to a higher number of crimes
- Certain economic factors, such as poverty and unemployment, can increase the incidence of crimes such as computer-related offenses.
- Karnataka is one of the economically developed states in India and has a strong technology sector. This can result in a higher number of computer-related offenses as technology-based crimes such as hacking and cyber-fraud are more common in technologically advanced regions.
- The level of law enforcement and the effectiveness of law enforcement agencies can also impact the number of computer-related offenses reported. So in Uttar-Pradesh & Karnataka might be the law enforcement agencies are more active and effective in investigating and prosecuting computer-related crimes so the number of reported offenses are higher compared to other areas.
- In Uttar-Pradesh & Karnataka, might be the level of awareness of computer-related crimes and the willingness of victims to report such crimes is high so it is increasing number of offenses reported. If people are not aware of the types of computer-related crimes and their consequences, they might not recognize when they have been a victim of a crime and therefore might not report it, which could be the reason for the decrease in rate of computer related offences in other states.

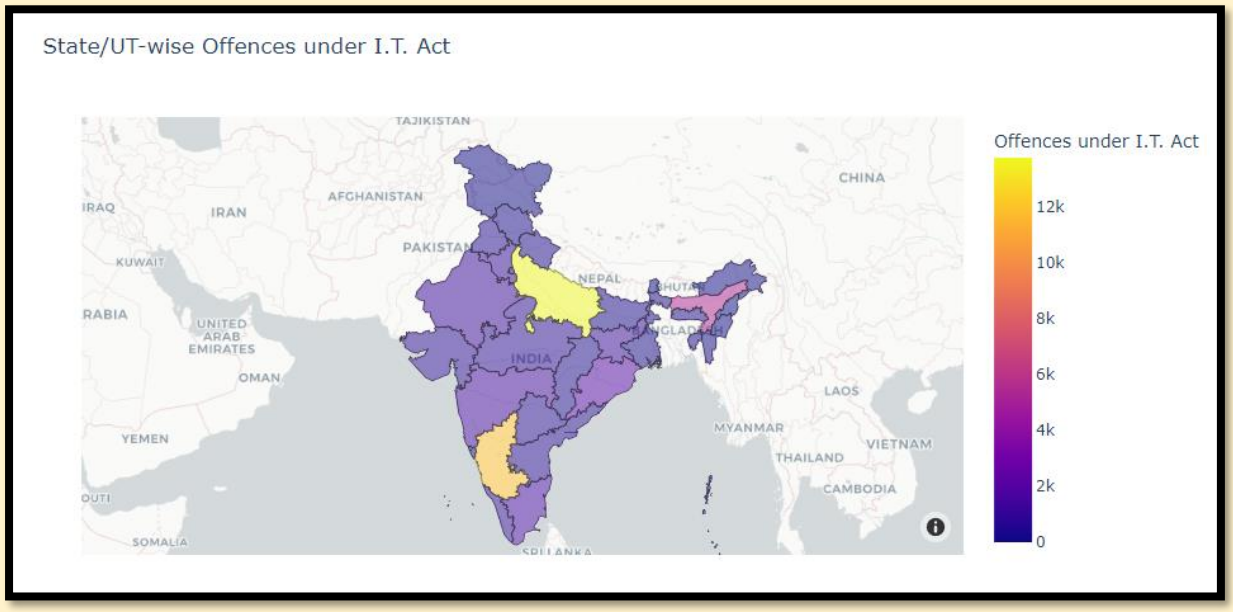
- Certain UTs have a low number of computer-related offenses, such as Ladakh (0) and Lakshadweep (0).The factors that are reducing the number of computer related cases could be:

- Ladakh and Lakshadweep, both the Union Territories are sparsely populated region in India, and a lower population can result in a lower number of computer-related crimes.
- Ladakh and Lakshadweep is a remote region in India, and the technology sector is not as developed as other regions. This can result in fewer computer-related offenses as technology-based crimes such as hacking and cyber-fraud are less common in regions with lower technological advancement.
- The level of awareness of computer-related crimes and the willingness of victims to report such crimes can also impact the number of offenses reported. It might be the awareness and reporting of such crimes is low in Ladakh & Lakshadweep, this could explain the lower number of reported offenses.

