Issue I: Use of the Internet for drug-related activities

Recommendation 1

Governments should be encouraged to ensure that their law enforcement agencies are well informed, professionally trained and suitably resourced so as to be effective in the investigation of cyber-related offences and the related use of the Internet for illicit trafficking.

Any action taken ☒ YES ☐ NO

Comments:

Organized crime groups present on the Internet have become highly sophisticated and refined in their activities, often moving assets and infrastructure from one part of the world to another. Cybercrime unit officers participate in domestic and foreign courses organized by European institutions, that is CEPOL (course on combating cyberspace crime in Budapest, Hungary) or Europol. In 2017, during the CEPOL Police Exchange Program, PCBI officers have been on the following study visits:

The purpose of such undertakings is to exchange experience and information, establishing contacts with other police forces and the private sector for collaboration in combating transborder crime, and extending knowledge on the manner of fulfilling police duties in case of crimes committed in cyberspace.

Recommendation 2

Governments must work together to overcome the obstacles encountered in undertaking the investigation of cyber-related trafficking offences across multiple jurisdictions and introduce the changes needed in legislation, practices and procedure to expedite information-sharing, enquiries with Internet service providers and the transfer of evidence.

Any action taken ☒ YES ☐ NO

Comments:

During their duties, PCBI officers from relevant units, supported by officers from cybercrime units, take part in multiple operational or analytical meetings related to cases in which crimes are committed on or through the Internet. Additionally, cybercrime officers participate in working meetings, workshops or projects intended to reach agreements, initiate collaboration or impact the shape of law.
Additionally, since 2018 an organizational change took place to implement a more comprehensive approach to handled cases and to facilitate and increase their effectiveness, consisting in assigning investigation officers to specialized cybercrime units.

Recommendation 3

Governments should encourage their law enforcement agencies to develop the specialist skills that will support the investigation of cyber-related offences and lead to successful criminal prosecutions.

Any action taken ☒ YES ☐ NO

Comments:

As part of police structures, specialized units combating cybercrime and supporting relevant units in combating drug, economic or criminal offences by performing activities in the Internet have been established. These specialized units have been established on both nationwide level in the Police Headquarters (Cybercrime Bureau) and on the regional level in all Regional Police Headquarters.

Issue II: Alternatives to imprisonment for certain offences as demand reduction strategies that promote public health and public safety

Recommendation 1

Governments are encouraged to make full use of alternatives to imprisonment for people with drug use disorders in contact with the criminal justice system, particularly at the time of their arrest and at the pretrial stage.

Any action taken ☐ YES ☐ NO

Comments:

Recommendation 2

Governments are encouraged to promote and implement institutional mechanisms, including through induction and training programmes, that enable the police to screen, assess and refer appropriate cases to treatment facilities, taking into account their dual role as the first responders and the first criminal justice actors encountered by people with drug use disorders when they come into contact with the criminal justice system.

Any action taken ☐ YES ☐ NO

Comments:

Recommendation 3

Governments are encouraged to adopt or amend legislation, policies, and guidelines that allow flexibility when handing down sentences for drug-related offences that take into account the nature and gravity of the offence as well as the personality and background of the offender.

Any action taken ☐ YES ☐ NO

Comments:

Recommendation 4

Governments are encouraged to employ a multidisciplinary approach in providing treatment and rehabilitation as an alternative to conviction or punishment and to promote and develop the capacity for institutional coordination between justice, health, and social services authorities.

Any action taken ☐ YES ☐ NO

Comments:

Recommendation 5

Governments are encouraged to implement measures to increase public awareness of the benefits of using alternatives to imprisonment.

Any action taken ☐ YES ☐ NO

Comments:

Recommendation 6

Governments are encouraged to collect and analyse gender- and age-disaggregated data on the use of alternatives to imprisonment and, if applicable, to undertake periodic evaluation of existing initiatives to provide treatment as an alternative to conviction or punishment for people with drug use disorders.

Any action taken ☐ YES ☐ NO

Comments:

Issue III: Mainstreaming gender perspectives in drug-related policies and programmes

Recommendation 1

Governments are encouraged to collect and analyse gender-disaggregated data to obtain more information about the situation and circumstances of women drug users and the various roles women assume in drug-related crime and in organized crime groups with a view to developing and implementing effective and comprehensive policies and programmes.

Any action taken ☐ YES ☐ NO

Comments:

Recommendation 2

Governments are encouraged to ensure non-discriminatory access to health-care services for women, including in prison, and to develop gender-sensitive prevention, primary care, treatment and reintegration policies and programmes, particularly for pregnant women and women with caretaking responsibilities.

Any action taken ☐ YES ☐ NO

Comments:

Recommendation 3

Governments are encouraged to ensure close cooperation and collaboration among all relevant national authorities in developing and implementing gender-sensitive drug policies and programmes that take into account the specific needs and circumstances faced by women and girls with regard to the world drug problem.

Any action taken ☐ YES ☐ NO

Comments:

Issue IV: Money-laundering, illicit financial flows and effective countermeasures

Recommendation 1

In support of the investigation of money-laundering offences and the recovery of the proceeds of crime, Governments are encouraged to enable access by their law enforcement authorities to the information held by their financial intelligence units.

Any action taken ☒ YES ☐ NO

Comments:

On 13 July 2018, the Act on Countering Money Laundering and Terrorism Financing of 1 March 2018 entered into force (except for provisions related to the Central Register of Beneficial Owners, which will enter into force on 13 October 2019). The objective of the act was to adapt Polish norms to the provisions of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and to amended FATF recommendations, as well as to increase the effectiveness of the national anti-money laundering and terrorism financing system. While the bill was being drafted, recommendations on the national anti-money laundering and terrorism financing system by the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), found in the 2013 report evaluating the Polish anti-money laundering and terrorism financing system, were taken into account.

