



GUIDELINES FOR THE GOVERNANCE OF STATISTICAL DATA IN THE CRIMINAL JUSTICE SYSTEM



GUIDELINES FOR THE GOVERNANCE OF STATISTICAL DATA IN THE CRIMINAL JUSTICE SYSTEM



Vienna, 2024

© 2024 United Nations Office on Drugs and Crime

This publication may be reproduced in whole or in part and any form for educational or non-profit purposes without special permission from the copyright holder, provided acknowledgement of the source is made.

Comments on the report are welcome and can be sent to:

Data, Analytics and Statistics Section (DASS)
Research and Trend Analysis Branch
Division for Policy Analysis and Public Affairs
United Nations Office on Drugs and Crime
P.O. Box 500
1400 Vienna
Austria
E-mail: unodc-iccs@un.org

Suggested citation:

United Nations Office on Drugs and Crime, *Guidelines for the Governance of Statistical Data in the Criminal Justice System* (Vienna, 2024).

DISCLAIMERS

The findings, interpretations, and conclusions expressed herein are those of the author(s) and do not necessarily reflect the views of the United Nations or its officials or Member States.

This document has not been formally edited. The designations employed and the presentation of material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Links contained in the present publication are provided for the convenience of the reader and are correct at the time of issue. The United Nations takes no responsibility for the continued accuracy of that information or for the content of any external website.

Preface

In 2015, the United Nations Statistical Commission (UNSC) and the United Nations Commission on Crime Prevention and Criminal Justice (CCPCJ) endorsed the International Classification of Crime for Statistical Purposes (ICCS). ICCS is the international standard for defining and classifying criminal offences for the production and dissemination of statistical data on crime and criminal justice.

Building on the process to implement ICCS and the report on crime and criminal justice statistics authored by the United Nations Office on Drugs and Crime (UNODC) and the National Institute of Statistics and Geography (INEGI) of Mexico,¹ the *Guidelines for the Governance of Statistical Data in the Criminal Justice System* are aimed at providing advice to the criminal justice system on the collection, production and dissemination of high-quality statistical data that can assist in performing and monitoring core functions, improving the measurement of access to justice and promoting the implementation of ICCS.

The present guidelines are part of a series on the production of statistical data by criminal justice institutions. The series comprises specific guidance for the police, the prosecution service and courts, and the prison system. The present guidelines are focused on the development and governance of an interoperable system of administrative data in the criminal justice system more broadly.

Acknowledgements

The development of the *Guidelines for the Governance of Statistical Data in the Criminal Justice System* was led by the Division of Policy Analysis and Public Affairs (DPA), under the supervision of Jean-Luc Lemahieu, Director of DPA and Angela Me, Chief of the Research and Trend Analysis Branch.

Core team

Martijn Kind
Martíño Rubal Maseda

Editor

Jonathan Gibbons

The team is grateful for the expert guidance and advice provided by (in alphabetical order):

Anna Alvazzi del Frate (Alliance of NGOs on Crime Prevention and Criminal Justice), Enrico Bisogno, Fiona Dowsley (Crime Statistics Agency, Victoria, Australia), Silja Emmel (United Nations Statistics Division), Adrian Franco Barrios (INEGI, Mexico), Shelly Hyland (Bureau of Justice Statistics, United States), Victoria Palanciuc, Gabriela Pérez García, David Rausis (UNODC) and Salomé Flores Sierra Franzoni (UNODC).

The production of this publication was made possible by the generous financial contribution of the United States of America.

Contents

Preface	iii
Acknowledgements	iv
1 Introduction	1
1.1 Background	1
1.2 Objective of the guidelines	1
1.3 Structure of the guidelines	2
2 Role of administrative data in crime and criminal justice statistics	4
2.1 Defining administrative data.....	4
2.2 Benefits and challenges of administrative data.....	5
2.3 Stages of the criminal justice process.....	9
2.4 Organizational modes of statistical systems.....	10
2.5 Producers and users of statistical data on crime and criminal justice.....	12
2.6 Approaches to data collection	14
2.7 International data collection on crime and criminal justice	17
3 Data governance in the criminal justice system	18
3.1 Vision and leadership.....	20
3.1.1 Vision and strategy.....	20
3.1.2 Leadership.....	22
3.1.3 Data stewardship	23
3.2 Regulations.....	24
3.2.1 Statistical legislation	26
3.2.2 Regulations on data privacy and security	27
3.2.3 Operational guidelines.....	29
3.2.4 Ensuring regulatory coherence	29
3.3 Coordination and cooperation.....	30
3.3.1 Formal mechanisms	31
3.3.2 Informal mechanisms.....	32
3.3.3 Memoranda of understanding.....	33
3.3.4 Use of standards	34
3.4 Data architecture	36
3.4.1 Data standardization.....	36
3.4.2 Statistical processes.....	41
3.4.3 Managing the data life cycle	42
3.4.4 Data security	51
3.4.5 Data quality.....	55
3.4.6 Use of open data standards.....	58
4 Conclusions and recommendations	62
Annex: Case Studies	66
Cameroon: Improving homicide statistics	66
Ecuador: Special Statistical Commission on Security, Justice, Crime and Transparency.....	68
Estonia: e-Justice system and interoperability	71
Indonesia: One Data Initiative and criminal justice statistics	75
Republic of Korea: Korea Information System of Criminal Justice Services (KICS).....	78
United Kingdom: Long-term strategic data vision	82

Results of the survey on criminal justice statistical systems	85
End notes	88

Figures

Figure 1	Stages of the criminal justice process	9
Figure 2	Producers and users of crime and criminal justice statistics	13
Figure 3	Data governance framework.....	19
Figure 4	National Strategy for the Development of Statistics (NSDS) life cycle.....	21
Figure 5	Basic data flow diagram	43
Figure 6	Road map for the improvement of data governance	63
Figure 7	e-File central case management system in Estonia	72
Figure 8	Structure of the Korean Information System of Criminal Justice Services (KICS)	79
Figure 9	Victim-perpetrator relationship in intentional homicide, Republic of Korea, 2021	80
Figure 10	Adequacy of staff training	87

Tables

Table 1	Influence of regulatory instruments and guidelines on administrative data.....	25
Table 2	Basic data dictionary components	39
Table 3	Selected international models and standards for managing statistical processes	41
Table 4	Selected data analysis tools	48
Table 5	Example of data classification	52
Table 6	Examples of access control policies	53
Table 7	Examples of network security tools	53
Table 8	Principles for statistical output quality.....	55
Table 9	Data governance maturity assessment.....	62
Table 10	Number of survey participants, by country.....	85
Table 11	Level of technical interoperability.....	86

Boxes

Box 1	Resources for improving the quality of administrative data.....	15
Box 2	Evolution of the data management system in Uruguay.....	16
Box 3	Strategic work on data in the United Kingdom	21
Box 4	Special Commission on Crime Statistics in Ecuador	23
Box 5	Role of trust in the collection, production and dissemination of data	25
Box 6	Law of the National System of Statistical and Geographical Information (SNIEG) of Mexico	26
Box 7	European Union directive on processing personal data in the criminal justice system ..	28
Box 8	Commissions on data protection: France and Singapore	28
Box 9	Informal collaboration in the Open SDG platform in the United Kingdom.....	32
Box 10	Elements of a memorandum of understanding	33
Box 11	Implementation of the International Classification of Crime for Statistical Purposes (ICCS) in Kenya.....	34
Box 12	Essentials of metadata	37
Box 13	Crime reporting in the United States	40
Box 14	Improving the flow of crime data in Lebanon	43

Box 15	Modernizing IT infrastructure: Colombia and Senegal.....	46
Box 16	Mexico: National Census of State Law Enforcement (CNIJE)	50
Box 17	X-Road: an open-source collaboration.....	59
Box 18	Free and Open-Source Software: the Kingdom of the Netherlands and Poland	60

1 Introduction

1.1 Background

In 2015, the United Nations Statistical Commission (UNSC) and the United Nations Commission on Crime Prevention and Criminal Justice (CCPCJ) endorsed the International Classification of Crime for Statistical Purposes (ICCS). ICCS is the international standard for defining and classifying criminal offences for the production and dissemination of statistical data on crime and criminal justice. When criminal offence statistics are compiled and distributed according to the comprehensive and standardized framework of ICCS, it is possible to collect better data and produce articulated analyses of crime trends and patterns harmonized across the different stages of the criminal justice system and jurisdictions.

The implementation of ICCS is part of the UNODC-INEGI road map to improve the quality and availability of crime statistics at the national and international levels, which comprises three pillars: i) the development of new methodological tools; ii) capacity-building activities; and iii) strengthening of international data collection and analysis.²

Although ICCS is an instrument for producing data in a systematic manner across criminal justice institutions, it needs other complementary tools to provide methodological guidance on how to build an integrated system of national crime and criminal justice statistics that can provide high-quality information on the effectiveness and efficiency of operations by the various institutions as well as on access to justice for all who come into contact with criminal justice institutions.

In 2003, the United Nations published the *Manual for the Development of a System of Criminal Justice Statistics*,³ which sets out a general framework for the development of such a system. The manual targets both users and producers of criminal justice statistics and recognizes that the underlying conditions and readiness to develop a system of criminal justice statistics vary markedly from country to country. The manual offers a useful general framework, but the rapid developments over the past two decades in information technology (IT), the exponential growth of data and the increase in importance of good data governance call for updated guidance.

The present guidelines are part of a series of guidelines on the production of statistical data by criminal justice institutions that are focused on expanding the scope of administrative data far beyond the mere recording of criminal offences. Expanding on how to improve the governance of criminal justice statistical systems more broadly, the present guidelines provide examples from a range of countries that have implemented such systems across different regions. The other guidelines in the series comprise specific guidance for the police, the prosecution service and courts, and the prison system on how to collect, produce and disseminate high-quality statistical data that can assist them in performing and continuously monitoring their core functions, improving access to justice for all and promoting the implementation of ICCS.

