

Comments received in accordance with the workplan of the Expert Group on Cybercrime for the period 2018-2020

***Reproduced as received
Status: Wednesday, 6 March 2019***

The present compilation was prepared in accordance with the workplan for 2018-2021 of the Open-ended intergovernmental expert group meeting on Cybercrime, based on Commission on Crime Prevention and Criminal Justice resolution 26/4,¹ approved by the extended Bureau of the expert group on at its meeting on 26 January 2018, which *inter alia* states that:

Prior to each IEG meeting, the Secretariat will invite Member States to provide, in writing, comments, good practices, new information, national efforts as well as recommendations regarding the meeting's main topics. Observers will be invited to provide relevant information. The Secretariat will then compile and disseminate the information collected not later than three weeks prior to the meeting.

An invitation to provide such comments was transmitted through Note Verbale CU 2019/4(A)/DTA/OCB/CSS. The comments reproduced below were received by the Secretariat within the deadline of 1st March 2019. A total of seven contributions were received from the following Member States: France, India, Japan, Morocco, Netherlands, Russian Federation and the United States.

France

La cinquième réunion du groupe intergouvernemental, à composition non limitée, chargé de réaliser une étude approfondie sur le problème de la cybercriminalité abordera les questions et enjeux relatifs à l'application de la loi et aux enquêtes, ainsi qu'à la preuve électronique et à la justice pénale, conformément au plan de travail proposé par la présidence pour la période 2018 -202.

La France est particulièrement impliquée dans la régulation du cyberespace. A ce titre, elle a rappelé, à l'occasion de l'Appel de Paris pour la confiance et la sécurité dans le cyberespace du 12 novembre 2018, son soutien à un cyberespace ouvert, sûr, stable, accessible et pacifique, dans lequel le droit international s'applique. Cet Appel est aujourd'hui soutenu par plus de 60 Etats et 300 représentants de la société civile.

La France a par ailleurs développé ces dernières années plusieurs initiatives nationales pour une meilleure réponse à la lutte contre la cybercriminalité. Le décret n° 2017-58 du 23 janvier 2017 institue, auprès du ministre de l'Intérieur, un délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces. Il est chargé de coordonner l'action du ministère en matière de lutte contre les cyberattaques et d'une unité dédiée à la lutte contre la cybercriminalité.

Afin de mieux appréhender la cybercriminalité, il paraît essentiel de mobiliser tous les acteurs concernés. Ainsi, le citoyen peut être un acteur important de la détection. C'est la raison pour laquelle

¹ Available at <http://www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmental-expert-group-to-conduct-a-comprehensive-study-of-the-problem-of-cybercrime2018.html>

la France a mis en place une plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS). L'internaute confronté à des contenus ou des comportements illicites sur Internet a la possibilité d'envoyer un signalement sur le portail du ministère de l'Intérieur français (www.internet-signalement.gouv.fr). La plateforme Pharos a enregistré plus de 160 000 signalements pour contenus illicites en 2018. Plus récemment, d'autres plateformes ont été établies, comme la plateforme PERCEVAL qui traite les signalements de fraudes à la carte bancaire. La plateforme THESEE doit prochainement contribuer au traitement des plaintes pour escroqueries en ligne.

Au plan judiciaire, la France a doté, en juin 2016, le Procureur de Paris d'une compétence nationale concurrente en matière de cyberattaque, permettant de mieux centraliser le traitement judiciaire de contentieux de cybercriminalité et de faciliter la coopération internationale, notamment au niveau d'Eurojust. De même une mission de lutte contre la cybercriminalité a été créée en 2015 au sein de la direction des affaires criminelles et des grâces du ministère de la Justice, dont les membres représentent la France au sein du « European Judicial Cybercrime Network » (EJCN).

Au sein de l'Union européenne, la France participe activement aux négociations dans le cadre des deux propositions législatives présentées par la Commission européenne le 27 avril 2018 : un projet de règlement fixant les conditions et modalités d'accès des preuves électroniques et un projet de directive imposant aux fournisseurs de service de désigner un représentant légal habilité à recevoir des injonctions et à y répondre. La France soutient également le projet de règlement européen permettant le retrait dans l'heure des contenus terroristes en ligne afin de lutter efficacement contre la propagation de la propagande en faveur du terrorisme sur internet.

La France a par ailleurs ratifié la Convention de Budapest du Conseil de l'Europe depuis 2006. C'est un outil précieux qui permet une coopération internationale efficace, d'autant plus que son cadre très large dépasse celui du Conseil de l'Europe, avec 62 Etats parties représentant tous les continents. En effet, elle offre une base juridique pour lutter contre la cybercriminalité, pour établir les différentes infractions dans les législations nationales, pour coopérer entre Etats pour les investigations.

Elle permet notamment de faire geler les données numériques en urgence et de faciliter la conservation des preuves numériques grâce à un réseau international de points de contact fonctionnant 24/7. Ainsi, la France a traité près de 250 demandes de gel pendant l'année 2018. Enfin, elle est un outil de mise en œuvre de l'entraide judiciaire internationale.

La France participe également au groupe de travail chargé de rédiger un protocole additionnel à la Convention de Budapest. Ce protocole additionnel permettra d'améliorer la coopération opérationnelle, d'accélérer le partage d'information et d'améliorer le cadre du régime traditionnel d'entraide judiciaire. Dans le cadre des travaux de ce groupe, la France soutient une approche volontariste permettant d'élaborer des mécanismes novateurs et efficaces de coopération internationale en matière d'accès à la preuve numérique tout en étant pleinement respectueux des droits et libertés fondamentales.

Au plan opérationnel, la France contribue au renforcement des compétences des services de pays étrangers, notamment dans le cadre des actions entreprises par le Conseil de l'Europe, à l'instar du programme Cybersud. Elle a également soutenu la création de l'École de cybersécurité à vocation régionale à Dakar, au Sénégal.

India

1. The exponential increase in cybercrimes in the past decade has raised new issues and challenges for law and law enforcement. This is because cybercrime differs significantly from traditional crimes in terms of nature, scope, means, evidence and activities. Unlike traditional crimes, information exchange in real-time or near real-time is essential for evidence collection to bring cyber criminals to justice. Cybercrime are technically complex and legally intricate than traditional crimes. Cyberspace/cybercrime has no physical boundaries so international cooperation is must for investigation, data/evidence collection, punishment etc. There are technological and legal challenges in combating cybercrimes.

2. **Agenda:** Agenda for the fifth meeting of Expert Group Meeting on cybercrime scheduled at Austria from 27-29 March, 2019 mainly include discussion on following:

(I) Law Enforcement and Investigation:

(A) Comments on National Efforts:

1. We are fully in agreement that while the problem of cybercrime is global in nature, the solutions mostly being adopted by LEAs are essentially local. As regards the critical elements of a consistent LE response to the problem of cybercrime in India, the following are already in place:

- i. Dedicated/specialized statute namely Information Technology Act, 2000 is in place to deal with offences committed using, targeting and incidental to electronic devices including computers and covers other cybercrimes. Based on the experiences, the Act underwent major changes in 2008 and newer, contemporary and technology neutral offences were introduced.
- ii. Based on the requirement of the Act, newer techniques and forms for collection and validation of electronic information have been developed. The information stored in electronic form when being reduced into physical form has to be validated by an accompanying certificate to be furnished by the custodian of the data.
- iii. Special emphasis has been placed on the capacity building of the LEA staff and especially of the cutting edge level staff so as to respond in the most effective manner. As the law and order in India is a state subject, State police forces are making efforts to train staff at every police station level and to equip each and every police station to respond to incidences of cybercrime.

2. The major mode of reporting remains information of the incidence by the victim and there is minimal reporting by the intermediaries. We also concur with the findings of the study regarding underreporting of the incidences and reasons thereof. National Crime Records Bureau of India maintains the data of reported cybercrimes, which show an ever increasing trend in the reported cybercrimes.

3. It has been observed that complexity and reach of the cybercrimes are increasing with each passing year and it is serious challenge to the resources of the LEAs and their preparedness for

Open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime

countering the same. LEAs in India do not possess the statutory powers to undertake proactive measures like undercover operations and online activities.

4. In India, computer data is not covered under any special class of evidence and can be requisitioned in the ordinary course of investigation like any other evidence. However, as outlined above, in cases where original evidence is not being seized, it has to be supported by a certificate vouching for the authenticity of the data and the copying process by the custodian of the record. Real time collection of traffic and content data is also possible within legal powers of LEAs on observing laid down process. Although there is no specific legal provision for preservation of data at the end of service providers but the LEAs get the same done under their general powers during investigation. India is also a member of G-8 24/7 network for preservation of computer data.

5. As regards extra territorial access to data by Indian LEAs, some of the ISPs like Google and Facebook are supplying data requisitioned under sec. 91 CrPC by the Indian LEAs subject to fulfilment of their conditions but in majority of cases the same is denied on several grounds. Also in case of other ISPs and service providers, the same is required to be requisitioned by formal processes.

6. As regards the protection of privacy and procedural safeguards, it may be mentioned here that sec. 66A of the IT Act was declared unconstitutional by the Apex Court of India for being vague and open ended. It was argued by the Human Rights activists many times that the same was allegedly misused by the LEAs.

(B) National Legislation:

1. The Information Technology Act, 2000

The Information Technology Act, 2000 is the primary law for dealing with cybercrime and digital commerce in India. The said Act, also provides the legal framework to deal with e-commerce, cyber security, cyber crime and cyber terrorism. Further, in case Information Technology Act, 2000 is seen in conjunction with traditional crime laws, it take most of the issues. The National Cyber Security Policy, 2013 was developed to build a secure and resilient cyberspace for India's citizens and businesses. The Indian Computer Emergency Response Team (CERT-In) is responsible for incident responses including analysis, forecasts and alerts on cyber security issues and breaches. The present position of Indian laws (the Information Technology Act, 2000) besides IPC and CrPC with regard to cybercrime are as under:

SI. No.	Section/chapter	Issue	Remark
1.	Chapter-II	Recognises Digital signature and electronic signature, electronic records	
2.	Chapter-III	Recognises electronic records	
3.	Section 43	Compensation for damage of computer, computer system etc – details are given type of damages	Shall liable to pay damages by way of compensation to the person so affected

Open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime

	Section 66	If any person, dishonestly or fraudulently, does any act referred above	Imprisonment upto 3 years or fine or both
4.	Section 43A	Compensation for failure to protect sensitive data	Shall liable to pay damages by way of compensation to the person so affected
5.	Section 65	Tampering with computer source documents – only when knowingly or intentionally conceals, destroys or alters computer source code. Definition of source code is explained	Imprisonment upto 3 years or fine or both
6.	Section 66B	Dishonestly receiving stolen computer resource or device	Imprisonment upto 3 years or fine or both
7.	Section 66C	Punishment for identity theft	Imprisonment upto 3 years or fine or both
8.	Section 66D	Punishment for cheating by personation by using computer resource	Imprisonment upto 3 years or fine or both
9.	Section 66E	Punishment for violation of privacy	Imprisonment upto 3 years or fine or both
10.	Section 66F	Punishment for cyber terrorism – with intent to threaten the unity, integrity, security or sovereignty or to strike terror in people or cause adversely affect critical information infrastructure	Imprisonment for life
11.	Section 67	Punishment for publishing or transmitting obscene material in electronic	Imprisonment for 3 to 5 years
12.	Section 67A	Punishment for publishing or transmitting of material containing sexually explicit act, etc in electronic form	Imprisonment for 3 to 7 years
13.	Section 67B	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form (children mean below the age of 18 years)	Imprisonment for 5 to 7 years
14.	Section 67 C	Preservation and retention of information by intermediaries – Need retain information in format and duration as prescribed by Central Govt.	Failure may attract imprisonment upto 3 years or fine or both
15.	Section 69	Interception or monitoring or decryption of information through any computer resource	Central or State Govt. has power
16.	Section 69A	Blocking of information for public access under certain conditions	Central Govt. has power
17.	Section 70	Govt can declare any computer resource to be protected system (Critical Information Infrastructure)	

18.	Section 73 & 74	Penalty for publishing false electronic signature or for fraudulent purpose	Imprisonment upto 2 years or fine or both
19.	Section 75	Application of Act for offence or contravention committed outside India irrespective of his nationality	
20.	Sector 76	Confiscation of computer resource is liable to confiscation in case of contravention of this Act	
21.	Section 79	Exemption from liability of intermediary in certain cases	
22.	Section 80	Power to Police officer and other officers to enter, search etc.	
23.	Section 80	Powers of Police Officers and others officers to enter, search, etc.	
24.	Section 81	Act to have overriding effect	
25.	Section 84B	Punishment for abetment of offences	
26.	Section 84C	Punishment for attempt to commit offences	
27.	Section 85C	Offences by companies	

2. Indian Telegraph Act, 1885

In India, there are legislations and policies which regulate/make provisions for the law enforcement agencies of the Central and the State Government for interception of messages. Now a day, the messages sent are in the electronic form and the same can be intercepted as provided in the legislations. One of such legislations is the **Indian Telegraph Act, 1885**.

