doubt that we should understand legally by boy and/or girl. It is to be said that most of the nations that have ratified the CON have taken it as a reference. It should also be expressed that within what is set out in the CDN in its numeral number 37 and 40, it has been established that the countries signatory to the CON, must create a specialized justice system to care for all those children and adolescents (NnyA) who are presumed to violate criminal laws.

The various international instruments recognizing children's rights, on the subject of criminal justice applied to them, lay down lines that seek to lead States parties, in the action to be directed for children in conflict with criminal law, so that the provisions laid down in international instruments can be fully realized within the States that have thus ratified the various international documents.

At first instance, it was relevant to return as a basis instrument to the Convention itself. One of the most important parameters that are rescued from the text of the CDN is not only the full recognition that the child is the subject of rights, but also that the principle of the best interests of the child stands, as a badge that States must follow in order to fulfil their obligations; therefore, it is the principle of the best interests of the child that, within the topic of children in conflict with justice, is of forced application.

However, for the issue of children in conflict with criminal law, within the text of the Convention, there are two numerals which to date consolidate not only guidelines for the annotated topic, but are a true parameter of implementation, just as States parties must necessarily consider.

The numerals that fall within the topic of children in conflict with criminal law are Articles 37 and 40 of the CNC, which consolidate the standard of application for children in conflict with criminal law, and harmonize with content that is regulated in other international instruments.

For the Mexican case, it is important to point out why Mexico, as a reference to the age of 12 years old as the minimum age of criminal liability and why to date, that is, fourteen years after the entry into force of the reform to article 18 of the Magna Carta, continues with that position.

UDC 614.2(043.2)

Zamroczyńska M., Doctor of Laws, Assistant Professor,
Poznan University of Medical Sciences, Poland

TELEMEDICINE AS A DIRECTION FOR THE DEVELOPMENT OF MEDICAL SERVICES IN THE PANDEMIC - BENEFITS AND RISKS

The development of the Internet, widespread access to mobile devices and new communication channels create unprecedented opportunities for the

provision of medical services. Thanks to the use of e-health applications, it is possible to collect a significant amount of medical data, data on physiology, lifestyle and everyday activities of people. This data can be used as a basis for shaping medical practice and scientific research. E-health can also support the provision of quality health services and enable more accurate diagnosis and treatment. There is no doubt that in the era of the COVID-19 pandemic, telemedicine has become an extremely useful way of delivering medical services remotely.

The World Health Organisation defines telemedicine as the provision of health care services, in which separation of location is essential, by all health professionals using means of communication to exchange relevant information for the purpose of diagnosis, treatment and prevention of disease and injury, to conduct research and its evaluation, to provide continuing education to health professionals, that is, to improve the health of individuals and the communities they form. This concept is quite broad and includes the requirement for appropriate qualifications, the aspect of the development of health professionals or reference to the positive effects to be achieved through the use of telemedicine for specific communities.

Telemedicine is primarily based on the following services: primary care and specialist medical assistance, provision of patient consultations for diagnosis; remote patient monitoring, including the use of devices to remotely collect and transmit data to the doctor for treatment; collection of information on medical products and health and medical education. In addition, telemedicine is based on the following modes of delivery: network programmes that connect hospitals with remote, local health centres; connections using hospital networks that provide specialised services; websites dedicated to e-health services for patients. Thus, it can be clearly stated that the use of telemedicine brings different types of benefits, such as overseeing healthcare for patients in remote locations, reducing healthcare costs, improving the quality of healthcare services, access to providers that may not otherwise be available, as well as medical services without having to travel long distances, and access to primary healthcare in an emergency situation such as the COVID-19 pandemic.

Regardless of which country and legal regime in which telemedicine is used, the starting point for the use of telemedicine is that the doctor should provide health services in accordance with professional ethics, current medical knowledge and is obliged to act with due diligence - regardless of whether the health service is provided in person or via teleinformation systems. Consequently, the principles of liability in the case of health services provided in-person at a medical facility and services provided via telemedicine are the same. Thus, a doctor may be civilly, criminally or professionally liable for improper treatment of a patient in a remote mode. The prerequisites for a doctor’s criminal liability for professional offences apply for performing a