1.2 Objective of the guidelines

Through the present guidelines, UNODC aims to contribute to maximizing the value of crime and criminal justice administrative data as a strategic asset by supporting countries in optimizing data collection, production, dissemination and use, strengthening data governance arrangements and data partnerships, and building robust statistical environments that are interoperable. The guidelines stress the need to adopt a holistic approach to data governance, including the formulation of a long-term

vision, developing the necessary regulatory instruments, coordinating the different institutions and designing a data architecture aligned with a country's needs and resources. These four elements are presented as key pillars of a framework aimed at strengthening data governance for crime and criminal justice data.

Any national system of crime and criminal justice statistics needs to be comprehensive and consistent: comprehensive as it should consider all the different institutions and actors that are involved in the criminal justice system, including the relevant ministries and agencies, the police, the prosecution service, the courts and the prison system; consistent as it should promote the standardized collection, exchange, dissemination, use and reuse of data that are produced by the different criminal justice system institutions. All such institutions produce administrative data as part of their daily activities that can be used to monitor, analyse and improve the functioning of the criminal justice system at the international, national, subnational and local levels. The data can also be used by institutions and non-governmental actors beyond the criminal justice system that produce research and policy analysis related to criminal justice and highlight how advancing crime prevention, criminal justice and the rule of law are instrumental for the achievement of sustainable development.

In other words, the criminal justice system should treat data as a strategic asset and consider its public value. High-quality data on crime and criminal justice have enormous potential benefits and can positively impact society when used appropriately. The responsibilities of the criminal justice system go beyond the collection of data (for statistical or other purposes) and include storing, securing, processing, sharing, curating, disseminating and using and reusing the data. Only when the relevant institutions have such a comprehensive approach to data can they realize the full potential that crime and criminal justice administrative data have for improving society, countering criminal activity and ensuring equal access to justice for all.

Improving the collection, production and dissemination of high-quality statistical data from the criminal justice system also serves to meet the growing international demand for such data. Data of this nature are essential for monitoring progress on a number of indicators under the Sustainable Development Goals, including indicator 16.1.1 (Number of victims of intentional homicide per 100,000 population, by sex and age) and indicator 16.3.2 (Unsentenced detainees as a proportion of overall prison population). Moreover, the 2021 Kyoto Declaration, adopted at the fourteenth United Nations Congress on Crime Prevention and Criminal Justice, reaffirmed the global commitment to evidence-based crime prevention through the collection and analysis of data using systematic and coherent criteria.⁴ Through the Declaration, Member States further highlighted the need to ensure the fair, effective, accountable, transparent and appropriate administration and delivery of justice, which is where standardized, accurate and reliable statistics derived from administrative data can play a key role.

1.3 Structure of the guidelines

Chapter 2 of the present guidelines discusses administrative data for the production of statistics and defines the key concepts when dealing with administrative data, the associated benefits and challenges and how administrative data are typically produced within the criminal justice system.

Chapter 3 introduces a framework for data governance in the criminal justice system and deals with four key elements: i) leadership and vision; ii) regulatory instruments that are typically in place to manage statistical systems; iii) aspects related to coordination and cooperation within the different sectors of the criminal justice system and beyond; and iv) data architecture, that is, the standards, models, policies and IT tools that are built around the data production process. The chapter also

suggests several basic assessment questions that countries can use to ascertain the status of their criminal justice data ecosystem.

Chapter 4 presents the conclusions and recommendations derived from the preceding chapters. All three chapters adopt a practical perspective and incorporate information from a range of countries on how they approach the different aspects of managing the criminal justice statistical system. A review of six specific country case studies is introduced in the annex to the present guidelines.

2 Role of administrative data in crime and criminal justice statistics

Core data for the ongoing production of national statistical information in the criminal justice area are extracted from administrative records kept by the police, the prosecution service, the courts, the prison system and other relevant stakeholders. This includes a wide variety of data such as the number of criminal offences, victims, offenders, persons brought into formal contact with the police, persons prosecuted, length of proceedings, persons convicted and acquitted, and persons held in prisons. Such administrative data offer the potential for highly significant insights into crime trends and the operations of criminal justice systems. This chapter provides an overview of the nature of administrative data, the associated benefits and challenges, and highlights how the collection, production and dissemination of administrative data are shaped by the specificities of both the criminal justice system and the national statistical system in each country.

2.1 Defining administrative data

The *United Nations National Quality Assurance Frameworks Manual for Official Statistics* defines administrative data sources as data sets created primarily for administrative purposes by government agencies or other entities working on behalf of the Government.⁵ These data are not primarily created in response to the need for statistical data but as part of a government function, such as the provision of services or the delivery of justice. The use of administrative data for statistical purposes is certainly not a recent phenomenon, but the advent of accelerated progress in technology and computing capacity over the past two decades has made such use increasingly widespread. Statistical agencies can be involved in the design, collection and production of administrative data with the aim of making the data suitable for statistical purposes. However, since such data are not primarily created for the production of statistics, there are specific challenges involved in doing so, as noted in section 2.2.

Administrative data sources can be contrasted with statistical data sources obtained from sample surveys and censuses, which are created primarily for official statistical purposes. The distinction between administrative and statistical data sources may not be immediately obvious, especially since administrative data sources can also be used for the production and dissemination of official statistics; a technical distinction is made between the intended purpose of the two different data sources. Unlike administrative data sources, statistical data sources are typically obtained according to specified needs and predefined statistical methods and concepts. In the case of the criminal justice system, this includes crime victimizations surveys, corruption surveys, surveys on violence against women and gender-based violence, and more.

Such statistical data sources can offer important complementary data to administrative records, which is particularly important for providing insight into the overall prevalence of crime and people's experiences with and perceptions of the criminal justice system. Moreover, survey data are essential for reporting on several Sustainable Development Goal indicators, such as indicator 16.3.1 (Proportion of victims of violence in the previous 12 months who reported their victimization to competent authorities or other officially recognized conflict resolution mechanisms). Hence, finding a balance between the use of administrative data sources and dedicated surveys is vital for generating a holistic overview of the functioning of the criminal justice system.

In addition, sources of information on specific crimes, offenders and victims are collected by private and other public agencies such as insurance companies, tax and customs authorities and

environmental protection organizations.⁶ These different sources are a good complement to administrative records from the criminal justice system and enable policymakers to better understand crimes that for different reasons are not reported to the competent authorities.

The scope of the current guidelines is limited to official administrative data collected by criminal justice institutions. That said, many of the components of the framework presented in chapter 3 are equally applicable to survey data.

2.2 Benefits and challenges of administrative data⁷

Although the data collection arrangements and the potential advantages of the use of administrative data vary from country to country depending on the national circumstances, some key general benefits of the use of administrative records for statistical purposes are described below.

Timeliness and frequency

Administrative records are generally collected in real time or with minimal delay for administrative purposes and can thus be made available relatively quickly. As a result, statistics based on administrative data can be prepared and released more quickly and more frequently than statistics based on surveys and censuses, which typically take significant time and resources to plan, design, execute and analyse. This allows for timely analysis and decision-making supported by frequent data updates.

An example is the collection of arrest records by the police. A police department will typically maintain a database that records the details of arrests made within its jurisdiction. Such a database can provide near real-time information about arrests, including details such as the date, time, location and charges of the arrest and the demographic characteristics of the arrested individual. This allows law enforcement agencies and policymakers to monitor trends and make informed decisions in a timely manner.

Cost-effectiveness

Collecting administrative data is relatively cost-effective compared with conducting censuses and surveys, since such data are collected as part of routine administrative processes. It is important to acknowledge, however, that the collection of high-quality administrative data is not cost free and requires adequate investment in IT systems, coordination mechanisms, human resources, legal frameworks and organizational resources (for example, a dedicated unit for statistics). Moreover, while the collection and use of administrative data are typically free of charge, setting up and maintaining a data exchange infrastructure can be costly.

An example of the cost effectiveness of administrative data is the use of court records. Courts maintain detailed administrative data on criminal cases, including the details of charges, the length of proceedings and case outcomes. The data are collected as part of an administrative function and can enable researchers to investigate topics such as case processing times, attrition rates, recidivism rates and the effectiveness of different custodial and non-custodial sentencing strategies. By leveraging such data, policymakers can make more informed decisions and allocate resources more efficiently within the criminal justice system.

Coverage and detail

Administrative data are typically collected under statutory, regulatory or administrative provision and comprehensively cover a large population, often the entire group of interest, which enables robust statistical findings. Moreover, since data are collected for specific administrative purposes, they can provide detailed information on events, victims, offenders and processes, allowing for in-depth analyses and insights using unique identifiers for individual records.

For example, the prison system typically maintains detailed files for each prisoner that are comprehensive, covering all individuals who enter the prison system, and offer a high level of detail about individual offenders, such as the nature of their offence, sentence imposed, participation in educational or work programmes and involvement in any incidents. Policymakers can use these data (in aggregated and anonymized form) to gain valuable insights into the offender population, assess the effectiveness of social reintegration programmes and design more targeted interventions, among other things.

Long-term data availability

Administrative data are often collected over an extended period of time, with some administrative records going back multiple decades, allowing for the study of long-term trends and patterns in crime and criminal justice data. An example is the tracking of homicide data over time, which can provide valuable insights into characteristics of both victims and offenders, the relationship between them, the type of weapon used, and how these factors have changed over time. This enables a more comprehensive understanding of the dynamics involved and the development of more effective crime prevention strategies.

Reduced response burden

Policymakers can access pre-existing administrative data that have been collected as part of routine operations instead of relying on individuals to provide information through survey instruments. This can be particularly beneficial for avoiding retraumatizing victims when obtaining information after the fact and/or following up on data collection with hard-to-reach offenders.