The Section 5 of the Indian Telegraph Act, 1885, empowers the Central Government and State Governments of India to order the interception of messages in two circumstances: (1) in the occurrence of any public emergency or in the interest of public safety, and (2) if it is considered necessary or expedient to do so in the interest of:

- the sovereignty and integrity of India; or
- the security of the State: or
- friendly relations with foreign states; or
- public order: or
- for preventing incitement to the commission of an offence.

Rule 419A of the Indian Telegraph Rules requires the establishment of a Review Committee by the Central Government and the State Government, as the case may be, for the interception of communications, as per the conditions provided therein.

This Act also deals with the terms of providing the services are regulated under the **Unified Access Service License (UASL)** which also contains provisions regarding surveillance/interception.

These provisions are regularly used by the state agencies to intercept telephonic and data traffic of subscribers.

(C) State/Central Police Agencies

1. With day to day increase in the Cyber Crime, the cases registered with the Central as well as State Police are rising manifold. The evidence in such cases is required to be immediately retrieved and analysed. Since the evidence pertains to e-mails, websites, chat rooms and databases has to be traced on the desktops, laptops as well as mobile phones, it is imperative that the data is retrieved at the earliest and following the prescribed procedure for its admissibility in courts.

2. The collection of evidence is one of the most important areas to deal with the Cyber Crime. The Police Agencies in India are using the tools and techniques of collecting the digital evidence. The CBI Academy is organizing training programme regarding collection of evidence.

3. In several states, there are dedicated District Cyber Cells to speed up the investigation in Cyber Crime under the IT Act. There is a need for constitution of such Cyber Cells at national level for co-ordination among various States and also with Central Agencies.

(D) Crime and Criminal Tracking Network & Systems

1. The Crime and Criminal Tracking Network & System (CCTNS) is a Mission Mode Project under the National e-Governance Plan (NeGP) of Government of India. CCTNS aims enhancing the efficiency and effectiveness of policing through creation of a nationwide networking infrastructure for evolution of IT-enabled-state-of-the-art tracking system around 'Investigation of crime and detection of criminals.'

2. As per the Journal 2018 of NCRB, an allocation of Rs.2000 crores has been made for CCTNS Project. Cabinet Committee on Economic Affairs (CCEA) has approved the project on 19.06.2009 and designated NCRB as implementing agency.

3. Although, the CCTNS is operational across the country but some issues obstruct the optimum utilization of the project at field level viz. 1. Poor and Unreliable Connectivity, Average Adoption at Field Level, Obsolete Hardware/Software, All FIR Registering Agencies not Covered under CCTNS, Absence of Specialised Solutions, Absence of Crime Data Analytics and Artificial Intelligence Tools.

4. However, as per NCRB Journal Vol. I 2018, it has been reported that sustenance of Project beyond 31st March 2018: no funds are allotted for the Operations & Maintenance (O&M) and Network connectivity after the project has officially ended by MHA on 31st March, 2018. In the absence of funds for O&M and network connectivity, the project will be adversely affected. NCRB is working on proposal for provisioning of funds required for Network Management and Operation & Maintenance (O&M) of CCTNS for next 5 years under Phase II of CCTNS. The CCTNS has the potential to transform the way policing is done. There is a need for the further efforts on the part of the Government to strengthen CCTNS.

(E) Recommendations:

1. Harmonization of laws and procedures
2. Standardization of forensic tools and forms for reports
3. Development of SOPs for different types of offences
4. Augmentation of capacity of LEAs in big way
5. There is a need for constitution of Cyber Cells at national level also and co-ordination among these cells with State Agencies
6. Research to deal with the issues is also required
7. Efforts on the part of the Government to strengthen CCTNS
8. The issue of extra-territorial jurisdiction during investigation also needs to be addressed.

(II) Electronic Evidence and Criminal Justice

This Chapter considers the criminal justice process in cybercrime cases, starting from the need to identify, collect and analyse electronic evidence through digital forensics. It examines the admissibility and use of electronic evidence in criminal trials, and demonstrates how a range of prosecutorial challenges can impact on criminal justice system performance.

Cyber-crime is often transnational and it involves multiple jurisdictions. The ease with which cybercrime crosses national borders, irreconcilable differences between national legal frameworks, and deceptions employed by cyber criminals impedes attribution, and prevents LEAs from apprehending offenders, holistic and uniform approach is must to counter the challenge. Prosecution in domestic scenarios and those carried out as a result of transnational investigations could fail if electronic evidence was not collected properly thus there is the need for standard-setting and technical assistance with respect to the collection, preservation and use of electronic evidence thus becomes essential. Thus, exchanging information and best practices, developing and/or upgrading legislation and strengthening international cooperation mechanisms as technical assistance priorities. Admissibility of electronic evidence in criminal investigations and prosecutions is needed to effectively counter cybercrime. The introduction of such legislation should be accompanied by adequate training and capacity-building for law enforcement officials, prosecutors and judges. The importance of sharing electronic evidence among jurisdictions was also underscored (E/CN.15/2018/12, para. 28).

(A) Comments on National Efforts:

1. Digital Forensics

Many forms of electronic evidence may be comparatively straightforward, such as a printout of a readily available email sent by a perpetrator or IP connection logs reported directly by an internet service provider. Other forms, on the other hand, may require sophisticated techniques in order to recover traces of activity or data from computers and networks that can provide evidence of criminal behaviour. To maintain sanctity of the digital evidence, the suspected systems are seized with all due care under SOP then the images are made using write blocker tools and then these images are analysed by the forensic experts cryptographic hashes are provided to courts for every relevant file, evidence etc.

Computer forensics and Mobile device forensics are done with the latest tools at par with the World wide standards.

Network forensic techniques though known to forensic examiners are yet evolving in India. A few cases have used these techniques and lot needs to be done in this regard.

2. Forensics Capacity

Though the LEAs have latest tools and techniques but the forensics part is done by the authorised Forensics organizations and not by LEAs. There is shortage of Forensic experts both at the Central and state level.

As regards the encryption, there are no legal remedies available to compel cooperation from the suspect as it would be against the spirit of Article 21 of Constitution.

3. Prosecution challenges and good practices

It is the need of the hour that Public Prosecutors, Legal advisors and also the Judges must be well versed with the changing trends in Cyber Crimes and they should also have thorough technical knowledge to understand a crime and the evidence brought before them.

Establishment of special courts can be one such idea which needs to be explored.

4. Legislation

To prevent cyber crime in India, the Specialized Act namely the Information Technology 2000 (as amended in 2008) and various provisions of Indian Evidence Act exist as of now. The Information Technology Act defines various technical terms used in the digital world.

The Electronic Record which includes printout on a paper, any information stored/recorded in optical or magnetic media, has now been treated as a document. The provisions of Indian Evidence Act pertaining to the procedural aspect of proving the document have suitably amended to include the Electronic Record as well.

Section 65 (B) of Indian Evidence Act deals with the admissibility of electronic record and necessary procedure to provide the same in the court.

Apart from the above, the National Cyber Security Policy, 2013 has also been formulated. It outlines a roadmap to create a framework for comprehensive and collective response to deal with the issue of cyber security at all levels within the country. It deals with measures with personal information, financial/banking information, sovereign data, et c. and also to facilitate the creation of secure computing environment.

5. Judicial Pronouncement

The Indian Judiciary is also sensitive to the issues of digital media and has time to time, provided interpretation in the grey areas. Such interpretations are valuable for the Law Enforcing agencies, prosecution department and other stakeholders of cyber crime.

The important judgments of Hon'ble Supreme Court that dealt with the issues of Section 65 (B) of Indian Evidence Act are Anvar PV vs PK Basheer (SC – 18.09.2014 (Full Bench) and Shafhi Mohd Vs. State of HP Supreme Court – 30.01.2018 (DB). In case of Anvar PV Vs. PK Basheer, the Hon'ble Supreme Court has held that electronic record which is to be produced in the court during evidence shall be accompanied by a certificate u/s 65 (B) of Indian Evidence Act from the competent authority as provided in the provisions of section 65 (B) of the said Act.

In case of Shafhi Mohd Vs State of HP, the Hon'ble Supreme Court of India further dealt with another grey area to prove the electronic record in the court. In this case, the Hon'ble Supreme Court of India has ordered that “we clarify the legal position on the subject on the admissibility of the electronic evidence, especially by a party who is not in a possession of device from which the document is produced, such party cannot be required to produce certificate under section 65B(4) of the Evidence Act”.

This order will be useful in the cases where the person in possession of electronic record is not in a position to produce 65 (B) for various reasons may be technical or otherwise.

6. Legal provisions on Electronic Evidence in India:

(i) As per **Section 2(t)** of the Information Technology Act, 2000, defines 'electronic record' as “data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro film”.

(ii) **Section 4 of the IT Act 2000 provides for Legal Recognition of Electronic Records, as under:**

Where any law provides that information or any other matter shall be in writing or typewritten or in printed form, then notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is-

- (a) rendered or made available in an electronic form; and
- (b) accessible so as to be usable for a subsequent reference.

(iii) **Section 17 of the Indian Evidence Act 1872** provides that an admission is a statement in [oral, document or electronic form] which suggests an inference to any fact in issue or of relevant fact and which is made by any of the persons, and under the circumstances.

(iv) **Sections 65A and 65B of Evidence Act 1872** pertain to admissibility of electronic evidence in Indian legal system.

7. International Cooperation:

India has Mutual Legal Assistance Treaty (MLAT) with 41 countries which takes care of sharing of information including on cybercrime. MHA is central authority for MLAT in criminal matters.

(B) Challenges and International Cooperation in Cybercrime:

1. Cybercrime is borderless by nature which also makes criminal investigations more complicated for law enforcement authorities. To effectively tackle cybercrime international cooperation amongst country need to be enhanced.
2. Time is the essence in cyber crime investigations and hence a timeframe for furnishing the digital evidence need to be defined for multilateral cooperation among member nations.
3. MLATs focus primarily on post crime scenarios, whereas, unlike traditional crimes, information exchange is essential for preventing cybercrime. There is also a need for cooperation in the field of cyber crime prevention.
4. MLATs have no clause for meeting the needs of emergent requirements, which is a key requirement for tackling cybercrimes. This aspect needs to be deliberated.
5. International cooperation in Cyber security is essential considering the widespread use of CnC, Botnets and deep web technologies.
6. Privacy laws and other laws of countries hinder in information sharing.
7. Information sought should be seen in the context of requesting party.
8. Mechanism to share intelligence on prevention of cybercrime needs to be deliberated.
9. There is a need for balancing internet freedom, privacy and security of State. Mandating KYC norms for use of Social Media platforms through framework may be helpful in containing misuse of cyberspace.
10. Grey Area vis a vis Prosecution in Cyber Crime Cases: As a general practice, the requirement of certificate u/s 65 (B) is insisted upon in all the cases where electronic record is produced in the form of evidence. Though, there are instances/cases where there is no requirement to obtain the certificate u/s 65 (B) of Indian Evidence Act. This issue has not been dealt with either in the Indian Evidence Act or in the Information Technology Act. Only the Hon'ble Supreme Court of India has recently ordered that a party who is not in a possession of device from which the document is produced, such party cannot be required to produce.
11. There is a lack of training institutions to educate on the technical issue of proving the electronic record in the court to the prosecutors. Only few experts are having the knowledge of this field but still there is a lack of concentrated effort to deal with the technical issues of proving the electronic record in the court.