The average number of computer-related offenses across the states and UTs is approximately 1125.It reflects that computer-related crimes are a common issue in India and that the states and UTs are facing similar challenges with regards to computer-related offenses. These insights could be used to understand the state of computer-related crimes in India and to develop strategies to prevent and mitigate them.

For Offences under I.T. Act:

```
fig = px.choropleth_mapbox(
    data,
    locations="id",
    geojson=india_states,
    color="Offences under I.T. Act",
    hover_name="State/UT (Col. 2)",
    hover_data=["Offences under I.T. Act"],
    title="State/UT-wise Offences under I.T. Act",
    mapbox_style="carto-positron",
    center={"lat": 24, "lon": 78},
    zoom=2.8,
    opacity=0.5,
)
fig.show()
```



Overview Analysis:

The dataset revealed the total number of I.T. Act offences reported in the various Indian states and Union Territories (UTs) as of 2021. The number of offences under the I.T. Act varies significantly among the states and UTs, according to some observations that can be drawn from this dataset and from the visualisation of it. These are the insights that we could figure out from the dataset about the state/UT-wise number of I.T. Act offences, are given as follows:

- Some regions, such as Uttar Pradesh and Jharkhand, have higher numbers of offences under I.T. Act compared to others, such as Ladakh and Lakshadweep. This could be because for the following reasons:

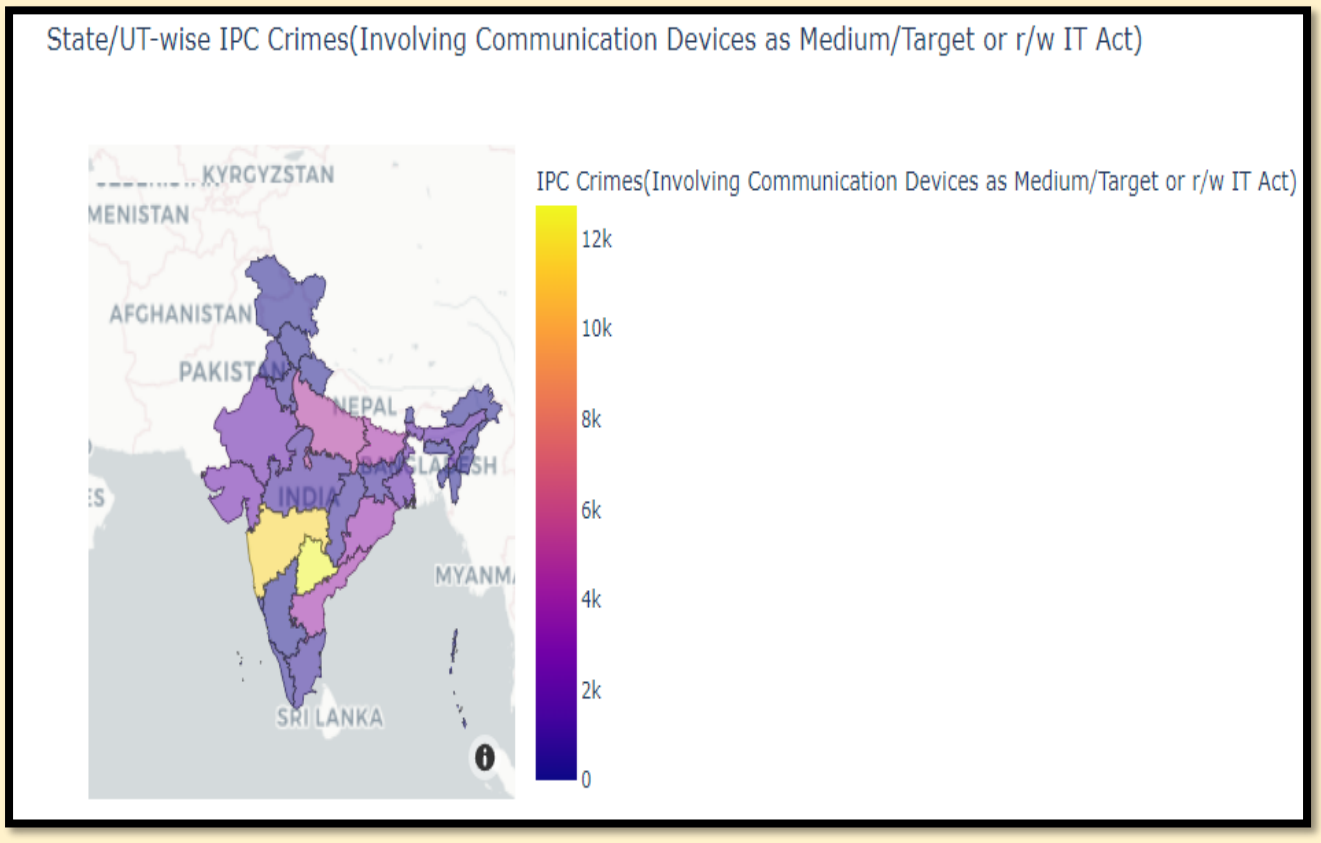
    - Since it has the largest population size, leading to more opportunities for offenses to occur higher levels of technology adoption and usage in these states, increasing the potential for offenses
    - It can be due to lower levels of awareness and education about cyber security practices and laws, making individuals and businesses more vulnerable to offenses.
    - In those regions there might be inadequate enforcement of the I.T. Act, resulting in fewer consequences for those committing offenses hence there is a higher level of corruption or a lack of resources available for law enforcement to tackle these types of offenses.
    - Lack of proper computer systems, lack of trained cybersecurity personnel, and lack of proper legal framework in those regions can also contribute to a higher number of computer-related offences.
    - Economic disparities and high levels of unemployment in these states could lead to an increase in cybercrime, as people may resort to illegal means to make money.

- This data could be used to track trends over time, such as changes in the number of offences in different states and UTs. This could help identify emerging trends and predict future trends.

- This data could be compared with other data sources, such as economic and demographic data, to gain a better understanding of the factors that contribute to computer-related offences in different regions.

For offence under IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act):

```
fig = px.choropleth_mapbox(
    data,
    locations="id",
    geojson=india_states,
    color="IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act)",
    hover_name="State/UT (Col. 2)",
    hover_data=["IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act)"],
    title="State/UT-wise IPC Crimes(Involving Communication Devices as Medium/Target or r/w IT Act)",
    mapbox_style="carto-positron",
    center={"lat": 24, "lon": 78},
    zoom=2.8,
    opacity=0.5,
)
fig.show()
```



Overview Analysis:

Based on this data, we can draw several insights:

- Uttar Pradesh and Telangana have high numbers of crimes involving communication devices as medium/target or related to IT Act. This could be because of the following reasons:
  High population:

  - Uttar Pradesh is the most populous state in India and Telangana has a significant population, which could contribute to a higher number of crimes.
  - Low Awareness of Cybersecurity: Lack of awareness of cybersecurity measures among people could make them more vulnerable to cybercrimes.
  - Lack of Cybersecurity Infrastructure: Limited infrastructure and inadequate law enforcement measures could also contribute to the higher number of cybercrimes.
  - Economic and Political Factors: Economic and political factors such as poverty, unemployment, and political instability can lead to an increase in cybercrime activities.
  - Technological advancement: With the rapid advancement of technology, the use of communication devices has increased, leading to more opportunities for cybercriminals to exploit.

- Nagaland and Lakshadweep have the lowest number of such crimes. This could be because due to various reasons such as low population density, better law enforcement and security measures, higher awareness about safe usage of technology, or other social, economic, and political factors.

- High-crime states like Karnataka, Tamil Nadu, and Maharashtra are also IT hubs in India, with a high concentration of technology companies, have more number of crimes. This could be because of following reasons:

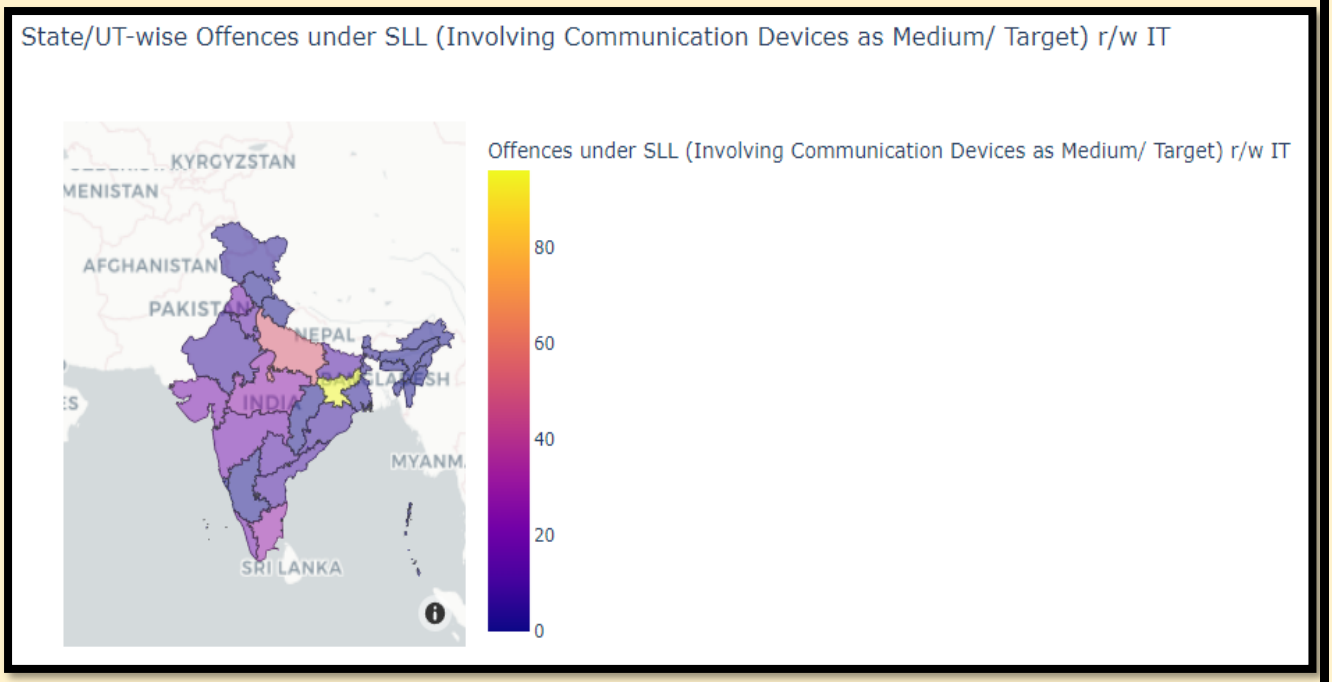
    - High concentration of technology companies and internet users: With a large number of technology companies and a high concentration of internet users, the potential for misuse of communication devices and technology increases, leading to a higher number of crimes.
    - Lack of awareness and proper implementation of cyber security measures: In areas with high IT usage, cybercrime incidents can occur due to lack of awareness of proper cyber security measures and practices.
    - Complex and constantly evolving technology: As technology evolves and becomes more complex, it becomes easier for malicious actors to exploit vulnerabilities, leading to a rise in cybercrime incidents.
    - Economic benefits: High-crime states often have a strong economy and higher purchasing power, making them attractive targets for cyber criminals.
    - Governance and law enforcement: The effectiveness of governance and law enforcement measures in preventing and prosecuting cybercrime incidents can also play a role in the incidence of such crimes.

- There is a geographical diversity in the number of crimes, with states like Assam, Odisha, and Chhattisgarh having a higher number of crimes compared to states in the north-west like Haryana and Punjab.

This could mean that the level of awareness and implementation of digital safety measures and laws, as well as the level of law enforcement, vary across states in India. It could also be influenced by factors such as the level of urbanization and economic development, which can increase the usage of communication devices and thereby the chances of crimes involving them.