Administrative data thus offer clear benefits that can assist in the effective day-to-day management of criminal justice institutions, the prevention of crime and the equitable delivery of justice. A number of key challenges are also associated with administrative data, however, as highlighted below.

Lack of standardization

Often, concepts, definitions and methods covering administrative data are not harmonized across different agencies and institutions. Each data provider may even have their own system(s) and process(es) in place for collecting administrative data. For example, the police may classify criminal offences differently from the prosecutor's office or have different counting and validation rules. Moreover, different departments within the same institution may use different systems of classification or data recording mechanisms.

This lack of standardization can lead to variations in data formats, definitions and statistical outputs across different sources, which in turn negatively affect data interoperability prospects. Harmonizing and integrating data from multiple administrative sources can be complex and require considerable effort. The implementation of ICCS and other internationally endorsed statistical standards and guidelines is an important means of addressing such problems and building harmonized, interoperable systems that maximize the potential of administrative data for statistical purposes.

Data quality and reliability issues

Administrative data can be comprehensive and highly detailed, but they are not immune to human error. Missing values, data entry mistakes, inconsistencies and poor reporting are common problems that can greatly impact the quality of the data. For example, the complexity of certain offences, such as those involving multiple charges or overlapping legal elements, can present challenges in accurately classifying them.

Moreover, errors in recording the offence code or failing to document certain details of the offence accurately can affect the reliability of the data. This can be strongly influenced by factors such as limited training or inconsistent practices among data entry personnel. Efforts to enhance training, standardize coding practices and implement quality control measures can help address these challenges and improve the accuracy and reliability of the data for analysis and policymaking.

Non-representativeness

Administrative data may not represent the population of interest accurately and be limited in scope. For example, administrative data in the criminal justice system only cover offences that are reported to or detected by competent authorities, providing no information on crimes that, for whatever reason, go unreported. If administrative data are exclusively relied upon, the prevalence of crime will thus be underestimated. Determining the true prevalence of crime is one of the main uses of additional data sources such as crime victimization surveys.⁸

Use of legacy systems

The collection of administrative data lacks flexibility since data recording formats and the data recording system itself are typically difficult to change. Also, data recording systems may have been designed and implemented years or even decades earlier. Such legacy systems may have limited

	<p>functionality, lack compatibility with modern standards and rely on outdated or unsupported software or hardware.</p> <p>Addressing the challenge of legacy elements in administrative data recording systems requires significant investment when developing modern, flexible and interoperable solutions. Although such transitions can be complex and costly, modernizing data recording systems and promoting the use of IT platforms that respect privacy, security and confidentiality policies within the criminal justice system can improve data quality, enhance data management capabilities and enable better information sharing and analysis – facilitating interagency collaboration, data interoperability and evidence-based decision-making.</p>
<p>Data access barriers</p>	<p>Methodological and technical difficulties can arise when managing access to administrative data sources, such as performing record linkage and integrating data across multiple administrative data sources, transmitting the data through secured channels and integrating them with data from other statistical sources. Moreover, establishing data-sharing agreements and obtaining the necessary approvals can be time-consuming, especially when there is a lack of clarity about the roles and responsibilities of different stakeholders.</p> <p>Different agencies or levels of government (for example, local, state, federal) may also have varying policies and procedures regarding data access or there may be trust barriers that prevent institutions from sharing data. This can potentially lead to the fragmentation of data and impede the viability of comprehensive data sets that cover the criminal justice system more holistically. Issues such as these can be addressed by implementing a strong data governance framework, which is discussed in greater detail in chapter 3 of the present guidelines.</p>
<p>Privacy and confidentiality concerns</p>	<p>Preserving the security and confidentiality of individuals when disseminating detailed statistics can be challenging, since administrative data often contain sensitive and personally identifiable information. This is especially true in the criminal justice system where data are often collected in challenging circumstances without giving individuals the chance to opt out (i.e., informed consent). Care has to be taken to protect individual privacy and adhere to legal and ethical guidelines for data handling, storage, anonymization and sharing.</p>
<p>Lack of documentation</p>	<p>Administrative data often lack documentation about how they were produced and on validation mechanisms in place to ensure data quality. Moreover, often there is little to no systematic recording of metadata (see Box 12 for more information on metadata). Without a thorough understanding of data collection and production practices, interpretation and analysis may lead to incorrect conclusions.</p>

2.3 Stages of the criminal justice process

Generally, four institutions are involved in the criminal justice process: the police, the prosecution service, the courts and, in the case of a guilty verdict and a custodial sentence, the prison system. There is a great deal of variation between Member States and jurisdictions in how exactly this process is organized and the powers assigned to each of the institutions, but that is the general direction of flow in the criminal justice process. Each institution involved produces a wealth of administrative data that can be used to inform policymaking and contribute to fairer and safer societies. A schematic overview of the flow is highlighted in Figure 1.

Note that a single criminal case can address one or multiple offences against one or more victims committed by one or more offenders. The data system thus needs to be flexible, as each new criminal case should record information that will allow for the generation of aggregate statistics at either the offence, case or person level.

Figure 1 Stages of the criminal justice process



Data recorded by the police normally represent the first stage in any system of crime and criminal justice statistics. Criminal events reported to or detected by the police are often used as a proxy for crime rates within the respective country. ICCS provides offence coding for classifying crimes along with a set of recommended disaggregating variables for collecting additional data on the characteristics of an event, victim and offender. In addition, the *Guidelines for the Production of Statistical Data by the Police* recommend the systematic collection of administrative data in four thematic areas, namely resources, crime statistics, other activities (such as community outreach) and conduct (for more information on the framework and the recommended variables, refer to the guidelines).⁹

In most criminal justice systems, the second stage involves the prosecution service. In essence, prosecution involves the initiation or confirmation of a formal criminal charge against an individual.¹⁰ Ideally, the case data contain a unique identifier that can be linked to police records. One challenge can be the correspondence between the crime incident as classified by the police and the charge assigned by the prosecution service. The prosecutor may decide that certain charges cannot be prosecuted due to a lack of evidence or add additional charges to a case as the investigation proceeds. If, in addition, different classifications are used by the police and the prosecution service, statistics become even more difficult to compare across the different stages of the criminal justice system.

In the third stage of the criminal justice process, data are generally collected by the courts when a new case is filed. The court component of the system may range from local courts with limited jurisdiction to general trial courts, appellate courts and courts with specialized jurisdictions, such as tax courts or juvenile courts.

Administrative data from the prosecution service and the courts provide information that can help monitor case filings, case processing times, conviction rates, case dispositions, case loads and more. The *Guidelines for the Production of Statistical Data by the Prosecution Service and the Courts* recommend the systematic collection of data along four thematic areas, namely resources, criminal justice statistics, other activities (such as extradition and mutual legal assistance) and conduct (for more information on the framework and the recommended variables, refer to the guidelines).¹¹

Administrative data held by the prison system are primarily concerned with persons entering a prison on pre-trial detention or to serve a custodial sentence ordered by a court. A prisoner file is opened for each new individual who enters a prison facility. Although collected at the final stage of the criminal justice process, these data are no less crucial for policymakers and the effective and equitable organization of a criminal justice system. In addition to the basic data necessary for the calculation of indicator 16.3.2. of the Sustainable Development Goals (unsentenced detainees as a proportion of overall prison population), many other data points can be collected that facilitate the safe, secure and humane custody of prisoners and their rehabilitation and social reintegration as well as provide guidance to authorities on at-risk populations for crime prevention policies. The *Guidelines for the Production of Statistical Data by the Prison System* recommend the systematic collection of administrative data in five thematic areas, namely prison resources, prisoner profile, reintegration, safety and security, and staff conduct (for more information on the framework and the recommended variables, refer to the guidelines).¹²

2.4 Organizational modes of statistical systems¹³

Countries have different organizational models that affect how criminal justice is structured and how the national statistical system (NSS) is configured. The NSS of a country comprises the national statistical office (NSO) and all other public producers of official statistics in the country.¹⁴ In the case of the criminal justice statistical system, this includes the police, the prosecution service, the courts, the prison system, the ministry of justice and any other actors involved in the collection, production and dissemination of crime and criminal justice statistics, such as forensic agencies and coroners' offices. Any system of criminal justice statistics has to take into account the needs of a country, its criminal justice system, its degree of (de)centralization, its traditions and the availability of personnel and resources. No single blueprint will be able to fit such a range of circumstances. This section presents some of the main advantages and disadvantages of different organizational approaches to national criminal justice statistical systems.

Centralized statistical systems

Statistical systems are said to be centralized when all, or most, of the products of the statistical system are produced and disseminated by a central organization at the national level. A good example is the Australian Bureau of Statistics, which produces almost all of the country's national statistics, including those related to crime and criminal justice.¹⁵ In a decentralized system, by contrast, the responsibility of producing and compiling official statistics can reside with many different ministries, departments or agencies (MDAs).

In a centralized system, data from local units, such as a police department, local prosecutor, court location or prison facility, are sent directly to the organization responsible for producing statistics, which can be an independent organization, an agency within a national ministry or department responsible for justice, or a department within the existing NSO.

Each of the above three centralized approaches comes with a number of advantages and disadvantages. For example, an independent agency may have more credibility and be in a better position to monitor the overall system in a more holistic manner. However, creating a new agency utilizes scarce resources and an independent office may struggle to establish good relations with the operational agencies that produce the data without a supportive legal framework. An agency within a national ministry or department responsible for justice will likely facilitate greater use of the data, but the credibility and objectivity of the agency may be questioned. Lastly, a specialized unit or department within the NSO would have ready access to complementary data sets and a skilled statistical workforce, but such a unit may not be prioritized by the NSO and may be far removed from the users of criminal justice statistics or face obstacles to access and publish criminal justice data.