(C) Recommendations:

- The legislative provisions need to be analyzed keeping in view the grey areas.
- The Training Institutions should be well equipped with the expert training personnels.
- The legislative provisions need to be analyzed from time to time
- There is a requirement for legislation to deal with the issues of cyber crime as it is having extra-territorial repercussions

Japan

1 Recognition of cybercrime

As cyberspace increasingly becomes part of people's living, cybercrime has become a serious social issue due to the occurrence of global scale damages from ransomware infections and cases in which unauthorized transmission of large monetary amounts apparently was carried out against domestic cryptocurrency exchange operators by malicious actors. In order to ensure the safety and security of the people, the government of Japan continues to work to grasp the actual state of cybercrime and promote a crackdown on such crime while cooperating with related institutions or organizations in carrying out public awareness campaigns to promote each individual person to take autonomous measures against cybercrime. Furthermore, we recognize that improvement of investigative and technological capabilities is also essential for addressing new types of cybercrime.

2 Current status of cybercrime in Japan

(1) Number of cleared cybercrime cases

The number of cleared cybercrime cases in 2017 was 9,014, which has increased by 690 (8.3%) compared to the previous year and recorded the highest number ever. 648 cases of them were for violation of the Act on Prohibition of Unauthorized Computer Access, 355 cases were for crime against computer or electromagnetic record. The number of cases of crime where information technology is used, which is the crime using advanced information communication network as a means indispensable for its commission, was 8,011.

(2) Number of consultations regarding cybercrime

The number of consultations with police concerning cybercrime in 2017 is about 130,000, which is still high from the previous year. About half of the consultations are the cases on fraud and illegal business practice.

3 Challenges posed and efforts taken to counter cybercrime with regards to investigation and use of digital evidence

(1) Strengthening the cybercrime investigation system

Dealing with threats in cyberspace has become a significant issue for all divisions of police, which requires the entire police force to strengthen their abilities to investigate and deal with such threats under a unified strategy. Therefore, in order to strengthen NPA's functions as headquarters for cyber security measures, the NPA in April 2014 established a Director-General position to manage and coordinate various cyber security initiatives.

The NPA has several departments to counter cybercrime and cyber-attacks as well as to support investigation for cybercrime and cyber-attacks. Each prefectural police construct has the same system as those of the NPA.

(2) Challenges in preserving traffic data and cooperation with private sector

In the event of cybercrime, it is necessary to ensure traceability in cyberspace for investigation. Securing communications history data log – traffic data - is essential for this. However, in Japan, there is no system in place which legally obliges service providers to retain such data on a daily basis. This is a major challenge when conducting cybercrime investigations.

In order to address this challenge, the police have been cooperating with the Ministry of Internal Affairs and Communications to promote adherence among the private sector with the "Guidelines on

the Protection of Personal Information in the Telecommunications Business”. This guideline, published by the Ministry, includes how to strike the balance between the need to secure evidence and the need to protect the secrecy of communication by setting out detailed guidance to the public sector regarding the specific period during which traffic data could be retained. It is expected that adherence to this guideline will enable the private sector to retain and provide traffic data to the investigative authorities in accordance with the principle of freedom of communication.

(3) Training and capacity building for law enforcement agencies

To address the threat in cyber space which is becoming more serious, the police are energetically working on training and securing cyber security personnel with both knowledge on investigation skills and information and communication technology (ICT). For this, the police adopt two measures which aim to train cyber security personnel within the police organization as well as to utilize knowledge of private enterprises.

(a) Training within the police organization

(i) Commission of a cyber security contest

The NPA holds a cyber security contest in which investigators from each prefectural police competes knowledge and skills related to dealing with threats of cyber space. Through this contest, the NPA endeavors to improve knowledge and skills among law enforcement agencies such as investigators by using scenarios modeled on actual cases, and also works to recruit talented people nationwide.

(ii) Efforts of the Research and Training Center for Cyber Security

The Research and Training Center for Cyber Security conducts research on state-of-the-art information and communication technologies (ICTs) that can be abused for cybercrime and also works to establish analyzing methods of various electronic equipments. The Center also distributes the outcome of its research to High-Tech Crime Technology Divisions nationwide. Also, each prefectural police conduct highly sophisticated and practical training modeled on actual cases for investigators in all divisions including investigators who are dedicated to fighting against cybercrime and cyber-attacks.

(b) Utilizing the knowledge of private enterprises

The NPA has taken actions to secure talented individuals from private enterprises through adopting mid-career recruitment, and collaborating with the Japan Cybercrime Control Center (JC3), which is an organization of industry/academia/government collaboration.

(4) Technical support for cybercrime crackdown

High-Tech Crime Technology Divisions are set up in the NPA and Regional Police Bureaus. They provide technical guidance to each prefectural police to appropriately seize computers at search and seizure sites and technical assistance by conducting analysis to extract information (evidence) from seized smartphones or computers.

The NPA have placed staff with highly specialized knowledge and skills at the NPA Digital Forensic Center. In addition, the Center has developed high performance analytical equipment and is conducting advanced analysis such as extraction of information recorded in damaged electronic devices.

(5) Efforts aimed at improving analysis capacity

The NPA are striving to accumulate know-how and techniques related to analysis of electromagnetic records, such as promoting technical cooperation with private enterprises, collecting

the latest technical information at all times, sharing information with domestic and overseas affiliated organizations.

4 Examples of recent successful prosecution of cybercrime

(1) First case is the mining case. The defendant created a mining program and uploaded it on to the internet disguising the program as an online games program. A third party, who did not know that the program was actually a mining program, downloaded the program and through this the defendant earned reward through the mining carried out by the said program installed into the device of the third party. The prosecutor secured evidence through the use of search and seizure and extraction of evidence from seized computers. The prosecutor charged the defendant with the crime of operating electromagnetic record giving an unauthorized command resulting in a conviction.

(2) Second case is the leech site case. Multiple defendants operated a so-called leech site that gathered links to websites containing data of manga and other books which was uploaded illegally. The prosecutor charged the defendants with the crime of violation of Copyright Act and secured convictions.

Netherlands

In his letter of 18 January 2019 (CU2019/4(A)/DTA/OCB/CSS) the Secretary-General of the UNODC invites participating countries in the IEG cybercrime to provide written comments, good practices, new information, national efforts as well as recommendations related to the main topics of the meeting to be held from 27 to 29 March 2019. In response The Netherlands expert delegation wishes to draw the attention to the following points.

Developments in The Netherlands

In order to evaluate the 2013 Chapters 5 and 6 of draft study we point at various relevant developments in the Netherlands.

General framework

The digital revolution offers major economies of scale and the possibility of connecting with people quickly and easily, no matter where they are in the world. The downside of this is that criminals also use the internet to significantly expand their activities. As a result, one in nine people were victims of cybercrime in 2017. Nowadays, more people are victims of hacking than of bicycle theft, and while crime in general is falling, cybercrime is not. Cybercrime has many faces, and its impact can be far-reaching. The term 'cybercrime' covers a wide range of different types of crime, including traditional offences in digital form as well as new forms of crime. Examples of cybercrime include hacking computers in order to transfer money to criminals' bank accounts and remotely activating devices' cameras and microphones in order to spy on people. Next to this, the more and more common use of digital equipment - eg smartphones - in everyday life leads to a sharp rise of electronic evidence in relation to traditional crime.

The anonymous and fast-paced nature of digital developments make investigating cybercrime particularly difficult. Communication via the internet is often anonymous and encrypted. Technology aimed at protecting users' privacy is also used by criminals to effectively mask their own identity. The

dark web hosts a diverse array of criminal marketplaces which facilitate the trade in items such as arms and narcotics. In addition, new digital products and services are being continuously developed, including ones that can be used for criminal purposes.

What sets the internet apart is the fact that it has no territorial boundaries. When it comes to organised cybercrime in particular, many of the perpetrators who target Dutch victims or use Dutch digital infrastructure for criminal purposes are not actually located in The Netherlands. There is usually no personal interaction between perpetrators and victims. Crimes can be carried out at several physical locations simultaneously, often across several different countries. Also, when it comes to offering services on the internet, the borderless nature of cyberspace is an essential and defining part. Data may be moved around servers all over the world, even taken apart, stored in particles and then only reassembled at the moment the user commands the data to be seen on a device. Cloud storage has become a huge and established service.

Such a multi-faceted phenomenon requires an integrated approach that ranges from prevention, investigation and prosecution, to reducing the rate of reoffending. The government plays various roles in this regard: it acts as an initiator, supporter, enforcer and, if necessary, creator of policy and legislation. Tackling cybercrime has a significant effect on strengthening cybersecurity, particularly when it comes to activities aimed at preventing cybercrime. The government's approaches to tackling cybercrime and strengthening cybersecurity are formulated in a cohesive manner in the broad-based National Cybersecurity Agenda².

The integrated approach to cybercrime comprises four focus areas:

1. Investment in prevention
2. Strengthening investigation, disrupting criminal activities and dealing with perpetrators
3. Tailoring support for victims of cybercrime
4. Enhancing academic research on cybercrime.

The second focus area is the most interesting one in light of the topics discussed in UN IEG cybercrime in March 2019.

Law Enforcement and Investigations

Criminal enforcement is one of the government's core tasks, also within the digital domain. Improvements in criminal enforcement remain necessary in order to protect (potential) victims and to ensure that crime doesn't pay. Addressing cybercrime as well as enhancing cybersecurity are government priorities. The current government's coalition agreement (2018-2022), 'Confidence in the Future', sets out investments in cybersecurity across various ministries. For cybercrime, this means a structural investment of up to €16 million a year. Furthermore, the coalition agreement sets out investments in the police force and the criminal justice system. The amounts set aside for this will be used in part to strengthen the approach to combating cybercrime and its knock-on effects. The Public Prosecution Service will receive a structural spending increase, which will be used for a limited expansion of capacity. In addition, a budget will be set aside for the establishment of a Digital Trust Center.

² https://english.nctv.nl/binaries/CSAagenda_EN_def_web_tcm32-339827.pdf

The High-Tech Crime Unit of the Central Unit of the National Police now has 120 members of staff. The police are strengthening cybercrime teams, both with detectives and digital forensics, in the 10 Regional Units of the National Police. The Public Prosecution Service has specialised capacity for investigating and prosecuting cybercrime at both the National Public Prosecutors' Office and the Regional Public Prosecutors' Offices. Both police and prosecution services developed and initiated specific training on cybercrime. The judiciary set up a dedicated expertise center. Because of required specialized skills, police and prosecution, next to adapting these skills in education of personnel pursuing a broad police career, also hire in ICT professionals. Recruiting those "side-entrants" and keeping them in the force for a longer period proves to be a difficult task because of their great attraction to a wide range of public and private organisations.

Police and prosecution services — according to the annual report of the National Police and the National prosecution service - succeeded in reaching almost all desired results in investigations and prosecutions, as stated in the National Agreement on Security between government, police, prosecution and local administrators³. When investigating cybercrime, international cooperation is essential. The Netherlands contributed to various international investigations, such as the taking down of huge internet marketplace (Hansa Market). Another success was the seizing of server holding data on so called PGP phones used by criminal organisations. We also highlight the start up of a proactive tool to mitigate the threat of ransomware with the launch of www.nomoreransom.org, set up together with international partners.