For Offences under SLL (Involving Communication Devices as Medium/Target) r/w IT:

```
fig = px.choropleth_mapbox(
    data,
    locations="id",
    geojson=india_states,
    color="Offences under SLL (Involving Communication Devices as Medium/ Target) r/w IT",
    hover_name="State/UT (Col. 2)",
    hover_data=["Offences under SLL (Involving Communication Devices as Medium/ Target) r/w IT"],
    title="State/UT-wise Offences under SLL (Involving Communication Devices as Medium/ Target) r/w IT",
    mapbox_style="carto-positron",
    center={"lat": 24, "lon": 78},
    zoom=2.8,
    opacity=0.5,
)
fig.show()
```



Overview Analysis:

The data shows the number of offences under SLL (Involving Communication Devices as Medium/Target) related to IT Act in different states/UTs in India. Here are some insights based on this data:

- High number of crimes: Uttar Pradesh, Jharkhand, Tamil Nadu and Jammu & Kashmir have a higher number of such crimes compared to other states/UTs.

    - The reasons for higher number of crimes involving communication devices in Jammu & Kashmir compared to other states and UTs can be attributed to various factors such as socio-economic conditions, infrastructure, digital literacy and awareness, policing and enforcement, and technology penetration.
    - The main reasons for the higher number of crimes in Tamil Nadu could be high population density and urbanization, strong economy and rapid development, availability of advanced technology and internet services, lack of awareness about cybercrime and its consequences, weak law enforcement and insufficient regulations to prevent cybercrime.
    - The higher number of crimes in Uttar Pradesh and Jharkhand may be due to several reasons, such as higher population density, lower socio-economic status, lower levels of education, poor law enforcement, and higher levels of poverty, leading to increased opportunities for cybercriminals to commit crimes. Additionally, the lack of awareness about online safety and the increasing use of

technology and internet usage may also contribute to the higher number of crimes in these states.

- Low number of crimes: Nagaland, Lakshadweep, Himachal Pradesh, Meghalaya, Mizoram, Tripura and Uttarakhand have the lowest number of such crimes. This could be due to various factors such as the population, the level of technology usage, law enforcement, and socio-economic conditions.

- Regional distribution: The number of crimes is not evenly distributed across the states/UTs. Some states in the east and north-east region like Assam, Chhattisgarh, and Odisha have a lower number of crimes, while states in the central and north region like Madhya Pradesh, Uttar Pradesh and Jharkhand have a higher number of crimes.

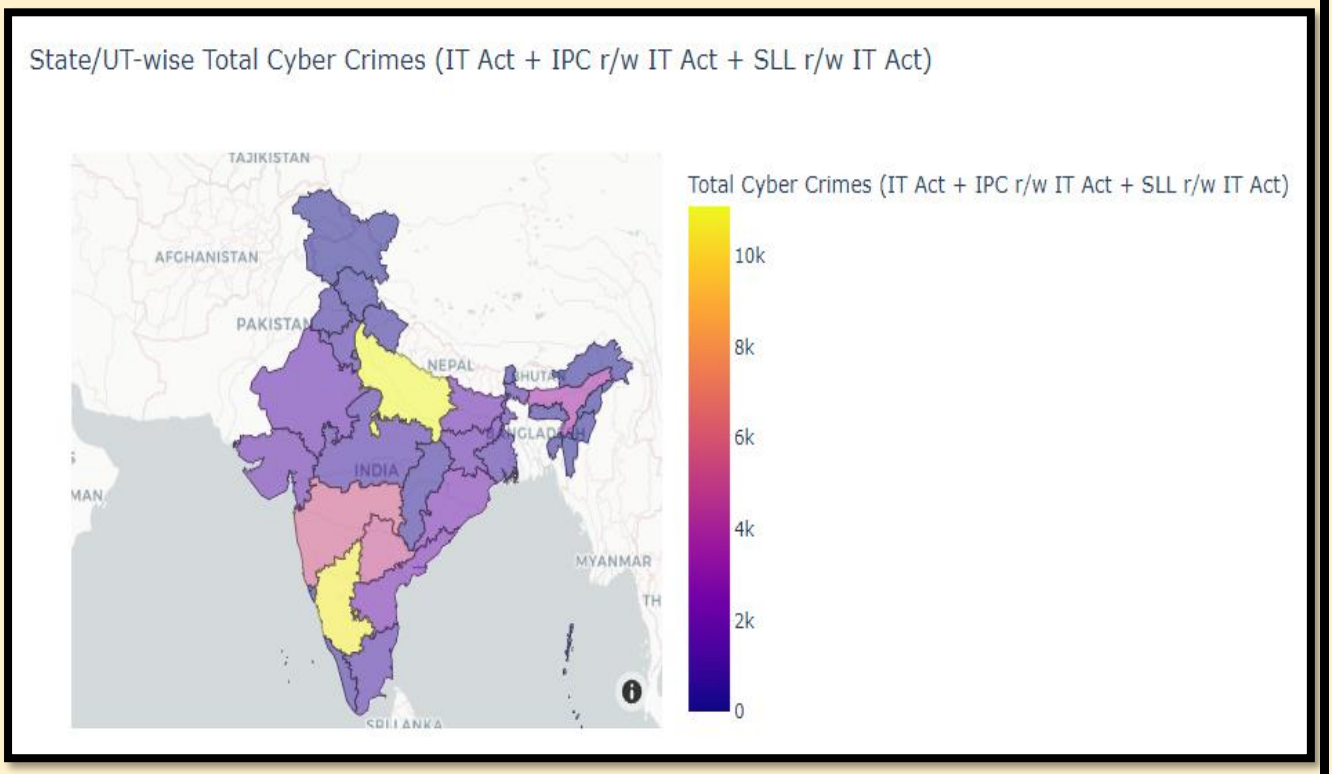
- IT hubs: High-tech states like Karnataka, Maharashtra and Tamil Nadu, which are also IT hubs, have a lower number of crimes compared to other states.

- Coastal states: Some coastal states like Andhra Pradesh, Kerala, and Maharashtra have a higher number of crimes compared to other states.

- Union Territories: Most of the Union Territories have a low number of such crimes.

For Total number of cybercrimes committed in India:

```
fig = px.choropleth_mapbox(
    data,
    locations="id",
    geojson=india_states,
    color="Total Cyber Crimes (IT Act + IPC r/w IT Act + SLL r/w IT Act)",
    hover_name="State/UT (Col. 2)",
    hover_data=["Total Cyber Crimes (IT Act + IPC r/w IT Act + SLL r/w IT Act)"],
    title="State/UT-wise Total Cyber Crimes (IT Act + IPC r/w IT Act + SLL r/w IT Act)",
    mapbox_style="carto-positron",
    center={"lat": 24, "lon": 78},
    zoom=2.8,
    opacity=0.5,
)
fig.show()
```



Overview Analysis:

The data shows that the total number of cybercrime offences under SLL (Involving Communication Devices as Medium/Target) related to IT Act, Offences under I.T. Act, Computer Related Offences, IPC Crimes

(Involving Communication Devices as Medium/Target or r/w IT Act) in different states/UTs in India. Here are some insights based on this data:

- Maharashtra has the highest number of cyber-crimes reported with 5496 cases, followed by Uttar Pradesh with 11097 cases.

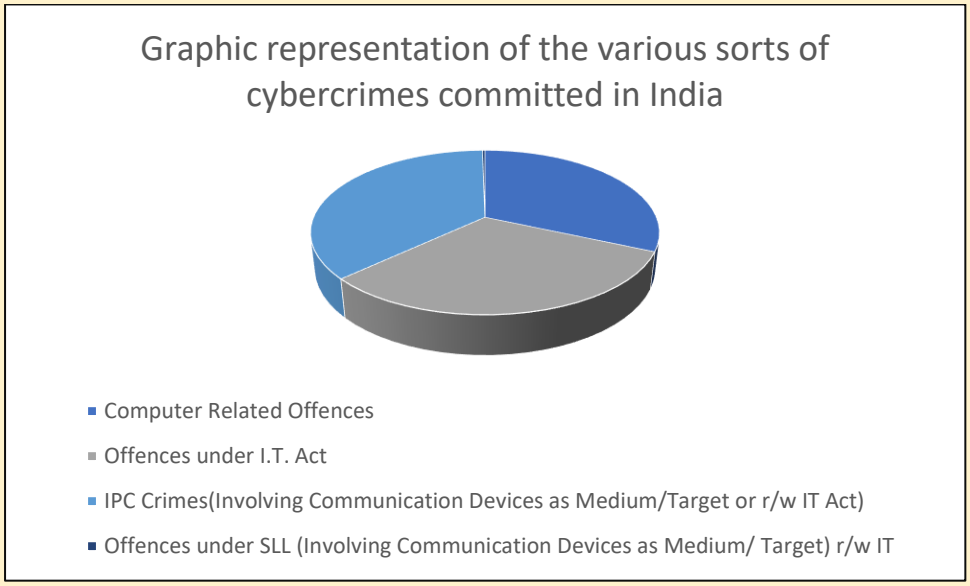
- The states with the lowest number of reported cyber-crimes are Lakshadweep and Sikkim, with 3 and 0 cases respectively.

- The southern states of Tamil Nadu, Kerala, and Telangana have a moderate number of reported cyber-crimes, with 782, 426, and 5024 cases respectively.

- There is a wide variance in the number of reported cyber-crimes across different states in India. This could be due to differences in the level of awareness about cyber-crimes, the quality of law enforcement, and the severity of the crimes committed in different states.

- The majority of states have a low to moderate number of reported cyber-crimes, with only a few states having a high number of reported cyber-crimes. This indicates that cybercrime is a serious concern in India, but is not as prevalent as in some other countries.

Various Sort of Cyber-Crimes Committed in India:



Overview Analysis:

- The highest number of offences is "IPC Crimes involving communication devices as medium/target or related to the IT Act" with 50,806 incidents.
- The lowest number of offences is "Offences under SLL (Involving Communication Devices as Medium/ Target) related to the IT Act" with only 382 incidents.
- The "Computer Related Offences" and "Offences under I.T. Act" categories have similar numbers with 43,852 and 43,668 incidents respectively.

- This information can give us a general idea of the types of cybercrimes that are most prevalent.

Predicting the future occurrence of cybercrimes is challenging as it depends on many factors such as technology advancements, the level of cybersecurity, and the actions taken by law enforcement and other organizations to prevent such crimes.

However, based on current trends and the increasing use of technology, it is likely that crimes involving communication devices and related to the IT Act will continue to be a significant issue in India. This includes crimes such as hacking, identity theft, online fraud, and cyberstalking.

It is also likely that new forms of cybercrimes will emerge as technology evolves and criminals find new ways to exploit vulnerabilities. Therefore, it is important for individuals and organizations to stay informed about the latest cybersecurity threats and take proactive measures to protect themselves.

CONCLUSION

The number of cyber-crimes reported in India in 2020 varies greatly among different states and union territories.

Some states and union territories have high numbers of computer related offences, offences under IT Act, IPC crimes involving communication devices, and offences under SLL involving communication devices, while others have relatively low numbers.

The total number of cyber-crimes (combining all categories) ranges from 0 in Sikkim to 19,609 in Andhra Pradesh.

Some states, such as Andhra Pradesh, have a large number of offences under IPC crimes involving communication devices, while others, such as Himachal Pradesh, have very few such offences.

There are states and union territories with zero reported cyber-crimes under SLL involving communication devices, while others have a small number.

The data provide insights into the types of cyber-crimes being committed, the geographical distribution of cyber-crimes, and the overall trend of cyber-crime in India. This information can be useful for policy makers, law enforcement agencies, and others to understand the magnitude of the problem and develop targeted strategies to prevent and address cyber-crimes in India.

FUTURE WORKS

- Analyse the state/UT-wise distribution of cybercrimes and identify the states/UTs with higher/lower incidences of cybercrime.
- Study the trend of cybercrime over the years and forecast the future trend.
- Investigate the correlation between various types of cybercrimes and their causes.
- Identify the most vulnerable groups and the areas of high-risk for cybercrime.
- Develop a prediction model to identify the risk of cybercrime in a particular state/UT.
- Analyse the effectiveness of existing laws and regulations in preventing cybercrime.
- Evaluate the impact of cybercrime on individuals and organizations, and suggest mitigation strategies.