Decentralized statistical systems

In the case of decentralized systems, the two main forms of decentralization are territorial decentralization and institutional decentralization, although in a number of countries the system is a mixture of these two forms.

Territorial decentralization often reflects the general political and administrative structure of a country. A straightforward example is the production of crime and criminal justice statistics at the provincial or state level. The advantage of collecting data in a territorially decentralized manner is that this will likely result in a data collection, production and dissemination process that is more relevant at the local level. However, individual provinces or states may not be sensitive to national level needs and may be unwilling or unable to ensure the interoperability of their data with those collected and produced by other provinces or states.

Different organizational solutions may exist in countries with regions that have some degree of autonomy (such as in a federal system). In most such systems, the collection, production and dissemination of statistical information is primarily the responsibility of statistical offices at the regional or local levels. In such cases, the NSO normally plays an important coordinating role, but this may only apply to certain types of statistics, with regional statistical agencies having the capacity to deal with specific regional statistical needs. More detail on the organizational models in federal countries can be found in the *The Handbook on Management and Organization of National Statistical Systems*.¹⁶

Institutional decentralization implies that each component of the criminal justice system produces its own statistics from its administrative data. The NSO typically plays a coordinating role instead of overseeing the compilation and production of all crime and criminal justice statistics. Each individual

institution is in a strong position to arrange for and ensure the collection of data within its own institution. Moreover, the personnel involved in the collection of data can be expected to have a high level of commitment to the accuracy and reliability of the data. The major limitation of this approach is that each institution will have the tendency to collect administrative data according to its own needs, priorities and available resources without considering which statistics may be relevant for other institutions or aligning concepts and definitions across the criminal justice system as a whole. In addition, as they are not statistical entities, the individual institutions may not employ qualified statisticians or be aware of or willing to comply with the United Nations Fundamental Principles of Official Statistics.¹⁷

Impact of organizational modes

Decentralization at either the territorial or institutional level strongly affects crime and criminal justice statistics. The different components of the criminal justice system are composed of independent institutions with a thematic or territorial scope. There are countries, such as Mexico and the United States of America, where law enforcement and access to justice are responsibilities shared by different levels of government, and various bodies compile administrative data that need to be collated at the state or federal levels in order to produce national statistics on crime and criminal justice. Other countries such as Estonia and the Republic of Korea have a stronger centralized tradition, with a lower degree of territorial decentralization. As seen throughout the present guidelines, the level and type of decentralization has the potential to affect the governance of data across various institutions.

2.5 Producers and users of statistical data on crime and criminal justice¹⁸

Systems of criminal justice statistics have varying degrees of organizational complexity, with statistics and data being collected and produced by the police, the prosecution service, the courts, the prison system, different ministries (Ministry of Justice or Ministry of Interior, for example), legal aid bodies and alternative criminal justice mechanisms. In addition, each of these institutions may be decentralized, both in territorial (local, regional or federal police, for example) or institutional terms (appeal courts or juvenile courts, for example). Combining data from the various parts of the criminal justice system allows for the production of more detailed crime and criminal justice statistics and better monitoring of the system as a whole. As noted in the *United Nations Manual for the Development of a System of Criminal Justice Statistics*, of 2004, an interoperable data system would be able to answer many policy-relevant questions, including:

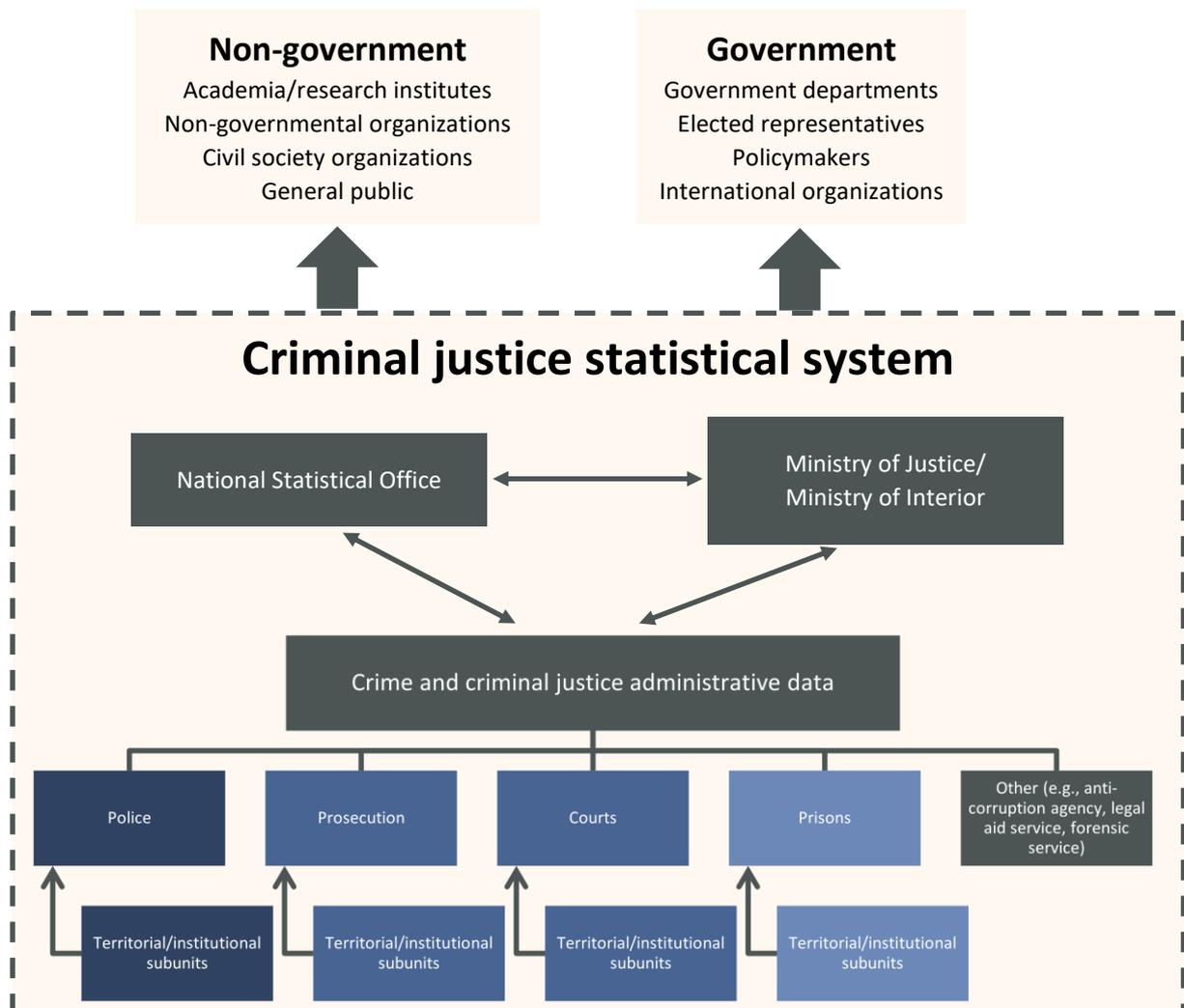
- Which areas of the country have the highest levels of reported crime?
- How many charges lead to prosecutions and convictions?
- How much does the Government spend on criminal justice?
- What type of sentences are given for different types of offences?
- Does the criminal justice system treat all alleged offenders equally?

The scope of a crime and criminal justice statistical system should not be limited to data producers, however, as the needs of data users beyond the criminal justice system itself should also be considered. Other government entities beyond the criminal justice system or international organizations also regularly request information in order to monitor different parts of the criminal justice system and measure progress towards the Sustainable Development Goals. Moreover, academia and civil society organizations can request access to various types of data, which can play a

critical part in ensuring continued support for the use of state power by the criminal justice system through transparency and accountability.

As data and statistics are most valuable when they are used, to enable their use and reuse, the crime and criminal justice statistical system should consider both internal and external users. The end user of the statistical outputs should be carefully considered in all steps of the process, from the design of data collection activities to their dissemination. The needs of criminal justice institutions, researchers, non-governmental organizations, national or regional institutions (such as the Ombudsman or equality bodies), other parts of the Government, international organizations and the general public are key to the design of statistical outputs that are relevant and will be in high demand. In other words, the value of crime and criminal justice statistics should not only be measured by the quality of the data but also by their potential use for strategic decision-making at different levels of government, their use by society at large and their contribution to the achievement of fair and equitable justice for all. Figure 2 schematically represents the complexity of criminal justice statistical systems.

Figure 2 Producers and users of crime and criminal justice statistics



2.6 Approaches to data collection

The format of data collection and data storage are important because they largely determine the processes needed for transferring and linking information to a national data collection system. Much information about the activities of the criminal justice system is initially recorded on some type of manual form that may or may not be transferred to a digital environment at a later stage.

Manual environment

In a purely manual environment, in which all or most information is stored on paper, information is usually transferred to the national data collection system through the use of questionnaires or data-collection forms, which contain boxes asking for different types of information. Respondents typically keep track of the required information manually using tally sheets and forward the results to the relevant institution on a regular basis. This is the case in Kenya, for example, where data collection is primarily done on paper and the NSO collects the information on standardized forms or even by telephone in the case of some inaccessible areas.

Automated environment

In automated environments all or most of the required data are stored in a digital system. Different options are available for transferring data from the operational system to the statistical office, the first being to send files summarizing the various data elements to the statistical office/unit. In the United States, many different institutions are involved in criminal data collection at the state or local levels and each can have its own crime management and database systems. Much of the information is aggregated at the federal level through surveys sent to all institutions.

The second option is to share (anonymized) microdata containing various data elements, which are then sent to the statistical office either in a hard copy or electronically via a secure means of data exchange. In the United States, such data are collected through the National Incident Based Reporting System (NIBRS) (for more details, see Box 13).