medical intervention negligently or inconsistently with the current state of knowledge, for failing to provide assistance to a patient, for treating a patient without his or her informed consent, for disclosing facts covered by medical secrecy. Faulty performance of medical intervention may lead to liability for unintentional offences against health and life, such as manslaughter, causing grievous bodily harm such as causing severe disability or life-threatening disease, as well as unintentional violation of bodily organ function or health disorder. Particular attention should be paid to the issue of failure to provide assistance in a situation where objectively there was a threat to human life or health, but in connection with the provision of medical services remotely the doctor did not recognize this condition and did not provide assistance at all or provided assistance inadequate to the situation, and where objectively there was a threat to life or health, and the doctor recognized this condition and did not provide assistance on purpose. By the way, it should be stressed that the above-mentioned offences will also be connected with the disciplinary liability of the doctor for professional misconduct and civil liability - for the damage inflicted upon the patient. Civil liability is assessed from the perspective of the fault of the doctor, the damage suffered by the patient and the causal link between the doctor's actions and the damage suffered by the patient. On the other hand, a doctor will be held professionally liable in the event of a breach of the rules of medical ethics and regulations related to the exercise of the medical profession.

An important element associated with the provision of telemedicine services is the aspect of threats posed by the computerization of health care. The use of means of communication carries the risk of losing sensitive data, including the results of medical examinations, information about past operations, addictions and diseases. The transition from paper records to data stored on a server or in an electronic cloud involves failures, battling malware and hacking attacks, which necessitate taking measures to secure medical data sets. Medical information is a valuable asset for cybercriminals, and healthcare providers often lack the awareness, expertise, organisational capacity and resources to implement cyber security procedures and solutions. Cybercriminals who gain access to this sensitive data may use it for blackmail, to block the provision of medical services in a particular healthcare provider, or even to paralyse the entire healthcare service. The healthcare sector should therefore be regarded as a critical sector that should be subject to special protection. Ensuring a high level of security of data contained in electronic medical records is extremely important for the proper functioning of the healthcare system.

The development of telemedicine cannot replace the primary form of service provision, which is personal contact with the patient, so it is primarily intended to support 'classic' treatment. Nevertheless, telemedicine is the future, an appropriate and modern direction for the development of medical services and, above all, a means of universal access to them, not only in times of pandemics.

Literature

1. Bujok J., Gierek R., Olszanowski R., Skrzypek M., Uwarunkowania Rozwoju Telemedycyny w Polsce. Potrzeby, bariery, korzyści, analiza rynku, rekomendacje. Raport zespołu ekspertów Krajowej Izby Gospodarczej i Izby Gospodarczej Medycyna Polska, Warszawa, 2016.
2. Chojecka M., Nowak A., Telemedycyna na tle polskich regulacji prawnych - szansa czy zagrożenie? Internetowy Kwartalnik Antymonopolowy i Regulacyjny, Warszawa, 2016.
3. Jak skutecznie wykorzystać potencjał telemedycyny w polskim systemie ochrony zdrowia? Raport. Fundacja Telemedyczna, Warszawa, 2018.
4. Основи законодавства України про охорону здоров'я: Закон України від 19 лист. 1992 р. № 2801-XII. *Відомості Верховної Ради України*. 1993. № 4. Ст. 19.
5. Про затвердження нормативних документів щодо застосування телемедицини у сфері охорони здоров'я: Наказ МОЗ України від 19 жовт. 2015 р. № 681.
6. Про національну програму інформатизації: Закон України від 04 лют. 1998 р. № 74/98-ВР. *Відомості Верховної Ради України*. 1998. № 27-28. Ст. 181.

УДК 343(043.2)

Самедова Ш.Т., доктор юридических наук,
Бакинский государственный университет, г. Баку, Азербайджан

ПОНЯТИЕ ДОЛЖНОСТНОГО ЛИЦА В УГОЛОВНОМ ПРАВЕ АЗЕРБАЙДЖАНСКОЙ РЕСПУБЛИКИ

Первоначальная редакция УК Азербайджанской Республики в примечании к ст. 308 (злоупотребление служебными полномочиями) содержала определение должностного лица, которое впоследствии неоднократно изменялось. Следует отметить, что понятие «должностное лицо», которое в советском уголовном праве определялось довольно четко, с каждым последующим изменением действующего уголовного законодательства Азербайджанской Республики получало все более широкое определение. Так, принятие 13 января 2004 года Закона Азербайджанской Республики «О борьбе с коррупцией» внесло серьезные коррективы в определение должностного лица как субъекта коррупции [2]. Вместе с тем следует отметить, что понятие «субъект коррупции» шире, чем понятие «должностное лицо», т.к. включает в себя также лиц, которые попадают под ответственность как взяткодатели или лица, торгующие авторитетом.

В действующей редакции УК по состоянию на 15 января 2021 года под «должностным лицом» подразумеваются следующие лица [3, с. 270-271]: