While profiling can be a useful tool for cyber police activities, there are a number of ethical and legal concerns that must be taken into account. These include concerns around privacy and data protection, as well as concerns around discrimination and bias.

In order to address these concerns, law enforcement agencies must ensure that they are transparent about the profiling techniques they use, and that these techniques are subject to appropriate oversight and accountability measures. They must also ensure that they are collecting and analyzing data in a manner that is consistent with relevant privacy and data protection laws and regulations.

Overall, while profiling can be a valuable tool for cyber police activities, it must be used in a manner that is consistent with ethical and legal standards, and that respects the rights and privacy of individuals.

Haborets Olha Andriivna
PhD, Associate Professor of the Department of Operational-search Activities and Information Security of Donetsk State University of Internal Affairs
Chernobrov Violetta Volodymyrivna
cadet of the faculty of training specialists for criminal police units of Donetsk State University of Internal Affairs

THE USE OF AUTOMATED INFORMATION SYSTEMS IN OPERATIONAL AND INVESTIGATIVE ACTIVITIES

Automated information systems have become increasingly prevalent in operational and investigative activities conducted by law enforcement agencies, intelligence services, and other government bodies. These systems enable the efficient and effective collection, processing, and analysis of large volumes of data, which can be used to inform operational strategies and support investigations.

Automated information systems (AIS) are computer-based tools that can store, process, and transmit data in a way that improves the efficiency and effectiveness of operational and investigative activities.

In operational activities, AIS can be used to support tasks such as data entry, record keeping, report generation, and communication. For example, in law enforcement, AIS can be used to manage criminal databases, track incidents, and issue alerts to officers in the field. In emergency services, AIS can be used to manage dispatch and track resources. In healthcare, AIS can be used to manage patient records and schedule appointments.

In investigative activities, AIS can be used to support tasks such as data analysis, evidence collection, and case management. For example, in law enforcement, AIS can be used to search databases for information on suspects, analyze patterns in crime data, and manage evidence. In healthcare, AIS can be used to track outbreaks and analyze medical records for evidence of fraud or abuse.

The use of AIS in operational and investigative activities has several benefits, including increased efficiency, accuracy, and accessibility of information. However, it is important to ensure that the systems are secure and that access to sensitive

information is controlled to prevent unauthorized use or disclosure. Additionally, it is important to have proper training and protocols in place to ensure that the systems are used effectively and ethically.

Here are some key points to consider when it comes to the use of automated information systems in operational and investigative activities:

Benefits of Automated Information Systems:

Automated information systems offer numerous benefits to operational and investigative activities. They can help to streamline processes, improve efficiency, increase accuracy and reduce errors. AIS can also provide real-time data, which is essential for timely decision-making. Additionally, AIS can help to reduce costs associated with data management and analysis.

Types of Automated Information Systems:

There are various types of automated information systems that can be used in operational and investigative activities. Some examples include:

Case management systems: These systems are designed to manage the process of investigating and prosecuting cases. They can help to track evidence, manage witnesses, and coordinate with other agencies involved in the case.

Intelligence systems: These systems are used to gather, analyze, and disseminate intelligence information. They can help to identify potential threats and assist with investigations.

Crime analysis systems: These systems are used to analyze crime data and identify patterns and trends. They can help to identify hotspots and assist with resource allocation.

Financial systems: These systems are used to track financial transactions and identify financial crimes such as money laundering.

Challenges of Automated Information Systems:

While automated information systems offer numerous benefits, they also present some challenges. One of the main challenges is ensuring the security of the system and the information it contains. Additionally, AIS can be complex and difficult to use, requiring specialized training for operators. There may also be issues with data quality and accuracy, as well as concerns about privacy and civil liberties.

Legal and Ethical Considerations:

The use of automated information systems in operational and investigative activities raises legal and ethical considerations. For example, the use of AIS may be subject to laws and regulations regarding data privacy and security. Additionally, there may be concerns about the potential for bias in the data or algorithms used by these systems.

In conclusion, automated information systems are an important tool in operational and investigative activities. They offer numerous benefits, but also present challenges and raise legal and ethical considerations. As such, it is important to carefully consider the use of AIS and ensure that appropriate measures are in place to ensure their effectiveness, security, and compliance with applicable laws and regulations.

Applications of Automated Information Systems:

AIS are widely used in various operational and investigative activities. Here are

some examples of their applications:

Law enforcement: Law enforcement agencies use AIS to manage cases, investigate crimes, track suspects, and analyze crime data. For example, they may use crime analysis systems to identify patterns and trends in crime data and allocate resources accordingly.

Military: The military uses AIS for a variety of purposes, including logistics, intelligence, and operations management. For example, they may use intelligence systems to gather and analyze information on enemy movements and activities.

Healthcare: Healthcare providers use AIS for patient management, electronic health records, and medical research. For example, they may use electronic health records systems to store patient data and provide healthcare professionals with real-time access to medical records.

Finance: Financial institutions use AIS for transaction processing, risk management, and fraud detection. For example, they may use financial systems to track transactions and identify suspicious activity.

Types of Data Used in Automated Information Systems:

AIS rely on various types of data to function effectively. Some examples include:

Structured data: Structured data is highly organized and can be easily searched and analyzed. Examples of structured data include names, dates, and numerical values.

Unstructured data: Unstructured data is more difficult to analyze as it is not highly organized. Examples of unstructured data include text, images, and video.

Big data: Big data refers to extremely large datasets that cannot be easily managed or analyzed using traditional data processing methods. Big data requires specialized tools and techniques to analyze effectively.

Trends in Automated Information Systems:

The use of automated information systems is evolving rapidly, and several trends are emerging. Some of the key trends include:

Artificial intelligence: Artificial intelligence is becoming increasingly prevalent in AIS. AI can help to automate tasks, identify patterns in data, and make predictions.

Cloud computing: Cloud computing is becoming more popular for AIS as it allows for greater scalability, flexibility, and cost-effectiveness.

Internet of Things: The Internet of Things (IoT) refers to the growing network of connected devices that can gather and transmit data. IoT devices are increasingly being integrated into AIS to provide real-time data and improve decision-making.

Blockchain: Blockchain is a distributed ledger technology that is being used in AIS to improve security, transparency, and accountability.

In conclusion, the use of automated information systems in operational and investigative activities is essential for organizations to operate effectively and efficiently. AIS offer numerous benefits, but also present challenges and raise legal and ethical considerations that need to be carefully considered. As technology continues to evolve, AIS will become even more advanced and integrated, which will have both positive and negative implications for organizations and society as a whole.