The third option is to have integrated systems, in which key data systems are readily accessible by all relevant institutions through electronic means, allowing for the generation of near real-time dashboards and statistics. A single, shared database management system for all institutions involved in crime and criminal justice is not common practice, however. Typically, each institution has its own recording mechanism or information system(s) and the information is later shared with a central system for statistical purposes. This is the case in the Republic of Korea, for instance, where each agency (the National Police Agency, the Supreme Prosecutors' Office and the Supreme Court of Korea) has its own standards and case management system. The information from each of these individual systems is shared with the NSO and harmonized in order to produce statistics for the whole country. In Estonia, information from different institutions is shared using an interconnected IT system and common statistics are generated in near real time. More details about Estonia and the Republic of Korea can be found in the case studies in the annex of the present guidelines.

Mixed environment

In some countries, there may be mixed environments where part of the information is collected and stored purely in paper form while other parts are housed in a digital environment. This is the case in Argentina, for example, where local police stations send paper summaries of each procedure to the central provincial unit, which oversees the input of all this information into a provincial management

system. The information is digitally aggregated at the national level by submitting part of the provincial information to a national IT system, either manually or using Excel files.

While collecting paper-based data may seem more affordable than doing so digitally, significant resources are required for capturing, aggregating and analysing such data. Moreover, paper-based data collection is vulnerable to human error and can lack sufficient methodological clarity (transparent counting and aggregation criteria, for example). Digital technology makes data collection vastly more efficient and provides greater flexibility in subsequent analyses; however, digital environments can differ between institutions or jurisdictions, making linking and aggregating the data more challenging. Digital environments also require the creation of interoperable IT systems and staff with technical skills who can design, maintain and continuously update and improve the different systems. This is the focus of chapter 3 of the present guidelines.

Box 1 Resources for improving the quality of administrative data

United Nations National Quality Assurance Frameworks Manual for Official Statistics (UN NQAF)¹⁹

Including recommendations that are directed at assuring the quality of official statistics throughout the entire national statistical system (NSS), this manual provides guidance for engagement with statistics producers and data providers from outside the NSS that cooperate in the production of official statistics and addresses quality assurance in the use of different data sources. As a result, the manual responds to the challenges posed by the new data ecosystem, which is characterized by the emergence of new data sources and new data providers and statistics producers. The manual can support the work of countries that are in search of quality assurance frameworks. In addition, those already using a quality framework can use the manual as an additional reference point that supports what they are already doing, and as a source of information on the application of quality assurance in different situations.

The United Nations Expert Group on National Quality Assurance Frameworks has issued a self-assessment checklist based on the Quality Assurance Framework contained in the manual, which is meant for conducting regular and rigorous quality assessments with the objective of identifying improvement actions. Also of use for providing an initial assessment of learning purposes and introducing staff to quality assurance, the checklist is available at:

<https://unstats.un.org/unsd/methodology/dataquality/tools/>

Guidelines for the production of statistical data by criminal justice institutions

As noted in the introduction, the present guidelines are part of a series aimed at improving the collection, production and dissemination of administrative data for statistical purposes in the criminal justice system. The three other guidelines in the series focus on specific parts of the criminal justice process and offer concrete recommendations on which administrative data to collect, illustrated with practical examples from around the world. The specific parts covered are the police, the prosecution service and courts, and the prison system. For more information, refer to the UNODC website:

<https://www.unodc.org/unodc/en/data-and-analysis/statistical-activities.html>.

Collaborative on the use of administrative data for statistics²⁰

In May 2020, the United Nations Statistics Division (UNSD) and the Global Partnership for Sustainable Development Data established a multi-stakeholder collaborative of countries and regional and international agencies aimed at strengthening the capacity of countries to use

administrative data sources for statistical purposes. Members of the collaborative work together in a coherent and cross-cutting manner to address both urgent and longer-term needs around the access and use of administrative data for statistical purposes. A platform for sharing resources, tools, best practices and experiences, the collaborative contributes to raising awareness among all members of national statistical systems about the benefits of sharing and combining administrative sources for enhancing the quality, timeliness, coverage and level of disaggregation of statistical data.

Box 2 Evolution of the data management system in Uruguay²¹

Since the centralization of police communications in the 1980s, Uruguay has continually worked to modernize its Public Security Management System, establish standards and procedures and promote data interoperability.

Established in 1996, the Oficina Centralizadora de Información Táctica (OCIT) was tasked with the management and use of (georeferenced) data for tactical purposes. The system was programmed in the Clipper programming language and was supported by a central server operating on Windows NT, which could be accessed from workstations operating on MS-DOS, Windows 3x, Windows 95 and Windows NT.

In 1998, a new project was launched with the help of the Inter-American Development Bank and the United Nations Development Programme. Within this framework, the Police Management System (SGP) for the police headquarters of Montevideo and Canelones was developed. Eventually, all the other police departments in the country joined in, which facilitated the transition away from traditional Excel templates to a fully digital system. This development was a joint effort between OCIT staff and staff from the University of the Republic (Udelar) and University ORT Uruguay. At the time, new computer infrastructure was also installed at the Montevideo police headquarters and subunits, which included the installation of network cabling, computers, printers and communications infrastructure.

The next step in the evolution of the system began in 2008 with the creation of the División de Sistemas de Información (DSI), bringing new features to the system in 2011. The first main change was technological, involving moving from a desktop application to a web-based application. The second major overhaul was the move from individual databases in each department to a single centralized system. This can be characterized as the start of the transition to the current Public Security Management System (Sistema de Gestión de Seguridad Pública (SGSP)). These technological developments required connectivity at the national level, which was achieved by investing in a server room, configuring the equipment around the country and installing wireless internet where necessary. It also involved training staff in police units throughout the country over a period of two months.

The use of mobile devices and tablets was incorporated into the SGSP system in 2013, a year that also featured the launch of the online complaint system, which is a publicly accessible website that interacts with SGSP and allows users to register and track complaints. Other important recent milestones are the entry into force of the new Code of Criminal Procedure in 2017, which enabled prosecutors to work directly with police officers through SGSP, and the launch of the “0800-Abigeato” instrument, a free telephone line for reporting livestock theft that is linked to the SGSP system. Finally, a recent development in the area of domestic violence includes the realization of

interoperability between the electronic monitoring system and SGSP, which enables the better monitoring of people wearing electronic monitoring devices.

As a result of the above developments, the National Police, the Ministry of the Interior and other relevant criminal justice actors now have access to a comprehensive information management system. By the beginning of 2021, all 280 police stations in Uruguay were connected to the SGSP and some 2,650 offices/departments had access to it. This means that roughly 30,000 users had access to the system, of whom 18,000 were permitted to enter information.

2.7 International data collection on crime and criminal justice

Although the focus of the present guidelines is on the development of a national system of criminal justice statistics, it is helpful for national offices involved in the collection of crime statistics to be aware of efforts to collect administrative data related to crime and criminal justice at the international level. At the global level, the administrative data collected at the national level feed directly into the United Nations Survey of Crime Trends and Operations of Criminal Justice Systems (UN-CTS).

The United Nations Economic and Social Council, in its resolution 1984/48 of 25 May 1984, requested of the Secretary-General the maintenance and development of the United Nations crime-related database by continuing to conduct surveys of crime trends and the operations of criminal justice systems. The major goal of UN-CTS today is to collect data on the incidence of reported crime and the operations of criminal justice systems in line with ICCS. The UN-CTS survey results provide an overview of trends and interrelationships between various parts of the criminal justice system in order to promote informed decision-making, nationally and internationally.

The data collected through UN-CTS are disseminated through the UNODC Data Portal (<https://dataunodc.un.org/>). Also used to monitor progress towards key Sustainable Development Goal 16 targets, the data are presented in several analytical publications, such as the *Global Study on Homicide* (<https://www.unodc.org/unodc/en/data-and-analysis/global-study-on-homicide.html>) and short research briefs included in the *Data Matters* series (<https://www.unodc.org/unodc/en/data-and-analysis/data-matters.html>). UN-CTS data pertaining to crime-related Sustainable Development Goal indicators are also published on the United Nations SDG Global Database (<https://unstats.un.org/sdgs/dataportal>).

UN-CTS relies on a network of national focal points responsible for compiling and submitting the questionnaire to UNODC. Their work is the cornerstone of international statistics on crime and criminal justice. Appointed by each Member State, the UN-CTS focal point is the primary technical point of contact with UNODC regarding the compilation and submission of the questionnaire for ensuring, as far as possible, a timely, accurate and complete response. For more information on UN-CTS and how to nominate national focal points, refer to the UNODC website (<https://www.unodc.org/unodc/en/data-and-analysis/United-Nations-Surveys-on-Crime-Trends-and-the-Operations-of-Criminal-Justice-Systems.html>) or contact our team by email at unodc-cts@un.org.

3 Data governance in the criminal justice system

Data governance can be defined as a system of decision rights and accountabilities for the management of the availability, usability, integrity and security of the data and information, and the resulting regulations, policies and frameworks that provide enforcement.²²

Data governance concerns decisions about data-related matters and ensuring data are fit for purpose. It focuses on establishing roles and responsibilities within the data lifecycle in relation to the availability, interoperability, security and integrity of the data that are collected and stored, and on establishing policies for access to, sharing of and (re)use of data and the conditions under which data access can be granted. In short, data governance entails taking decisions about the people, the processes and the technologies involved in managing data.

Broadly speaking, the technologies and methods necessary for making data speak to each other between different systems already exist. Rather, the most serious impediments to the creation of systems that are interoperable are often related to how data are produced, managed and how the lifecycle of data within and across organizations are governed.²³ Effective data governance systems are thus crucial to the effective management of data through the data lifecycle, from collection, storage and processing to dissemination, use and reuse.

There may be a tendency to view data as a technical issue or by-product of daily operations that should be dealt with by IT departments, but data are a strategic asset that should be dealt with at multiple levels, from the decision-makers that define strategies and design policies, to the staff who implement and deliver services. Data should be a cross-cutting issue for any ministry, department or agency (MDA) involved in the criminal justice system in the same manner as human rights, access to justice, gender or the Sustainable Development Goals.