However, the current nature and scope of cybercrime, as well as its expected impact, still require additional strengthening of criminal justice expertise and practice, as well as appropriate powers. Since identifying and apprehending cybercriminals proves difficult, criminal activities will be disrupted through the application of new statutory powers set out in the Computer Crime III Act. This includes infiltrating servers and taking them offline. Disrupting activities is not only a case-specific response; it is also part of the wider strategy to combat cybercrime. Where necessary, proposals will be developed to adapt national and international legal frameworks. In addition, private parties will be consulted to make it harder for criminals to carry out their activities via legitimate service providers. To limit repeated offending, it is also vital that interventions targeting perpetrators of cybercrime are adapted to the risk factors that are relevant to them.

Electronic evidence and criminal justice

Today, much of the useful information needed for criminal investigations and prosecutions - be it traditional offences in general or in digital form as well as new forms of crime- is stored in the cloud, on a server in another country and/or held by service providers that are located in other countries. Even when all other elements of a case are located in the investigating country, the location of the data or of the service provider can create a cross-border situation.

First of all, The Dutch police and judicial authorities are equipped with the necessary powers to retrieve electronic evidence. From 2006 onwards the Dutch legislation has been adapted towards this need. Starting with the transposition of the powers as laid down in the 2001 Cybercrime Convention, or Budapest Convention, in particular search and seizure powers and the power to order disclosure of data and the power to preserve data awaiting the order to disclose data. Because of the ever-growing

³ These are four year agreements. The results referred to here fall under the agreement 2015-2018, currently a new agreements for 2019-2022 is in force.

number of State parties to the convention - 62 current - this also lays a foundation for international cooperation.

Second, the police and prosecution services, as noted already above, invested heavily in investigation capacity and expertise, also when it comes to digital forensic expertise.

Acquiring timely and effective access to electronic evidence over the years proved to be harder and harder. Because of the rising volume of data, resulting of the already mentioned increase of digitization in everyday life in both open as hidden cyberspace (dark net), the huge industry of cloud computing that emerged as well as the trend of safeguarding privacy via inbuilt protection in both software and hardware relating to encryption.

Especially the borderless nature of cyberspace makes it hard to operate fast and effective in criminal investigations. To obtain electronic evidence stored abroad and/or by a service provider located in another country, EU national authorities such as The Netherlands rely on either traditional existing judicial cooperation tools or voluntary cooperation from service providers. For requests within the EU, judicial authorities normally use the European Investigation Order to obtain evidence. The limits of Mutual Legal assistance, which proves to be a too lengthy process, have now been reached. It may easily happen that data no longer exists or has been altered when the MLA procedure is fulfilled. It also proves to be impossible to engage in mutual legal assistance if police and justice authorities do not know where data are located and thus cannot determine a concrete other State or service provider to ask for assistance. Because of this lack of knowledge of location, many investigations have to be stopped and justice is not served.

In recent years, the Netherlands has led the way in discussing on improving international frameworks for online investigation and will continue these efforts, both in the EU and the Council of Europe. These frameworks should help make gaining access to electronic data faster and more efficient. In the meantime The Netherlands try to make the best use of existing powers, like the power to order subscriber information with service providers not established in the Netherlands but offering services in the Netherlands, using the Guidance Note on the article 18, para 1, b, of the Cybercrime Convention. Over time case law is developed to better define the boundaries of existing powers, eg, when it comes to extended network search. From March St 2019, The Netherlands enact new statutory powers set out in the Computer Crime III Act on remote searches.

Next to this, The Netherlands maintain good relations with many US based service providers which may voluntary disclose subscriber data upon request from non US governments.

Closing remarks

Drivers for the effectiveness of the practices as described above are:

- Emphasis on a dedicated legal framework for procedural powers in the investigation of traditional offences in general or in digital form and new forms of crime, as well as for gathering electronic evidence. The ratification of the cybercrime convention, the subsequent studies on implementation of the convention and on related topics, the discussion thereof in the Cybercrime convention committee and the issued Guidance notes have been of great help.
- Specific and structural attention for capacity, education and training, specific digital skills within police, prosecution and judiciary are vital.

- Constant innovation of the possibilities of acquiring access to data, also in cross border situations, is highly needed.
- In order to pursue a more effective result, adopting policy frameworks like an integrated plan of action for addressing cybercrime and a cyber security agenda, adequate budgets for implementation there of are necessary.

Russian Federation

I. Общие комментарии

Проблема противодействия использованию информационно-коммуникационных технологий (ИКТ) в преступных целях по своему масштабу и всеохватности давно превратилась в глобальную угрозу, от которой страдают как развивающиеся, так и развитые страны. Если в 2017 г. потери мировой экономики от этой угрозы оценивались в 1 трлн. долл. в год, то в 2018 г. эта цифра возросла до 1.5 трлн.

Эти цифры – подтверждение того, что существующие уголовно-правовые механизмы в этой сфере буксуют, а международное сотрудничество заметно отстает от противоправных деяний. На наш взгляд, давно назрела необходимость в разработке уголовно-правовой конвенции под эгидой ООН в данной сфере, которая учитывала бы современные реалии и принципы суверенного равенства и невмешательства во внутренние дела государств.

II. Комментарии по темам V заседания МГЭ

1. Правоохранительная деятельность и расследования

В связи с интенсивным развитием информационного общества все большую актуальность приобретает совершенствование правового регулирования общественных отношений в сфере обеспечения информационной безопасности. Вопросам противодействия информационной преступности в ее широком понимании в Российской Федерации уделяется большое внимание.

Уголовным кодексом Российской Федерации (УК РФ) предусмотрена ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если деяние повлекло уничтожение, блокирование, модификацию либо копирование информации; за

создание, использование и распространение вредоносных программ для ЭВМ; за причинившее крупный ущерб нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Уголовное наказание установлено за побуждение к самоубийствам и содействие совершению самоубийств с использованием интернет - ресурсов, в том числе за вовлечение в это несовершеннолетних.

Статьей 159.6 УК РФ установлена ответственность за мошенничество в сфере компьютерной информации. Кроме того, совершение преступления с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет») рассматривается в целом ряде составов в качестве криминообразующего или квалифицирующего признака.

В январе 2018 года в России вступила в силу норма УК РФ об ответственности за неправомерное воздействие на критическую информационную структуру Российской Федерации.

К числу наиболее распространенных киберпреступлений в России относятся: хищение денежных средств через информационно-коммуникационные сети, в том числе Интернет, компьютерный шпионаж, распространение идей терроризма и экстремизма, иной запрещенной информации, представляющей опасность для общества.

В 2018 году в Российской Федерации зарегистрировано 4917 преступлений, предусмотренных статьей 159.3 УК РФ (Мошенничество с использованием электронных средств платежа) (в 2017 г. – 228), 970 преступлений, предусмотренных статьей 159.6 УК РФ (Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей) (в 2017 г. – 2195), 1761 преступление, предусмотренное статьей 272 УК РФ (Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации) (в 2017 г. – 1079), 733 преступления, предусмотренные статьей 272 УК РФ (Создание, использование и распространение вредоносных компьютерных программ, т.е. создание, распространение или использование компьютерных программ либо

иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации) (в 2017 г. – 802).

2. Сбор электронных доказательств

В Уголовно-процессуальном кодексе Российской Федерации (УПК РФ) отсутствует определение термина «электронные доказательства».

Вместе с тем, согласно статье 74.1 УПК РФ доказательствами по уголовному делу являются любые сведения, на основе которых суд, прокурор, следователь, дознаватель в порядке, определенном УПК РФ, устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела.

В статье 81.1 УПК РФ закреплено, что вещественными доказательствами признаются любые предметы:

1) которые служили орудиями, оборудованием или иными средствами совершения преступления или сохранили на себе следы преступления;

2) на которые были направлены преступные действия;

2.1) деньги, ценности и иное имущество, полученные в результате совершения преступления;

3) иные предметы и документы, которые могут служить средствами для обнаружения преступления и установления обстоятельств уголовного дела.

Вещественные доказательства в виде электронных носителей информации:

а) хранятся в опечатанном виде в условиях, исключающих возможность ознакомления посторонних лиц с содержащейся на них информацией и обеспечивающих их сохранность и сохранность указанной информации;

б) возвращаются их законному владельцу после осмотра и производства других необходимых следственных действий, если это возможно без ущерба для доказывания (пункт 5 части 2 статьи 82 УПК РФ).

После производства неотложных следственных действий в случае невозможности возврата изъятых в ходе производства следственных действий электронных носителей информации их законному владельцу содержащаяся на этих носителях информация копируется по ходатайству законного владельца изъятых электронных носителей информации или обладателя содержащейся на них информации. Копирование указанной информации на другие электронные носители информации, предоставленные законным владельцем изъятых электронных носителей информации или обладателем содержащейся на них информации, осуществляется с участием законного владельца изъятых электронных носителей информации или обладателя содержащейся на них информации и (или) их представителей и специалиста в присутствии понятых в подразделении органа предварительного расследования или в суде. При копировании информации должны обеспечиваться условия, исключающие возможность ее утраты или изменения. Не допускается копирование информации, если это может воспрепятствовать расследованию преступления. Электронные носители информации, содержащие скопированную информацию, передаются законному владельцу изъятых электронных носителей информации или обладателю содержащейся на них информации. Об осуществлении копирования информации и о передаче электронных носителей информации, содержащих скопированную информацию, законному владельцу изъятых электронных носителей информации или обладателю содержащейся на них информации составляется протокол в соответствии с требованиями статьи 166 УПК РФ (часть 2.1 статьи 82 УПК РФ).

При наличии достаточных оснований полагать, что сведения, имеющие значение для уголовного дела, могут содержаться в электронных сообщениях или иных передаваемых по сетям электросвязи сообщениях, следователем по решению суда могут быть проведены их осмотр и выемка (часть 7 статьи 185 УПК РФ)

При наличии достаточных оснований полагать, что телефонные и иные переговоры подозреваемого, обвиняемого и других лиц могут содержать сведения, имеющие значение для уголовного дела, их контроль и запись допускаются при производстве по уголовным делам о преступлениях средней тяжести, тяжких и особо тяжких преступлениях на основании судебного решения, принимаемого в порядке, установленном статьей 165 УПК РФ настоящего Кодекса. При наличии угрозы совершения насилия, вымогательства и других преступных

действий в отношении потерпевшего, свидетеля или их близких родственников, родственников, близких лиц контроль и запись телефонных и иных переговоров допускаются по письменному заявлению указанных лиц, а при отсутствии такого заявления - на основании судебного решения. Постановление о производстве контроля и записи телефонных и иных переговоров направляется следователем для исполнения в соответствующий орган. Производство контроля и записи телефонных и иных переговоров может быть установлено на срок до 6 месяцев. Оно прекращается по постановлению следователя, если необходимость в данной мере отпадает, но не позднее окончания предварительного расследования по данному уголовному делу (статья 186 УПК РФ).

При наличии достаточных оснований полагать, что информация о соединениях между абонентами и (или) абонентскими устройствами имеет значение для уголовного дела, получение следователем указанной информации допускается на основании судебного решения, принимаемого в порядке, установленном статьей 165 УПК РФ. В случае принятия судом решения о получении информации о соединениях между абонентами и (или) абонентскими устройствами его копия направляется следователем в соответствующую осуществляющую услуги связи организацию, руководитель которой обязан предоставить указанную информацию, зафиксированную на любом материальном носителе информации. Указанная информация предоставляется в печатанном виде с сопроводительным письмом, в котором указываются период, за который она предоставлена, и номера абонентов и (или) абонентских устройств. Получение следователем информации о соединениях между абонентами и (или) абонентскими устройствами может быть установлено на срок до шести месяцев. Соответствующая осуществляющая услуги связи организация в течение всего срока производства данного следственного действия обязана предоставлять следователю указанную информацию по мере ее поступления, но не реже одного раза в неделю. Следователь осматривает представленные документы, содержащие информацию о соединениях между абонентами и (или) абонентскими устройствами, с участием специалиста (при необходимости), о чем составляет протокол, в котором должна быть указана та часть информации, которая, по мнению следователя, имеет отношение к уголовному делу (дата, время, продолжительность соединений между абонентами и (или) абонентскими устройствами, номера абонентов и другие данные). Представленные

документы, содержащие информацию о соединениях между абонентами и (или) абонентскими устройствами, приобщаются к материалам уголовного дела в полном объеме на основании постановления следователя как вещественное доказательство и хранятся в опечатанном виде в условиях, исключающих возможность ознакомления с ними посторонних лиц и обеспечивающих их сохранность (статья 186¹ УПК РФ).