In addition, the act stipulates a new scope of GIFI tasks and amends the rules on which this authority can collect information necessary to fulfil its statutory duties and to share such information with other entities.

The act lists information which obliged institutions must report to the GIFI (the so-called *threshold transaction reports* – TTR), and information about circumstances that might raise a suspicion of money laundering or terrorism financing (*suspicious activity report – SAR*).

The act also establishes a number of informational obligations for both the GIFI and law enforcement authorities:

1) The prosecutor notifies the GIFI about a decision to freeze an account or put a transaction on hold, initiate proceedings and bring an indictment in cases involving money laundering or terrorism financing. In such case, the GIFI immediately notifies the prosecutor about possessing any information related to information previously submitted by the prosecutor.
2) Collaborating units (including law enforcement authorities) immediately notify the General Inspector about a suspected money laundering or terrorism financing offence. The GIFI sends back information about circumstances pointing to a connection between information found in the notification to law enforcement authorities and information provided by obliged institutions.
3) If information held, processed or analysed by the GIFI points to a justified suspicion of a money laundering or terrorism financing offence, the GIFI notifies the relevant prosecutor of the suspected offence together with information or documents validating the suspicion.
4) Following a written request, the GIFI makes available to courts and prosecutors for the needs of penal proceedings all information or documents, including information or documents subject to legally protected secrets, collected under the provisions of the act.
5) The General Inspector makes information available on the written and justified request of the Police, Internal Security Agency, Border Guard and Central Anti-Corruption Bureau.

Additionally, if the commission of a fiscal offence or an offence other than money laundering or terrorism financing is suspected, the GIFI submits information validating this suspicion to relevant authorities.

It should be noted that information collected and made available by the GIFI in the manner provided for in the act is treated as a financial secret.

Recommendation 2

Governments are encouraged to ensure that evidence gathered through investigations of money-laundering offences by their financial intelligence units has legal standing in their courts if used in prosecutions brought by other law enforcement agencies.

Any action taken ☒ YES ☐ NO

Comments:

At this stage, under the currently effective Code of Penal Procedure, materials collected as a result of investigations conducted by financial intelligence divisions cannot be put forward as evidence, but are nevertheless used in penal proceedings as a valuable source of information subsequently verified while taking evidence as provided for in the Code. It should, however, be noted that activities undertaken by the General Inspector of Financial Information in proceedings concerning money laundering to freeze a bank account or put a transaction on hold are each time notified to the relevant prosecutor's office unit together with a notification of suspected offence. For the prosecutor, this serves as basis to make a decision to launch an investigation and, when the pre-trial proceedings result in an indictment, to file a bill of indictment together with evidence.

Recommendation 3

Governments are encouraged to make use of the tools available for training and building the capacity of their law enforcement authorities, financial investigators and prosecutors available through the Global Programme against Money-Laundering of the United Nations Office on Drugs and Crime (UNODC) and other training institutions.

Any action taken ☒ YES ☐ NO

Comments:

In 2018, Poland organized a specialist practical course on money laundering held under the auspices of CEPOL and attended by international experts and 30 law enforcement representatives from EU member states and others, such as Georgia.

This training session on money laundering took place on 3-8 June in Warsaw. The substantive portion of the course was prepared with the participation of many entities (such as representatives of Europol, financial intelligence units, asset recovery offices, the Ministry of Finance, Border Guard, the private sector, academic experts), which provided added value and enriched the course's foundations. The object of the training was to discuss the newest trends and opportunities for use of innovative technology to combat money laundering.

In addition, in 2017 and 2018 PCBI representatives took part in multiple training initiatives organized by CEPOL and devoted to combating money laundering, as well as in the CEPOL Police Exchange Program that allowed Polish Police officers to attend internships abroad.

Recommendation 4

Governments are encouraged to share with UNODC the results of their national money-laundering risk assessments to facilitate a coordinated global response and to strengthen the capacity of competent authorities and financial institutions to thwart attempts at money-laundering.

Any action taken ☒ YES ☐ NO

Comments:

Under the Act on Countering Money Laundering and Terrorism Financing of 1 March 2018, the GIFI, together with the Financial Security Committee, cooperating units and obliged institutions, drafts a national money laundering and terrorism financing risk review. The Financial Security Committee acts as a subsection of the GIFI and provides opinions and advice on countering money laundering and terrorism financing. The FSC, in addition to the GIFI, also includes representatives of the Minister of Internal Affairs, Minister of Justice, Minister of Foreign Affairs, Minister of National Defence, Minister of Public Finances, Minister of Economy, Minister of Information Technology, the central bank, and law enforcement authorities (Police, ISA, NRA, Public Prosecutor General, Border Guards).

While drafting the national risk assessment, the GIFI takes into account the European Commission report referred to in Article 6(1)-(3) of Directive 2015/849. The GIFI checks whether the national risk assessment is up to date and updates it when necessary, not less frequently however than once in 2 years.

The national risk assessment includes in particular:

1) a description of the national risk assessment methodology;
2) a description of events related to money laundering and terrorism financing;
3) a description of effective regulations concerning money laundering and terrorism financing;
4) the level of money laundering and terrorism financing risk in the Republic of Poland, together with justification;
5) conclusions resulting from the money laundering and terrorism financing risk assessment;
6) issues related to protecting personal data related to countering money laundering and terrorism financing.

The General Inspector, based on the national risk assessment, designs a draft strategy to counter money laundering and terrorism financing, hereinafter the “strategy”, which includes a plan of actions intended to mitigate the risk related to money laundering and terrorism financing.