Data interoperability is about ensuring that systems are using the same set of definitions, classifications and methodologies, as well as technologically compatible platforms, allowing for full harmonization of interfaces and access protocols.²⁴

Modern public data governance arrangements are designed to foster data interoperability. Interoperability is a key enabling factor in promoting the digitization of administrative data and allowing for the electronic exchange of meaningful information between MDAs in ways that are understood by all parties. It can be achieved at four distinct levels:²⁵

- **Legal interoperability** is about ensuring that laws, regulations and legal frameworks do not prevent the exchange, use and reuse of data for justified purposes between different MDAs in the criminal justice system and beyond. It involves ensuring compliance with relevant legal frameworks and addressing issues such as data security, privacy and liability.
- **Organizational interoperability** refers to the way in which MDAs align their business processes, responsibilities and expectations to achieve commonly agreed and mutually beneficial goals. In practice, organizational interoperability implies aligning business processes and addressing challenges related to communication, workflow integration and decision-making processes.
- **Semantic interoperability** ensures that the precise format and meaning of exchanged data and information is preserved and understood when exchanged between parties. In other words, it ensures that what is sent is what is understood. Standard classifications and

vocabularies, such as those discussed later in this chapter, enable semantic interoperability across different applications and systems.

- **Technical interoperability** covers the compatibility of different applications, interfaces and protocols, which enables the exchange and use of data or services. Aspects of technical interoperability include data formats, interface specifications, communication protocols and security mechanisms. This ensures that different systems or technologies can work together seamlessly.

Linking data from different data sources is particularly important for criminal justice systems, which, by definition, have complex structures and are the custodians of highly sensitive data. The output of one agency within the system can serve as the input of another. For example, cases brought to the prosecution service by the police represent output statistics for the police and input statistics for the prosecution service. Similarly, cases disposed by the courts that result in a custodial sentence are both a judicial output statistic and a prison input statistic.²⁶ For this reason, there is much to gain from a criminal justice statistical system that is interoperable and where administrative data are shared within and between institutions using unique identifiers, while ensuring compliance with relevant legislative and ethical frameworks. This chapter pays special attention to the role of interoperability in creating a criminal justice system that allows for the collection, production, dissemination, use and reuse of administrative data for monitoring performance, evidence-based policymaking and improving equitable access to justice for all.

Building on previous work by the Organisation for Economic Co-operation and Development (OECD) and the United Nations Economic Commission for Europe (UNECE) that focused on data governance in the public sector,²⁷ four elements have been identified that are essential for good data governance and data interoperability: vision and leadership in the medium to long term; the need for regulatory instruments that translate this vision into legal acts and guidelines; coordination and cooperation among the different institutions involved in the production of administrative data; and the data architecture that provides the models, policies and standards as well as the IT solutions to build the criminal justice statistical system.

Figure 3 Data governance framework

3.1 Vision and leadership	3.2 Regulations	3.3 Coordination and cooperation	3.4 Data architecture
3.1.1 Vision and strategy	3.2.1 Statistical legislation	3.3.1 Formal mechanisms	3.4.1 Data standardization
3.1.2 Leadership	3.2.2 Regulations on data privacy and security	3.3.2 Informal mechanisms	3.4.2 Statistical processes
3.1.3. Data stewardship	3.2.3 Operational guidelines	3.3.3 Memoranda of understanding	3.4.3 Managing the data life cycle
	3.2.4. Ensuring regulatory coherence	3.3.4 Use of standards	3.4.4 Data security
			3.4.5 Data quality
			3.4.6 Use of open data standards

Source: UNODC, based on Organisation for Economic Co-operation and Development (OECD), *The Path to Becoming a Data-Driven Public Sector* (2019).

It is important to note that national contexts can differ and some countries may face more difficulties than others as they lack the infrastructure and skills to capture data and the institutional and regulatory frameworks to create trust in data systems.²⁸ Moreover, statistical capacity and data literacy remain limited in some countries and the capacity to exchange data rapidly and secure cost-effective access to modern data storage and cloud computing facilities may be lacking, although such countries can also use the latest technology to leapfrog the statistical development process. Whatever the national context, the four elements identified above can serve as a road map for the improvement of the criminal justice statistical system in any country. They represent the basic building blocks that should be in place to improve the ability to collect, produce and disseminate relevant crime and criminal justice statistics.

A non-exhaustive list of sample assessment questions for each of the four elements is included in the following sections. The questions are meant to offer a starting point for evaluating the maturity of a system of criminal justice statistics. Countries are encouraged to customize these questions according to their specific contexts and needs and expand on them whenever relevant.

3.1 Vision and leadership

3.1.1 Vision and strategy

Vision involves articulating a desired future state or outcome for crime and criminal justice statistics then formulating policies and strategies that align with that desired outcome. Vision acts as a guiding principle for ensuring policy coherence and consistency in the governance of data across different MDAs, both within and outside the criminal justice system. It also helps policymakers integrate various initiatives and align them with the role they have designated to crime and criminal justice statistics in society, minimizing contradictory or conflicting policies.

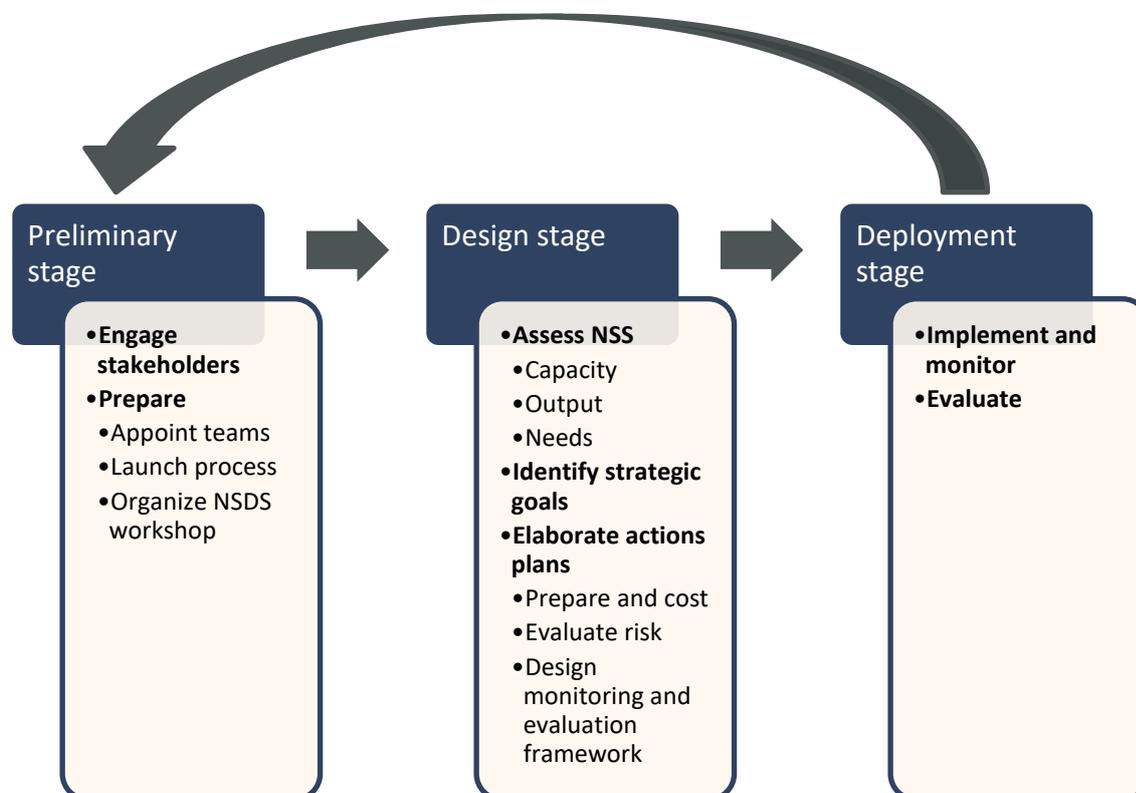
The translation of vision into reality typically requires the creation of strategic documents that are applied at the territorial (national/regional/local) and/or institutional levels. Achievable priorities should be set to ensure that the vision is operationalized with a clear scope and timeline. It is also important that the establishment of a vision and the related strategic documents are developed in partnership with the institutions of the criminal justice system and other key stakeholders beyond the system, such as the NSO and other data users. This broad participation can facilitate long-term commitments and align all stakeholders with a shared vision.

In Ireland, the Criminal Justice Sectoral Strategy 2022–2024, jointly developed by the Department of Justice, Courts Service, Prison Service, Probation Service, National Police, Legal Aid Board, Public Prosecution and Forensic Service provides an example.²⁹ The vision it sets out is the creation of a joined-up criminal justice system that respects human rights, builds public confidence and trust, and works together to improve the experience of users of the criminal justice system. One of the five strategic pillars of the strategy is focused on data and improved interoperability to facilitate the use and sharing of high-quality data that can inform evidence-based decision-making across institutions. The strategy also notes that this will require improved management and use of knowledge, data and research through the ability to link different criminal justice data sets and thinking beyond organizational boundaries.

Another example, PARIS21 developed guidelines for countries to develop and strengthen their NSS by developing and implementing a National Strategy for the Development of Statistics (NSDS),³⁰ which provides countries with a five-to-ten-year strategy for developing statistical capacity across the entire NSS and effectively responding to increasing national, subnational and international data demands.

NSDS is designed to be in line with a country’s national development plan and other international and regional data requirements and is meant to be a government-owned strategy. The NSDS lifecycle consists of a preliminary stage, a design stage and a deployment stage (see Figure 4).

Figure 4 **National Strategy for the Development of Statistics (NSDS) life cycle**



Source: Based on Paris 21, “NSDS Lifecycle”, available at <https://new.nsdsguidelines.paris21.org/nsds-lifecycle>.

Box 3 Strategic work on data in the United Kingdom

National data strategy³¹

At the national level, the Government of the United Kingdom of Britain and Northern Ireland developed and published a National Data Strategy in 2019. The overall objective of the strategy is to build a world-leading data economy while ensuring public trust in data use and the data ecosystem and that people have the skills required to operate within it and access data when they need to. Additionally, the strategy creates a shared understanding of how data are used and provides coherence to a wide range of data related activities across the Government.

Ministry of Justice digital strategy³²

This line of thinking has been followed by the Ministry of Justice, which oversees the collection, production and dissemination of crime and criminal justice statistics. The Ministry of Justice elaborated a digital strategy to set its priorities for the period 2022 to 2025 and specify the outcomes it hopes to achieve. The ministry’s vision is to deliver a justice system that works for everyone in society by making the user experience of justice simpler, faster and better for all.

Practically speaking, the Data Improvement Programme of the Ministry of Justice is focused on creating a more data-driven justice system through a three-year data improvement plan. A core

theme is the improvement of the quality of data, the flow of data and data interoperability. The programme sits within the Performance, Strategy and Analysis Group in the Ministry of Justice and is divided into five workstreams: i) data landscape; ii) data architecture; iii) data sharing and linking; iv) data governance; and v) data culture, literacy and ethics.

National Police digital strategy³³

The Digital Policing Strategy 2020–2030 was developed in response to the digital challenges facing the police in the United Kingdom. At the heart of the police’s digital transformation both locally and nationally, the strategy contains five key digital ambitions, each with a set of digital priorities to guide focus and investment: i) deliver a seamless experience for the public; ii) use digital technologies to identify and mitigate potential harm and protect vulnerable individuals; iii) invest in personnel and establish digital leadership; iv) foster openness and collaboration with public sector partners; and v) strengthen the relationship with the private sector in order to share in public safety responsibilities appropriately.

Other actors

The above provides an illustration of how national-level data strategies can feed into different MDAs. Other actors involved in the collection, production and dissemination of crime and criminal justice statistics in the United Kingdom – such as the Home Office, the Attorney General’s Office, the Crown Prosecution Service, HM Courts & Tribunals Service and HM Prison and Probation Service – all have equally key roles to play in ensuring the interoperability of data and promoting their use.

3.1.2 Leadership

Vision alone, however, will not drive change without adequate leadership, which is crucial to the push for the implementation of policies that contribute to a strategic vision about the role of crime and criminal justice data and statistics. Leadership is essential for designing and driving the process of creating effective policies and formulating strategies that address the need for crime and criminal justice data in society. The case studies in the annex to the present guidelines highlight the fact that strong political support is crucial to building an interoperable statistical system across the different institutions of the criminal justice system. Leadership is key to improving the collection, production and dissemination of crime and criminal justice statistics across the different institutions, enhancing data interoperability and promoting the use and reuse of data.

In Estonia, for example, strong political support has enabled the interconnection of all institutions within the criminal justice system and linked the interoperable system with several other MDAs outside it. Estonia places a lot of emphasis on developing interoperable technical solutions across all government institutions and has moved towards a fully digital criminal justice system. The Republic of Korea also has an interoperable technical system with strong political support. The Korean case study in the annex to the present guidelines shows the importance of both high-level political leadership in reaching agreements that can be translated into regulatory instruments and mid-level operational leadership that steers the process on an operational level.

The importance of leadership is also illustrated by the experience of other countries. In Ecuador, for example, the commitment from top-level political leadership enabled the creation of an advanced national monitoring system for intentional homicides and femicides compiled by the Special Commission on Security, Justice, Crime and Transparency Statistics with data updated monthly since January 2014 (see Box 4).

Box 4 Special Commission on Crime Statistics in Ecuador³⁴

The aim of the Special Commission on Security, Justice, Crime and Transparency Statistics in Ecuador is to promote the production of statistics and strengthen information on security, justice, crime and transparency through the design, development and implementation of statistical plans and projects in order to ensure compliance with the national development agenda, sectoral and territorial agendas, and international development plans.

The commission collaborates in the preparation of sectoral statistics programmes and suggests adjustments in the production of statistics by the various bodies of the National Statistical System. The commission also proposes the principles, standards and guidelines that can be applied for the coordination within the National Statistical System.

Commission members include, the National Institute of Statistics and Censuses (INEC), the Ministry of Interior (MDI), the Ministry of National Defence (MIDENA), the National Planning Secretariat (SNP), the National Police (PPNN), the Attorney General's Office (FGE), the Judiciary Council (CJ) and the National Service for the Comprehensive Care of Adults Deprived of their Liberty and Adolescent Offenders (SNAI).

For details on the history of the commission and its achievements to date, see the case study in the annex to the present guidelines.

3.1.3 Data stewardship

Although political leadership provides the high-level support needed to advance the policy agenda, it can be subject to potential changes in political will (for example, after a change of Government). The support of leadership by high-ranking public officials, by contrast, increases the continuity and sustainability needed to deliver results across terms of office.³⁵ Data stewardship can provide such leadership as it is an approach to data governance that formalizes accountability for managing information resources on behalf of others and, in the case of government, in the best interests of the public.³⁶

Data stewardship involves implementing the policies, standards and principles outlined by the data governance framework and ensures the ethical and responsible creation, collection, management, use and reuse of data. It is expressed through the long-term, inter-generational curation of data assets so that they benefit the entire community of data users and are used for the public good. As, in most cases, data stewards are likely to perform a number of roles, their role as data steward should be a formal part of their job description regardless of their primary job title and form part of their performance evaluation.

Data stewardship means ensuring the ethical and responsible creation, collection, management, use and reuse of data so that they are used in the public interest and benefit the entire community of data users.³⁷

The responsibilities listed in the preceding paragraph can be linked with high-ranking public officials in organizations such as the NSO, which is the data steward for the NSS. However, data stewardship should also be fostered within the different institutions of the criminal justice system.³⁸ For example, a court may designate a data steward for data from juvenile courts who is a specialist in data generated in and used by juvenile courts and responsible for monitoring data quality, ensuring data

are suitable for release, making data governance recommendations on matters pertaining to juvenile data, and participating in decisions regarding the exchange of juvenile data.

Having data stewards with clear roles and responsibilities in the different MDAs of the criminal justice system will facilitate the move towards a comprehensive data governance model within the sector. Data stewards can ensure that organizations comply with policy and that internal processes and standards are aligned with other institutions. In this way, data stewards can contribute to data interoperability across the criminal justice system and also contribute to increased trust in the use of data by ensuring public institutions handle data ethically, disseminate data in user-friendly formats and uphold data security and privacy.

Sample assessment questions on leadership and vision

- Has a national strategy or vision for the development and improvement of the criminal justice statistical system with clearly defined priority areas been developed?
- Does a generic data strategy exist for the country as a whole and is the sector-specific strategy aligned with it?
- Are specific goals and targets outlined in the strategy and have they been effectively communicated to and endorsed by all relevant stakeholders?
- Is a mechanism in place to monitor progress towards the goals and targets set in the strategy and update the strategy in response to changing needs and priorities?
- Have dedicated positions been created in each of the relevant institutions to implement the strategy and oversee the ethical and responsible creation, collection, management, use and reuse of data?

3.2 Regulations

Legal frameworks define and give shape to the institutional and administrative structures of a country. Regulations define which institutions comprise the criminal justice system, the degree of territorial and institutional decentralization, and the way the institutions coordinate. Moreover, regulations influence how data privacy and security are guaranteed and delineate which data should be recorded, how it should be collected and who has access to it. Having a strong regulatory environment with clear limits on the use and reuse of data also fosters public trust that the data will not be misused. Public trust in official statistics is vital for the demand for data and their perceived relevance and integrity, as highlighted in the United Nations Fundamental Principles of Official Statistics (for a brief discussion on the role of trust, see Box 5).³⁹

Legislation affects the collection, production, dissemination, use and reuse of administrative data in the criminal justice system through the three main avenues listed in Table 1.⁴⁰

Table 1 **Influence of regulatory instruments and guidelines on administrative data**

Avenue	Description
National law on official statistics	Defines the role of the NSO and its relation to those who are producing data in the different parts of the NSS
National law on data privacy and security	Shapes how data should be handled by the NSO and all other producers of official statistics
Guidelines and handbooks	Clarify methodological and technical issues in order to implement the regulatory instruments across all stakeholders involved in the NSS

All three avenues highlighted in the table above can also be related to or influenced by supranational laws (for example, the General Data Protection Regulation in the European Union), sub-territorial legal acts or other national legal acts relating to data. Examples include regulations on the use of artificial intelligence, freedom of information acts or legislation regulating the activities of producers of official statistics.

Box 5 **Role of trust in the collection, production and dissemination of data**⁴¹

Data create opportunities to improve policymaking and the design and delivery of public services. However, the increasing use of, availability of and access to data raise a number of questions not only about the ethical use, collection, treatment and storage of data, but also about responsibility, accountability, fairness and the respect of human rights in relation to the data. Moreover, increasing access to data while retaining trust is a major challenge. Since trust is difficult to earn and maintain, and even more challenging to restore, preserving public trust has been and will continue to be crucial for Governments. It is therefore important to understand how trust can be maintained through regulations and practices on the use of data.

Countries and relevant MDAs have been developing their own data principles in order to make their practices more ethical and transparent. Building clear data practices is fundamental to retaining citizens' trust. For this to happen, people need to understand how their data are being collected, analysed, stored, disseminated and how long they will be kept for, so that they see the value created by their input, as well as the values and culture of the Government handling the data. Although Governments use different approaches when addressing trust challenges in their respective country, four main elements need to be considered: ethics, privacy, transparency and security.