В Российской Федерации при исполнении запроса о правовой помощи по уголовному делу применяются нормы УПК РФ, однако могут быть применены процессуальные нормы законодательства иностранного государства в соответствии с международными договорами Российской Федерации, международными соглашениями или на основе принципа взаимности, если это не противоречит законодательству и международным обязательствам Российской Федерации (часть 2 статьи 457 УПК РФ).

III. Рекомендации

Российская Федерация продолжает призывать международное сообщество приступить к принятию решительных мер для борьбы с глобальной преступностью в сфере использования ИКТ. В подобных условиях очевидна необходимость выработки универсальных принципов и норм, которые разделяли бы все заинтересованные стороны и которые закладывали бы основы эффективного международного сотрудничества в данной сфере.

Таким инструментом могла бы стать подготовленная под эгидой ООН Конвенция по противодействию преступлениям в сфере использования ИКТ, которая учитывала бы реалии всех без исключения стран и основывалась бы на принципах суверенного равенства сторон и невмешательства во внутренние дела государств. Идея разработки подобного документа впервые была отражена в итоговой декларации 12-го Конгресса ООН по предупреждению преступности и уголовному правосудию (Бразилия, апрель 2010 года).

В основу такой работы мог бы лечь российский проект универсальной конвенции ООН о сотрудничестве в сфере противодействия информационной преступности, который 28 декабря 2017 г. был распространен в качестве официального документа Генассамблеи ООН (№A/C.3/72/12).

Предполагаем, что представленный проект конвенции станет «пищей для размышлений», позволит начать дискуссию по данной теме на ключевых международных площадках, в первую очередь, ООН, а также объединит и направит усилия мирового сообщества на выработку практических решений в этой области.

United States of America

The Permanent Mission of the United States of America is pleased to respond to the Note Verbale of January 18, 2019 (CU 2019/4(A)/DTA/OCB/CSS) regarding the organization of the fifth meeting of the Open-Ended Intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime (Expert Group), and to provide written comments on the main topics under consideration at this meeting. In this context, the United States submits the following comments regarding the substantive content contained in Chapter 5 (Law Enforcement and Investigations) and Chapter 6 (Electronic Evidence and Criminal Justice) of the Draft Comprehensive Study on Cybercrime (Draft Study) produced by the UN Office on Drugs and Crime (UNODC) for further consideration by the Expert Group.

Chapter 5 - Law Enforcement and Investigations

As the Draft Study notes, more than half of countries report that between 50 and 100 percent of cybercrime involve a transnational element. Cybercrime requires medium- and long-term law enforcement strategies, including cooperation with international partners, to disrupt cybercrime markets. These strategies must be proactive and target organized cybercrime groups, which may have members in numerous countries. An effective domestic law enforcement response depends on three key factors:

1. a legal framework based on widely adopted standards for substantive offenses and procedural authorities for investigation;
2. use of investigative tools and best practices in online investigations; and
3. sufficient and continuous training for police and forensic analysts in handling electronic evidence.

These factors strengthen domestic law enforcement capability and are the foundation for effective and timely international cooperation.

Effective Legal Frameworks

Member states continue to accede to the Budapest Convention on Cybercrime because it provides a common legal framework for both substantive offenses and procedural authorities. In addition, the Convention serves as a mutual legal assistance agreement for parties. The Convention continues to receive international acceptance even by countries which choose not to accede because its provisions meet prevailing and widely adopted international standards. In addition to substantive

provisions, which have been incorporated into every regional instrument, the Convention provides for harmonized investigative authorities, which are crucial for transnational cybercrime investigations.

Some member states noted that under their domestic law, traditional procedural authorities may not be applicable to intangible data or may not authorize sufficiently rapid collection of volatile electronic evidence. As ever, outdated laws will not be sufficient to meet the many challenges of electronic crime investigations, including novel technologies such as widespread encryption and cloud computing services. Specialized procedural authorities for cybercrime investigation are essential. These laws should be drafted with applicable technical concepts in mind as well as the practical needs of cybercrime investigators. Member states should ensure that domestic legislation authorizes:

1. Requests for expedited preservation of computer data to the person in control of the data—that is, internet and communications service providers—to keep and maintain the integrity of the data for a specified period of time. Because of the potential volatility of this data, preservation of information is essential;
2. Search and seizure of stored content data and computer data from digital devices, which is often the most relevant evidence of an electronic crime to prove attribution;
3. Orders to produce computer data that may have less privacy protection, such as traffic data and subscriber data; and
4. Real-time collection of traffic data and content in appropriate cases.

In ensuring a legal basis for these procedural tools, member states should also consider appropriate limits and safeguards to balance law enforcement interests and privacy and human rights concerns. These limits and safeguards depend on the existing domestic framework and may include, for example: judicial oversight of law enforcement orders to produce data; the legal standards for such orders, such as reasonable suspicion or probable cause for search warrants; and appropriate oversight of investigative techniques for real-time collection of data.

Technical Assistance and Capacity Building

More than 75% of countries have a dedicated unit for cybercrime-related issues within existing law-enforcement organizations, and about 15% have a specialized dedicated agency for cybercrime. This underscores the specialized nature of cybercrime investigation, including the need for specialized training. Moreover, as the Draft Study notes, the “complexity of cybercrime offenses and cybercrime elements of traditional offenses has increased significantly, which places additional demands for the training and maintenance of highly-skilled investigators and technical experts.”

The United States believes that insufficient domestic capability is the most common reason for countries to fail to cooperate internationally. For most countries, international cooperation does not fail from lack of will, but from limitations either in domestic law or in the expertise of law enforcement agencies. The Draft Study notes that many member states, particularly developing countries, are not well resourced with respect to law enforcement capacity for cybercrime or handling electronic evidence. According to the Draft Study, some 70% of specialized law enforcement officers in developing countries lack computer skills and equipment. Accordingly, there is international consensus that technical assistance and capacity building for law enforcement agencies remains the most urgent requirement for an effective response to cybercrime. Moreover, as electronic evidence

becomes a component of almost every type of crime, even “non-specialized” law enforcement officers will require some basic understanding of computer-related investigations.

Chapter 6 - Electronic Evidence and Criminal Justice

Criminal justice systems rely on the lawful collection of accurate and reliable evidence to present to a neutral fact-finder such as a judge or a jury. While cybercrime prosecutions in most cases do not rely solely on digital evidence and the entire body of traditional investigative techniques—such as reliance on witness interviews and analog evidence—are employed, electronic evidence is at the heart of cybercrime prosecutions and is increasingly important to proving criminal cases in general. In these cases, successful prosecutions depend on maintaining the integrity of digital information from collection to presentation as evidence. In addition, trained and specialized prosecutors and a judiciary informed and familiar with electronic evidence and cybercrime are also essential elements of a comprehensive response to cybercrime.

Digital Forensics

Digital forensic experts support successful cybercrime prosecutions by examining electronic devices, to collect evidence in a reliable manner. Electronic evidence may be collected from devices, from network servers, and from “cloud” servers. As with investigative resources, countries report insufficient numbers of forensic examiners, a lack of forensic tools, which are often expensive, and difficulties that arise from the sheer quantity of collected data for analysis. Developing countries, in particular, highlight a lack of resources for forensics equipment and challenges in recruiting personnel with sufficient skills. These challenges are compounded when dealing with the widespread use of encryption technologies. As the Draft Study notes, encryption is a “daunting challenge” for every police force in the world.

Prosecutors

In addition to law enforcement training, the Draft Study also notes that prosecutors must have sufficient training and resources to handle and present electronic evidence. At the federal level, the United States employs the “prosecution team” approach, which combines the skills and resources of various agencies to bring together prosecutors, investigative agents, and forensic analysts to pursue an investigation. Engagement by all law enforcement stakeholders at the beginning of an investigation multiplies the capabilities of the “prosecution team,” which in turn increases the likelihood of a successful outcome. The Draft Study similarly notes that close working relationships on the prosecution team may result in the increased successful collection of relevant, properly authenticated evidence. However, in many countries, there is sometimes little or no coordination early in an investigation among the various law enforcement participants. This ad-hoc, approach, drawn from investigation models for traditional crimes, is generally not suitable to strategic, pro-active cybercrime investigations, which often involve complicated legal and evidentiary questions. On the other hand, specialized teams for cybercrime investigations can be expensive to maintain.

Prosecutors also note the delay in international cooperation procedures as posing additional challenges. Much of the delay in the mutual legal assistance process may be ameliorated by further training on mutual legal assistance requirements and procedures, including the drafting of sufficient requests for electronic evidence.

Judiciary

Finally, no less than police and prosecutors, the judiciary may also benefit from cybercrime-specific training. Specialized cybercrime judges are usually not necessary in legal systems that use an adversarial adjudication model and indeed may be counterproductive because electronic evidence frequently appears in all types of criminal and civil cases. In contrast, in legal systems that use an inquisitive model, where judicial officers are also investigators, specialized training for judicial officers is necessary.

As noted above, evidence is admitted based on rules that must be updated to account for electronic evidence. This is critical, as proof of a defendant's criminal liability will depend on the persuasiveness of evidence, including digital information, and inferences to establish the defendant's access, motivation, opportunity, and knowledge with which to commit the crime. According to the Draft Study, electronic evidence is admissible in court in more than 85% of responding countries. However, in some countries, because judges are unfamiliar with digital evidence, this type of evidence is often subjected to higher standards for authentication and admission. It should be noted that there is no practical reason to impose higher standards for the integrity of digital evidence in contrast to traditional evidence. Digital evidence is no more likely to be altered or fabricated than other evidence. Indeed, it is arguably harder to alter or fabricate digital evidence because various mathematical algorithms, i.e. "hash values," can be used to authenticate or prove an alteration.

Similarly, admissibility should not depend on whether evidence was collected from outside a country's jurisdiction, as long as the reliability of the evidence is not impaired and the evidence is lawfully collected, for example, pursuant to an MLA agreement, multilateral agreement, or in cooperation with the country that has jurisdiction. Because cybercrime evidence is often located outside a country's jurisdiction, a blanket prohibition on admissibility of such evidence would significantly impair investigations and prosecutions.

Morocco

Please see below (two submissions)



إن تطور الجريمة واستغلالها لوسائل الاتصال الحديثة أصبح يفرض على مختلف التشريعات إيلاء أهمية خاصة لهذا النوع من الجرائم التي أصبح البعض يصنفها ضمن خانة الجرائم التكنولوجية. كل هذا التحول الذي عرفته الظاهرة الإجرامية حديثا يعطي انطبعا على أننا لم نعد أمام جريمة عادية أو أمام جريمة بشكلها الكلاسيكي، بل أصبحنا أمام زمرة جديدة من الجرائم التي يمكن تصنيفها ضمن خانة الجرائم المنظمة، حيث يتقاطع ارتكاب هذه الجرائم في استغلالها لشبكة الإنترنت من أجل التواصل والتخطيط لتنفيذ مشاريعها الإجرامية. ويقع هذا في الوقت الذي أصبح فيه المجال المعلوماتي وشبكة الإنترنت مجالا خصبا لارتكاب الجريمة سواء من خلال استعمالهما كوسيلة أو كهدف للجريمة في حد ذاتها. ولا شك في أن هذا الواقع بات يتطلب من التشريعات الحالية مواكبة هذا النوع من الجرائم وذلك عبر وضع آليات قانونية ومؤسسية كفيلة بمكافحتها.

لذلك ووعيا بأهمية مكافحة هذا النوع من الجرائم، بادر المغرب إلى المصادقة على الاتفاقية الأوروبية المتعلقة بالجريمة المعلوماتية الموقعة ببودابست في 23 نونبر 2001 وبروتكولها الإضافي الموقع بستراسبورغ في 28 يناير 2003، حيث دخلت حيز النفاذ بتاريخ فاتح أكتوبر 2018. كما بدار المغرب إلى وضع آليات قانونية لمكافحة جرائم الحاسوب من خلال سن قانون خاص بالمس بنظام المعالجة الآلية للمعطيات يهدف إلى حماية الأنظمة وبرامج الحاسوب ومكافحة استغلالها في ارتكاب الجريمة.

ومن أجل مكافحة استخدام تقنيات المعلومات وبرامج الحاسوب في ارتكاب مثل هذه الجرائم، بادر المشرع المغربي إلى مراجعة قانون المسطرة الجنائية بهدف ملاءمة تشريعه الداخلي مع الاتفاقيات الدولية المعنية بمكافحة جرائم الحاسوب لا سيما اتفاقية بودابست المذكورة، كما وضع آليات قانونية تسمح بمكافحة هذا النوع من الجرائم الذي باتت خطورته تزداد يوما عن يوم، وفي هذا الإطار تم وضع مقتضيات إجرائية خاصة بالبحث والتحري لتلاءم

وطبيعة هذه الجريمة كما تم وضع مقتضيات قانونية تلاءم طبيعة إجراءات التفتيش والحجز المرتبطة بهذا النوع من الإجرام.

ولضمان السرعة اللازمة لتجميع الأدلة المرتبطة بجرائم الحاسوب، خاصة وأن آثارها يمكن أن تندثر بسرعة، راعى مشروع قانون المسطرة الجنائية أهمية وضع مقتضيات تشريعية تتوخى سرعة التحفظ على البيانات المخزنة بالحاسوب علما بأن عملية التجميع الفوري أو ما يعرف بالتجميع في الوقت الحقيقي تتطلب إمكانيات تقنية وبشرية مؤهلة بإمكانها جمع المعلومات والبيانات المطلوبة في الوقت المناسب، وهو ما يتجلى من خلال تشكيل فرق للبحث متخصصة في هذا النوع من الإجرام.

والجدير بالذكر أن طبيعة البحث في الجرائم المعلوماتية، يتطلب إيجاد أطر بشرية مؤهلة للتعامل مع هذا النوع من الجرائم وتوفير الإمكانيات التي تمكنها من قيامها بمهمتها في الوقت وبالشكل المطلوب. وفي هذا الإطار قامت وزارة العدل بتنظيم عدة دورات تكوينية لفائدة القضاة وضباط الشرطة القضائية بتعاون مع خبراء دوليين متخصصين في الميدان تم خلالها إطلاعهم على التجارب الرائدة في هذا المجال وعلى تقنيات البحث الحديثة من أجل تمكينهم من مواكبة التطور الذي يعرفه البحث الجنائي بالنسبة للجريمة المعلوماتية التي أصبحت جريمة عابرة للحدود ومرتبطة بجرائم دولية أخرى أقل ما يقال عنها أنها تدخل في خانة الجرائم المنظمة.

ولما كانت الجريمة المعلوماتية من صنف الجرائم العابرة للحدود، فإن تعزيز التعاون الدولي بين الدول يظل مدخلا أساسيا لمكافحة هذه الجريمة التي باتت تتجاوز الحدود الجغرافية وتمس مصالح أكثر من دولة، ولهذا فالتعاون الدولي بجميع أشكاله القضائي والأمني يبقى سبيلا أساسيا لتطويق هذه الظاهرة، التي يمكن في إطارها توظيف القدرات الذاتية واستغلال الآليات القانونية والمؤسسية من أجل مكافحة الجريمة المعلوماتية.

ولتعزيز هذا الجانب، فقد تضمن القانون المغربي مقتضيات جد مرنة على مستوى العلاقات القضائية مع السلطات الأجنبية تسمح بتعزيز التعاون القضائي بين الدول وتمكن

من تقديم المساعدة اللازمة وتنفيذ طلبات التعاون القضائي في مجال مكافحة الجريمة بشتى أنواعها.

ومن أجل تقريب وضعية قانون المسطرة الجنائية إزاء ما نصت عليه الاتفاقية الدولية لمكافحة الجريمة المعلوماتية وكذا أيضا تجاه ما أخذت به بعض التشريعات المقارنة، فإننا سنقوم ببسط هذه الجوانب اتباعا كما يلي:

أولا: الجوانب الإجرائية المتعلقة بالبحث والتحري عن الجريمة المعلوماتية في قانون

المسطرة الجنائية ومدى ملاءمتها مع اتفاقية بودابست.

نصت المادة 14 من اتفاقية بودابست التي جاءت ضمن أحكام الباب الثاني المعنون بالقانون الإجرائي على أنه يتعين على الدول الأطراف أن تتخذ تدابير تشريعية، وتدابير أخرى من أجل إقرار الإجراءات التي نصت عليها هذه الاتفاقية.

وإذا ما حاولنا استقراء النصوص القانونية المتعلقة بإجراءات البحث بالشكل الذي جاءت به في قانون المسطرة الجنائية، فإنه يمكن القول بداية بأن الإجراءات التي نص عليها قانون المسطرة الجنائية فيما يخص البحث والتحري عن الجرائم، هي إجراءات لا تخص جريمة معينة دون أخرى، بل هي قواعد عامة يمكنها أن تنطبق على كافة الأفعال المخالفة للقانون بما فيها الجريمة المعلوماتية التي تبقى وإن اختلفت عن غيرها من الجرائم في طبيعتها أو خصائصها إلا أنها تظل خاضعة من حيث المبدأ للقواعد العامة التي تسري على جميع الجرائم.

وهكذا فباستقراء مقتضيات المادة 57 نجد بأنها أناطت بالشرطة القضائية جمع وحفظ الأدلة والأدوات التي استعملت في ارتكاب الجريمة بغض النظر عن طبيعة هذه الأخيرة.

وبالإضافة إلى المادة 57، فإن مقتضيات المادة 59 من قانون المسطرة الجنائية نصت على قواعد إجرائية يمكن أن تستوعب حتى الجريمة المعلوماتية بحيث أناطت هذه المادة بضباط الشرطة القضائية كلما تعلق الأمر بجناية أو جنحة بأن يقوموا بحجز الأوراق والوثائق والمستندات والأشياء الأخرى المتعلقة بالأفعال الإجرامية.

غير أنه وبالرغم من اتساع هذه المقتضيات التي يمكن أن تشمل في تطبيقها حتى الجريمة المعلوماتية إلا أنه تم التفكير في وضع مقتضيات قانونية تلاءم طبيعة هذه الجريمة التي تتميز بسرعة اندثار آثارها، لاسيما فيما يخص إجراءات البحث وحجز البيانات والوثائق المعلوماتية وتفتيش الأجهزة أو الأنظمة المعلوماتية على غرار ما هو منصوص عليه في بعض التشريعات المقارنة كالقانون الفرنسي (المادة 56 من القسم الخاص بالجرائم وحالات التلبس) حيث نصت هذه المادة على أنه في حالة ما إذا كانت الجريمة المرتكبة مما يمكن إثباته بواسطة معطيات أو وثائق معلوماتية توجد في حوزة الغير، فإنه يمكن لضابط الشرطة القضائية أن ينتقل إلى مقر هذا الأخير، لإجراء تفتيش وتحرير محضر في الموضوع.

ومن هذا المنطلق جاء مشروع قانون المسطرة الجنائية المعروض عليها على الأمانة العامة للحكومة كإجراءات التحقيق في الجرائم المعلوماتية، لاسيما عمليات الحجز من طرف الشرطة القضائية وذلك في المواد 59 إلى 60، حيث حدد طريقة حجز المعطيات والبرامج الإلكترونية في وضع الدعامات المادية المتضمنة لهذه المعلومات أو بأخذ نسخ منها، بحضور الأشخاص الذين حضروا التفتيش ووضعها رهن إشارة العدالة، واشترط لذلك أن تكون ضرورية لإظهار الحقيقة. كما نص على ضرورة قيام ضابط الشرطة القضائية بإحصاء تلك المعطيات والبرامج المعلوماتية وثفها أو وضعها في غلاف أو وعاء أو كيس والختم عليها. كما خول لضابط الشرطة القضائية إمكانية استدعاء أي شخص لسماعه، إذا تبين له أن بوسع هذا الشخص أن يمدّه بمعلومات حول المعطيات أو الأدوات أو البرامج المعلوماتية المحجوزة، وأن يرغمه على الحضور في حالة امتناعه بعد إذن النيابة العامة؛

ومن ناحية أخرى خول للوكيل العام للملك أو وكيل الملك كل فيما يخصه، صلاحية الأمر بالحذف النهائي للمعطيات أو البرامج المعلوماتية الأصلية من الدعامات المادية التي لم توضع رهن إشارة المحكمة بعد أخذ نسخة منها إذا كانت حيازتها أو استعمالها غير مشروع أو كانت تشكل خطرا على أمن الأفراد أو الممتلكات أو منافية للأخلاق العامة.

كما أجاز المشروع لقاضي التحقيق اتخاذ نفس الإجراءات المذكورة والخولة لضابط

الشرطة القضائية طبقا للمادة 104.

هذا وقد عاقب المشروع بموجب المادة 105 كل إبلاغ أو إفشاء لمعطيات أو برامج معلوماتية وقع الحصول عليها من تفتيش، يتم لفائدة شخص ليست له صلاحية قانونية للاطلاع عليها دون الحصول على موافقة المشتبه فيه أو ذوي حقوقه أو الموقع عليها أو من وجهت إليه وكل استعمال آخر لها، بالعقوبات المقررة في الفصل 446 من مجموعة القانون الجنائي.

أما بخصوص وضعية قانون المسطرة الجنائية إزاء المادة 14 من اتفاقية بودابست، فهي تنطبق على المادة 15 منها والتي نصت على أنه على الدول الأطراف أن تكون الإجراءات المتخذة خاضعة للضمانات والشروط المنصوص عليها في قانونها الوطني وهو مقتضى يعتبر من المبادئ الأساسية في النظام القانوني المغربي الذي يشرف فيه قضاة النيابة العامة على الأبحاث الجنائية ويقومون بتسيير عمل الشرطة القضائية المكلفة بالبحث والتحري عن الجرائم.

ولضمان السرعة اللازمة لتجميع الأدلة المتعلقة بالجريمة المعلوماتية لاسيما أن آثارها يمكن أن تندثر بسرعة، فقد نصت المادتين 16 و17 من اتفاقية بودابست على ضرورة وضع مقتضيات تشريعية تتوخى سرعة التحفظ على البيانات المخزنة بالكومبيوتر.

إن استقراء مقتضيات المادة 57 من قانون المسطرة الجنائية يفيد أن النص المغربي راعى عامل الزمن في جمع الأدلة المرتبطة بالجريمة، فوفقا لهذه المادة، فإن ضابط الشرطة القضائية يتعين عليه أن ينتقل فورا إلى مكان ارتكاب الجريمة وأن يجري المعاينات اللازمة بشأنها وأن يحافظ على الأدلة القابلة للاندثار، علما بأن الجريمة المعلوماتية ينطبق عليها هذا الوصف لأنها يمكن أن ترتكب في وقت قصير ثم تختفي معالمها بعد ذلك بسرعة.

وبالإضافة إلى ذلك، فقد ألزم قانون المسطرة الجنائية ضابط الشرطة القضائية بأن يحافظ على جميع الأشياء التي يمكن أن تساعد على إظهار الحقيقة وأن يقوم بحجز الأدوات التي تم استعمالها في ارتكاب الجريمة.

ولضمان البحث في مواجهة الأشخاص الذين يحوزون إحدى الوثائق أو البيانات المعلوماتية، فقد نصت المادة 18 من الاتفاقية الدولية على أنه يتعين على الدول الأطراف أن

تتخذ التدابير التشريعية التي تسمح بمطالبة كل شخص أو متعهد للخدمات بتقديم المعلومات التي توجد في حوزته أو تحت سيطرته.

ويمكن أن نجد تطبيقات هذه المادة في المقتضيات التي نصت عليها المادة 59 من قانون المسطرة الجنائية كقاعدة عامة يمكنها أن تنسحب أيضا على الجريمة المعلوماتية إضافة إلى المادة 114 التي نصت على أنه يمكن قصد القيام بعمليات التقاط الاتصالات المأذون بها وتسجيلها وأخذ نسخ منها وحجزها، الحصول على المعلومات والوثائق الضرورية للتعرف على الاتصال الذي يتم التقاطه من أي مستغل لشبكة عامة أو مصلحة للاتصالات.

نفس المقتضيات نظمها القانون الفرنسي بشكل خاص بالجرائم المعلوماتية حيث أُلزم المؤسسات والأشخاص الذين يتوفرون على البيانات أو الوثائق المعلوماتية الإدلاء بها بناء على أمر قضائي (المادتين 56 و60). لذا يتعين وضع مقتضيات أوضح تلزم متعهدي ومزودي الخدمات وشبكات الإنترنت بتزويد السلطات القضائية المشرفة على الأبحاث القضائية أو الشرطة القضائية المكلفة بالبحث، بالمعلومات التي يتوفرون عليها أو ولوج أنظمتها المعلوماتية تحت إشراف قضائي بالشكل الذي يسمح بالحصول عليها في الوقت المناسب.

وبخصوص الجانب المتعلق بتفتيش ومصادرة البيانات المخزنة بالكمبيوتر كما نصت على ذلك المادة 19 من اتفاقية بودابست، فإن مقتضيات المادة 60 من قانون المسطرة الجنائية نصت على مقتضيات عامة تنظم التفتيش كإجراء تخضع له كافة الجرائم بغض النظر عن طبيعتها. إضافة إلى هذا الجانب، فإن القانون المغربي ينسجم مع الاتفاقية الدولية بخصوص مصادرة الوثائق المعلوماتية التي استعملت في ارتكاب الجريمة حيث أتاح القانون المغربي للمحكمة التي تنظر في القضية إمكانية مصادرة الوسائل أو الأشياء التي تم استغلالها في ارتكاب الجريمة (الفصل 11-607 من القانون الجنائي).

وبالنظر لطبيعة الجريمة المعلوماتية التي يعتبر عامل الزمن عنصراً مهماً فيها فقد نصت اتفاقية بودابست في المادة 20 على ضرورة التجميع الفوري لبيانات الكمبيوتر من خلال جمع أو تسجيل أو إجبار مقدم الخدمة في نطاق قدرته الفنية على جمع أو تسجيل سير البيانات المرتبطة باتصالات معينة.

وعلاقة بهذا المقتضى، يمكن الإشارة إلى أن قانون المسطرة الجنائية المغربي يتضمن مقتضيات عامة تتعلق بجمع أو تسجيل الاتصالات أو أمر شبكات الاتصال بتخزين هذه الاتصالات كما أشارت إلى ذلك المادة 108 التي حولت للوكيل العام وقاضي التحقيق لضرورة البحث بأن يلتصق إصدار أمر بالتقاط الاتصالات المنجزة بوسائل الاتصال عن بعد وتسجيلها وأخذ نسخ منها أو حجزها كلما تعلق الأمر بإحدى الجرائم المتعلقة بالإرهاب أو القتل أو العصابات الإجرامية، كما أتاحت نفس المقتضيات للوكيل العام للملك في حالة الاستعجال أن يأمر بالتقاط الاتصالات المنجزة بوسائل الاتصال عن بعد وتسجيلها وأخذ نسخ منها متى كانت ضرورة البحث تقتضي التعجيل خوفاً من اندثار وسائل الإثبات إذا كانت الجريمة تمس بأمن الدولة أو الإرهاب أو المؤثرات العقلية أو الاختطاف أو أخذ الرهائن.

هذا وقد وسع مشروع قانون المسطرة الجنائية من وعاء الجرائم الخاضعة لتقنية التقاط المكالمات أو الاتصالات المنجزة بوسائل الاتصال عن بعد بأن أضاف مجموعة من الجرائم الأخرى من بينها الجرائم المنسوبة بتنظيم المعالجة الآلية للمعطيات والجريمة المنظمة والجريمة المتعلقة بالعصابة الإجرامية وغسل الأموال والرشوة واستغلال النفوذ والفساد واختلاس وتبييد المال العام، وجريمة الإبادة الجماعية والجرائم ضد الإنسانية وجرائم الحرب وجرائم الاختفاء القسري أو التعذيب والاتجار بالبشر وتهريب المهاجرين.

ولما كانت الجريمة المعلوماتية من صنف الجرائم العابرة للحدود، فإن التعاون الدولي لمكافحة هذا النوع من الجرائم، يشكل ضرورة ملحة لجميع الدول، وهو الجانب الذي نظمته القسم الثالث من اتفاقية بودابست المعنون بالتعاون الدولي، وهي على العموم أحكام تتطابق مع ما نص عليه قانون المسطرة الجنائية في هذا الباب، فالمادتان 713 و 714 من قانون المسطرة الجنائية وضعت القواعد العامة المؤطرة للتعاون القضائي في عموميتها، حيث خص القانون المغربي للاتفاقيات الدولية وضعاً خاصاً حيث تحظى بالأولوية في التطبيق على القوانين الوطنية فيما يخص التعاون القضائي مع الدول الأجنبية، ولا يتم اللجوء إلى تطبيق مقتضيات القانون الوطني إلا في حالة عدم وجود اتفاقيات أو خلوها من الأحكام المتعلقة بالطلب موضوع التعاون (المادة 713 من قانون المسطرة الجنائية).

ووفقا لما هو معمول به في إطار التعاون القضائي بين المغرب وباقي الدول، تجب الإشارة إلى أن المغرب تلقى عدة إنابات قضائية تتعلق بالجريمة المعلوماتية، وقامت السلطات القضائية بتنفيذها بحضور ضباط ومحققين وقضاة أجنب بشكل فعال يراعي عامل الوقت المطلوب في البحث والتحقيق في هذا النوع من الجرائم، وبالتالي فإن أحكام القانون المغربي في هذا المجال تنسجم مع اتفاقيات بودابست. ونفس الأمر ينطبق على باقي مجالات التعاون كالتسليم حيث يتم تطبيق الاتفاقيات الثنائية، وفي حالة عدم وجودها يتم تطبيق القانون الداخلي، وعلى العموم فإن آليات التعاون القضائي لا تنظر إلى جريمة معينة بذاتها وإنما تضع القواعد والمبادئ التي يتم على أساسها تنفيذ طلبات التعاون القضائي وبالتالي فهي مقتضيات تشمل الجريمة المعلوماتية وغيرها من الجرائم التي يعاقب عليها القانون.

وحفاظا على سرية المعلومات التي يمكن أن تتضمنها طلبات التعاون فإن اتفاقية بودابست نصت في مادتها 28 على أنه يتعين على الدول في حالة عدم وجود اتفاقية أن تجعل توفير المعلومات متوقفا على المحافظة على سريتها، وعدم استخدامها في تحقيقات غير تلك التي قدم بشأنها الطلب.

إن هذه الأحكام تعتبر من ضمن المبادئ العامة المعمول بها في إطار التعاون القضائي بين الدول، وبالتالي فالقانون المغربي ليس فيه ما يخالف هذا المبدأ. كما أن العديد من الاتفاقيات الثنائية تشير إلى ذلك. فضلا عن ككون قانون المسطرة الجنائية ينص كمبدأ عام في المادة 15 على سرية البحث والتحقيق، ومن باب أولى كلما كانت إحدى المعلومات موضوع طلب التعاون القضائي مقيدة بعدم استعمالها في تحقيق آخر أو ضرورة التقيد بسريتها، فإن الدولة المطلوب منها ذلك وفي إطار مبادئ التعاون الدولي لا يمكنها إلا أن تتقيد بذلك إلا إذا كانت هناك أسباب تخص هذه الدولة كمساس ذلك بأمنها أو غيرها من الأسباب التي تبقى محل توافق بين الأطراف المعنية.

ومن بين مجالات ومواضيع التعاون التي نصت عليها اتفاقية بودابست إمكانية تقديم طلب التحفظ العاجل على البيانات المخزنة بالكمبيوتر والكشف عن خط سير البيانات

المتحفظ عليها ومصادرة البيانات المعلوماتية كما أشارت إلى ذلك المواد 29-30-31 من الاتفاقية.

إن موقف القانون المغربي بهذا الخصوص، لا يوجد به ما يمنع من تقديم طلب التعاون القضائي بشأن هذه المعلومات إلى السلطات القضائية المختصة، فوعاء التعاون الدولي هو وعاء أكبر يشمل أكثر من بحث أو إجراء أو معلومة ويختلف باختلاف طبيعة المهمة المطلوبة أو الجريمة موضوع طلب التعاون، وبالتالي فمن حيث المبدأ فإن مقتضيات القانونية المنصوص عليها في القسم الثالث من الكتاب السابع من قانون المسطرة الجنائية الخاص بالعلاقات القضائية مع السلطات الأجنبية تبقى إطارا عاما يوظف مختلف أشكال التعاون القضائي المنصوص عليها في قانون المسطرة الجنائية، وهو ما ينسجم مع مقتضيات الاتفاقية. كما أن أحكام التعاون القضائي المنصوص عليها في قانون المسطرة الجنائية تماثل بعض التشريعات المقارنة لبعض الدول المصادقة على اتفاقية بودابست، كقانون المسطرة الفرنسي في المواد 695-1 و695-2 و695-3 و695-10 و695.

ولتعزيز التعاون في مجال مكافحة الجريمة المعلوماتية فإن اتفاقية بودابست نصت في مادتها 32 على أنه يمكن للدول الأطراف وبدون تفويض من الطرف الآخر الدخول إلى البيانات المخزنة بالكمبيوتر بغض النظر عن مكان تواجد البيانات جغرافيا.

نعتقد بخصوص هذه الإمكانية أنها متاحة بين الدول المنضمة للاتفاقية من دول الاتحاد الأوروبي والتي تتوفر على أنظمة مماثلة ومرتبطة ببعضها البعض بواسطة شبكة معلوماتية، بحيث يمكنها ذلك من ولوج نظام البيانات المتوفرة لدى الطرف الآخر. والواقع أن هذا المجال يقترب من التعاون الأمني أكثر منه للتعاون القضائي، فضلا عن كون المعلومات التي قد يتطلبها الولوج غير المأذون به يمكن أن تكون موضوعا لطلب التعاون القضائي بالشكل الذي حدده الفصل الثالث من هذه الاتفاقية.

وعلى العموم، يمكن القول بأن قانون المسطرة الجنائية الحالي يتضمن مجموعة من مقتضيات العامة التي يمكن أن تسري وتنسحب على الجريمة المعلوماتية كما أشارت إلى ذلك اتفاقية بودابست، كما تم تعزيز هذه المقتضيات بمقتضيات أخرى جديدة ضمن مشروع

قانون المسطرة الجنائية تضي على إجراءات البحث وإثبات هذا النوع من الجرائم نوعا من الخصوصية تلاءم طبيعة هذه الجريمة وفق ما تم تفصيله أعلاه.

وعموما يمكن القول بأن اتفاقية بودابست التي صادقت عليها المملكة المغربية نظمت مختلف المجالات المتعلقة بإنفاذ القانون والتحقيقات والتعامل مع الأدلة الإلكترونية لأغراض العدالة الجنائية، منها تقديم طلب التحفظ العاجل على البيانات المخزنة بالكمبيوتر والكشف عن خط سير البيانات المتحفظ عليها ومصادرة البيانات المعلوماتية، وليس هناك ما يمنع السلطات القضائية المغربية من تطبيق مقتضيات الاتفاقية مباشرة لسموها عن التشريع الداخلي حسب ما جاء به تصدير دستور المملكة لسنة 2011.

ثانيا : الجهود المبذولة في مجال تعزيز القدرات وإنشاء الآليات المؤسسية

إن طبيعة البحث في الجرائم المعلوماتية تتطلب إيجاد أطر بشرية مؤهلة للتعامل مع هذا النوع من الجرائم وتوفير الإمكانيات التي تمكنها من قيامها بمهمتها في الوقت وبالشكل المطلوب، وفي هذا الإطار فإنه يمكن تكوين ضباط الشرطة القضائية في مجال الجريمة المعلوماتية وإطلاعهم على التجارب الرائدة في هذا المجال وعلى تقنيات البحث الناجعة حتى يستطيعوا مواكبة التغيرات والتطور الذي يعرفه البحث الجنائي بالنسبة للجريمة المعلوماتية التي أصبحت جريمة عابرة للحدود ومرتبطة بجرائم دولية أخرى أقل ما يقال عنها أنها تدخل في خانة الجرائم المنظمة حيث أضحت الجانب المعلوماتي وشبكة الانترنت مجالاً خصبا لارتكاب الجرائم سواء من خلال استعمالها كوسيلة أو هدف للجريمة في حد ذاتها.

وفي هذا الإطار انخرطت وزارة العدل في برنامج التعاون في مجال مكافحة الجريمة الإلكترونية بين دول الجوار جنوب الاتحاد الأوروبي CyberSud، والذي يرمي إلى تعزيز التشريعات وتأهيل المؤسسات في مجال الجريمة الإلكترونية والإثباتات الإلكترونية في منطقة الجوار الجنوبي لدول الاتحاد الأوروبي، وفق ما تقتضيه المتطلبات المتعلقة بحقوق الإنسان ودولة القانون.

ويهم هذا البرنامج بالخصوص كل من دول الجزائر والأردن ولبنان والمغرب وتونس، ويتم تمويل هذا البرنامج المشترك بين الاتحاد الأوروبي ومجلس أوروبا للتعاون في

مجال الجريمة الإلكترونية، في إطار الآلية الأوروبية للجوار، وقد انطلق هذا البرنامج في فاتح يوليوز 2017 وهو يمتد على ثلاث سنوات باعتمادات تقدر بـ 3,35 مليون أورو.

ويطمح هذا المشروع إلى تحقيق بعض التناغم على مستوى التشريعات وزيادة القدرات المؤسساتية في مجال مكافحة الجريمة السيبرانية والأدلة الرقمية، وذلك في إطار تعاون دولي وثيق يكون فيه هذا المشروع الحجر الزاوية لوضع خطة العمل التي ستسهم في تعزيز التشريعات والقدرات المؤسسية للبلدان ذات الأولوية.

وقد شارك ممثلون عن وزارة العدل في أشغال المؤتمر المخصص لانطلاق هذا البرنامج الذي امتدت أشغاله من 21 إلى 23 مارس 2018 بعاصمة الجمهورية التونسية، كما شارك ممثلون آخرون عن نفس الوزارة في ورشة، نظمت في إطار هذا البرنامج بالمعهد العالي للقضاء خلال الفترة الممتدة ما بين 2 و5 شتنبر 2018 والتي خصصت للتكوين القضائي في مجال الجريمة السيبرانية والأدلة الرقمية.

هذا وتعمل وزارة العدل على تعزيز التعاون الدولي الثنائي في مجال محاربة الجريمة المعلوماتية، ففي إطار تفعيل برنامج العمل للتعاون التقني والإداري بين وزارتي العدل المغربية والإسبانية، عقدت هذه الوزارة ورشة عمل حول "التوجهات الجديدة لآليات التعاون القضائي الدولي في مجال محاربة الجريمة الإلكترونية" بمقر المعهد العالي للقضاء بتاريخ 29 يناير 2019، خصصت لمناقشة سبل تعزيز التعاون الدولي في التصدي للجريمة الإلكترونية.

- القانون 24.03 الصادر بتنفيذه الظهير الشريف رقم 1.03.207 وتاريخ 11 نونبر 2003 والذي جرم استغلال الأطفال في مواد إباحية ؛
 - القانون 103.13 المتعلق بمحاربة العنف ضد النساء الصادر بتنفيذه الظهير الشريف رقم 1.18.19 بتاريخ 22 فبراير 2018، والذي جرم بمقتضاه التحرش الجنسي المرتكب بواسطة وسائل إلكترونية وكذا المس بالحياة الخاصة للأفراد المرتكب بواسطة الأنظمة المعلوماتية ؛
 - القانون 08.09 المتعلق بحماية الأشخاص الناطقين تجاه معالجة المعطيات ذات الطابع الشخصي الصادر بتنفيذه الظهير الشريف رقم 1.09.15 بتاريخ 18 فبراير 2009 ؛
 - القانون 88.13 المتعلق بالصحافة والنشر الصادر بتنفيذه الظهير الشريف رقم 1.16.122 بتاريخ 10 غشت 2016 ؛
 - القانون 2.00 المتعلق بحقوق المؤلف والحقوق المجاورة الصادر بتنفيذه الظهير الشريف رقم 1.00.20 بتاريخ 15 فبراير 2000 ؛
 - القانون 31.08 المتعلق بحماية المستهلك الصادر بتنفيذه الظهير الشريف رقم 1.11.03 بتاريخ 18 فبراير 2011.
- وتجدر الإشارة أنه، ولئن كان المشرع المغربي لم يشر صراحة إلى استعمال الوسائل الإلكترونية لارتكاب بعض الجرائم التقليدية كالنصب والابتزاز وغيرها، إلا أن العناصر التكوينية لهذه الجرائم جاءت في صيغة عامة تسمح بتحريك المتابعة بغض النظر عن الوسيلة المستعملة في ارتكابها.

2- على المستوى المؤسسي؛

تتوفر المملكة المغربية على مجموعة من الأجهزة والهيئات المختصة في اليقظة والحماية من مخاطر الإجرام السيبراني وكذا مجموعة من المؤسسات والأجهزة المكلفة بزجر هذا النوع من الإجرام .

أ- الأجهزة المختصة في اليقظة والحماية من مخاطر الإجرام السيبراني؛

من أهم الأجهزة نذكر ما يلي ؛

- اللجنة الاستراتيجية لأمن النظم المعلوماتية ؛
- المديرية العامة لأمن الأنظمة المعلوماتية (D.G.S.S.I)؛
- المركز المغربي لليقظة وتحليل العوارض والمعلوماتية maCERT التابع لإدارة الدفاع الوطني.

ب- الأجهزة المكلفة بزجر الإجرام السيبراني:

بفضل الاستراتيجية المعتمدة من قبل المديرية العامة للأمن الوطني، تم إحداث 29 فرقة أمنية متخصصة في محاربة الجرائم المرتبطة بالتكنولوجيا الحديثة، فضلا عن إحداث المكتب الوطني لمحاربة الجرائم المرتبطة بالتكنولوجيا الحديثة التابع للفرقة الوطنية للشرطة القضائية، وتضم هذه الفرق ضباطا للشرطة القضائية راكموا تجربة مهمة واستفادوا من تكوينات تروم تعزيز قدراتهم في هذا المجال الذي يعرف تطورا سريعا.

من جهة أخرى، تم تكوين مكونين متخصصين في الجرائم المعلوماتية في صفوف القضاة وضباط الشرطة القضائية. وبعد مصادقة المملكة المغربية على اتفاقية بودابست للجرائم المعلوماتية ودخولها حيز التنفيذ في فاتح أكتوبر الماضي، تم تعيين قاض للنيابة العامة كنقطة اتصال دائمة على مستوى محاكم الاستئناف والمحاكم الابتدائية مكلف بتتبع القضايا المرتبطة بالجرائم المعلوماتية وبالسهر على حسن تنفيذ الالتزامات الملقاة على عاتق المملكة المغربية بمقتضى هذه الاتفاقية.

وفي نفس الإطار، نظمت رئاسة النيابة العامة بتاريخ 03 دجنبر 2018 بمراكش يوما دراسيا حول آليات التعاون الدولي وفقا لأحكام اتفاقية بودابست للجرائم المعلوماتية، حضره مجموعة من القضاة وضباط الشرطة القضائية وكان مناسبة لتدارس الإشكاليات واقتراح الحلول المرتبطة بالأبحاث القضائية في مجال الجرائم المعلوماتية.

3- الدليل الإلكتروني والمادة الجنائية:

الأصل في المادة الجنائية، أنه يمكن إثبات الجرائم بأي وسيلة من وسائل الإثبات، باستثناء الحالات التي يقضي فيها القانون بخلاف ذلك، حسب مفهوم الفقرة الأولى من المادة 286 من قانون المسطرة الجنائية، إلا أن المشرع المغربي، أحاط جمع الأدلة من مكان ارتكاب الجريمة أو بمناسبة إجراء تفتيش في منازل المشتبه فيهم بمجموعة من الضمانات وهيدها بسلك مجموعة من الإجراءات التي قد يؤدي عدم احترامها إلى بطلانها وبالتالي عدم قبولها أمام القاضي الجنائي.

وعلى هذا الأساس، ولئن كان المشرع المغربي لم يحدد مسطرة خاصة لجمع الأدلة الإلكترونية بالنظر إلى طبيعتها وسرعة اندثارها، فإن الدليل الإلكتروني شأنه في ذلك كسائر وسائل الإثبات التقليدية يخضع فيما يتعلق بجمعه، إلى قانون المسطرة الجنائية لا سيما المواد 57 و59 إلى 63 و79 و81 منه.

وبالنظر إلى طبيعة الدليل الإلكتروني الذي يحتاج إلى أجهزة مختصة لتحليله وتقديمه كوسيلة إثبات للمحكمة، فإن المملكة المغربية تتوفر على مختبرين وطنيين وأربع مختبرات جهوية لتحليل الأدلة الرقمية بكل من فاس ومراكش والعيون والدار البيضاء.

ووعيا من المملكة المغربية بأهمية التعاون الدولي في هذا المجال، فقد صادقت المملكة المغربية على اتفاقية بودابست للجرائم المعلوماتية وأصبحت بذلك عضوا في الشبكة 24/7 التي تسمح بتقديم طلب إلى إحدى الدول الأعضاء لحفظ المعطيات الإلكترونية مؤقتا في انتظار تقديم طلب رسمي في شكل إنابة قضائية للحصول عليها في أفق استعمالها كوسيلة إثبات أمام المحكمة.

4- توصيات ومقترحات :

- لمحاربة الجرائم المعلوماتية بشكل فعال نقترح ما يلي :
- ملاءمة التشريعات الوطنية مع خصوصية الأبحاث المرتبطة بالجرائم المعلوماتية لا سيما في الشق الإجرائي ؛
 - تعزيز قدرات العاملين في العدالة الجنائية من قضاة وضباط شرطة قضائية من خلال تنظيم دورات تكوينية وندوات تهم هذا المجال ؛
 - توفير مختبرات علمية متخصصة في تحليل الأدلة الرقمية ؛
 - تعزيز التعاون الدولي بشقيه الرسمي وغير الرسمي لتسهيل جمع الأدلة الرقمية وتحديد هويات المشتبه فيهم ومحاكمتهم في احترام تام لحقوق الإنسان ولقواعد المحاكمة العادلة.