Ethics refer to ways data are handled without causing direct or indirect harm to anyone. Legislation is one route to ensuring the ethical management and use of personal information in the public sector. Countries may have formal requirements articulating the principles for collecting, processing, sharing, accessing, disseminating and (re)using data in order to prevent, and sanction, behaviour outside the public interest. Another way Governments can establish ethical behaviours is through a framework or the development of guidelines, which provides users with information, resources and approaches to help support ethical practices and decision-making. In order to

enforce ethical practices, countries can establish independent bodies and develop frameworks around the management and use of data.

Privacy is a concept that applies to data subjects. Individuals whose data are being collected should be aware of the purpose of the data collection and their privacy should be protected. People may not be aware of the value of making their data accessible and may fear that they are being monitored by the State. Countries can set formal requirements, including legislation, to protect a person's right to privacy across data collection, storage, sharing, processing and dissemination.

Transparency is an environment in which the objectives of government policies are provided to the public in a comprehensible, accessible and timely manner. Showing people ways in which data are used is an important aspect to ensuring their confidence in public services. Governments can establish frameworks to release standardized information in non-proprietary and user-friendly formats, communicate the intended use of data more clearly and highlight how data feed into decision-making processes. Transparency also involves being clear about the applied methodologies, classifications and procedures involved in the generation of statistics.

Security refers to the measures taken to prevent unauthorized access to or use of data. The importance of data management in government is not only relevant in relation to how it can be applied and made use of to design better policies and to improve services, but also in how it preserves the privacy of people and their trust. People need to know that efforts are being made to ensure that their privacy is respected and that they can trust government to handle their personal information and to protect them from potential risks associated with how government handles their data (see section 3.4.4. for specifics on data security).

3.2.1 Statistical legislation

National statistical laws define the principles of official statistics, the structure of the national statistical system, the coordination within the system, how data collection is carried out and how important issues such as data quality, confidentiality and international cooperation are dealt with. National statistical laws may also define restrictions on the sharing of crime and criminal justice data that contain personally identifiable information due to their sensitive nature. The United Nations Economic Commission for Europe has developed guidance on the development of a generic law on official statistics aimed at supporting further development of legal and institutional frameworks for official statistics based on international recommendations (available in English, French and Russian). The guidance was translated into Spanish and Arabic and adapted by the United Nations Economic Commission for Latin America and the Caribbean and the United Nations Economic and Social Commission for Western Asia for their respective contexts.⁴²

Box 6 Law of the National System of Statistical and Geographical Information (SNIEG) of Mexico^{43, 44}

In April 2008, the Law of the National System of Statistical and Geographical Information (SNIEG) was promulgated in Mexico to change the legal status of the NSO (National Institute of Statistics and Geography (INEGI)) and provide it with technical and managerial autonomy. The main purpose of the NSO is to ensure the NSS provides society and the State with relevant, high-quality and timely information in order to contribute to national development. The guiding principles of the system are accessibility, transparency, independence and objectivity. To enable it to accomplish this purpose, the NSO has the following powers:

- Regulate and coordinate the development of SNIEG
- Regulate statistical and geographical activities
- Produce statistical and geographical information
- Provide public information
- Promote the understanding and use of information
- Safeguard information

SNIEG comprises INEGI, a national advisory council and four national information subsystems, one of which is focused on government, public safety and the administration of justice. This subsystem is aimed at producing, integrating and disseminating information of national interest on the management and performance of public institutions in the area of government, public security and the administration of justice in order to support the design, implementation, monitoring and evaluation of public policies in these areas. The subsystem has an executive committee and seven specialized technical committees (government, public security, administration of justice, prosecution, prison system, human rights and corruption). The specialized technical committees coordinate all data producers and discuss proposals for information of national interest and elaborate proposals for key indicators for consideration by the executive committee.

3.2.2 Regulations on data privacy and security

National regulations on data privacy and security are another pillar of statistical production, with privacy, security and confidentiality being important elements of the Fundamental Principles of Official Statistics.⁴⁵ National statistics are aggregated from individual records and often contain personal information, thus security mechanisms have to be implemented in order to preserve data confidentiality and ensure data are accessible only by authorized people and only on an as-needed basis.⁴⁶ The sensitive nature of crime and criminal justice statistics implies that dedicated rules on the protection of personal data are required in order to facilitate the exchange of data and promote cooperation between the MDAs involved while ensuring the rights of all persons are upheld. In this sense, administrative data in the criminal justice system are not merely used to monitor crime rates but are also a valuable resource that can contribute to crime prevention and ensure the criminal justice system is effective, fair and equitable. Ensuring that such data are adequately protected also fosters public trust in the fact that the data will not be misused.

One of the elements that could be regulated by national data security acts and/or national statistical laws is how data are shared. The challenge is to enable the flow of sensitive data between competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, while ensuring the protection of personal data. This requires the creation of a coherent framework for the protection of personal data backed by strong enforcement. The myth that security and confidentiality considerations preclude the sharing of administrative data for statistical purposes should be avoided. Legal frameworks can facilitate data exchange between different criminal justice institutions while setting clear limits to data access, defining under what conditions data can be shared and restricting the different uses of the data within the criminal justice system and beyond.

Box 7 European Union directive on processing personal data in the criminal justice system⁴⁷

Directive 2016/680 of the European Parliament and the Council of the European Union specifies the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

The directive recognizes that rapid technological developments have brought new challenges for the protection of personal data, with the scale of the collection and sharing of data having increased significantly. The directive is aimed at ensuring that the processing of personal data by law enforcement authorities and the free flow of such data between competent authorities are done in a way that respects individuals' fundamental rights and freedoms, including the right to privacy and data protection. To do so, it sets out principles and rules that competent authorities must follow when handling personal data, including conditions for lawful processing, data transfers, time limits for storage and right of access by the data subject.

Regulations that define who can see what data and at which stage of the proceedings can be integrated into the IT solutions that shape the system. In such a system, as highlighted by the Estonian case study described in the annex to the present guidelines, the different MDAs involved in the criminal justice system can share selected data with authorized stakeholders from their respective information systems. The different information systems automatically exchange information whenever any stakeholder requires information or documentation from another system, provided that they are authorized. Estonia invested substantial resources in developing a digital infrastructure that allows for the secure transfer of information between the different sub-systems of the criminal justice system and parts of the larger e-Government framework. This infrastructure, named X-Road, is an open-source software and ecosystem solution that provides unified and secure data exchange between private and public sector organizations.

Box 8 Commissions on data protection: France and Singapore

France

The Commission on Information Technology and Liberties in France is an independent government agency responsible for ensuring the protection of both public and private personal data contained in computer or paper files.⁴⁸ The commission ensures that information technology is at the service of the citizen and that it does not undermine human identity, human rights, privacy or individual and public liberties. The commission has four primary aims:

- **Inform and protect rights:** The commission responds to requests from individuals and professionals. Anyone who has difficulty exercising their rights can contact the commission and submit a complaint.
- **Support and advise on compliance:** The commission helps private and public organizations comply with the General Data Protection Regulation (GDPR) and provides advisory services.
- **Anticipate and innovate:** As part of its forward-looking activities, the commission monitors emerging issues. In this way, it is helping to create a societal debate on the ethical issues surrounding data.

- **Monitor and sanction:** The commission can monitor organizations and, in the event of non-compliance, may decide to issue formal notices or impose penalties.

Singapore

In Singapore, the Personal Data Protection Commission was established in 2013 to promote and enforce personal data protection and to foster an environment of trust among citizens and businesses.⁴⁹ The commission's aim is to balance the protection of the personal data of individuals with the need of organizations to use the data for legitimate purposes. Among its functions, the commission develops guidelines related to personal data protection for helping organizations understand and comply with the law. The commission also reviews the data protection practices of organizations and issues decisions or directives for compliance where necessary.

3.2.3 Operational guidelines

It is important to ensure alignment among all acts that shape the regulatory framework in order to allow for full legal interoperability. Nonetheless, regulation alone may not meet the objective of the legislator if it is not supported by implementation guidelines, tools and other supporting documents for those who deal with crime and criminal justice data in their daily activities. These elements support legislation at the operational level, providing clear guidelines to those at the forefront of data operations and ensuring that different MDAs within the criminal justice system treat data similarly while respecting the privacy of individuals.

Furthermore, guidelines and handbooks are essential for ensuring that all institutions within the criminal justice system (and beyond) interpret and implement the relevant legislation in the same way. Legislative language can be very complex and, as such, be difficult to interpret for operational staff and the general public. Therefore, it is important to translate complex legislative frameworks into operational manuals that allow staff to collect, produce, disseminate and use statistics in a way that empowers them to do their jobs more effectively. Such operational manuals are also essential in illustrating the added value of statistics to staff members at all levels.

3.2.4 Ensuring regulatory coherence

Regulations can promote the exchange of data and enforce common data standards that enable interoperability, but it is crucial that national statistical law and data security legislation are aligned if this is to be accomplished. The storage and processing of data poses many questions, such as those related to security and privacy, and minimum-security measures can be defined in the regulation, including issues related to the electronic or physical environment that prevents access by unauthorized persons. Providing for the security of information in statistical legislation would enable the NSO to establish IT security systems and procedures to protect against unauthorized access to data, ensure the privacy of users, and assess the risks associated with the release of microdata and information-sharing more effectively.⁵⁰

In many cases, legal frameworks may be outdated, however, which can pose significant challenges to sharing administrative data for statistical purposes. In such circumstances, there may be a need to adopt new legislation to accommodate the needs of the criminal justice statistical system. Yet such modifications are neither easy nor quick to implement and may require the establishment of a long-term vision for the sector.

It should be noted that regulations can also be an obstacle for good data governance as the proliferation of fragmented instruments and uncoordinated efforts can hinder cross-institutional

collaboration and data integration and sharing.⁵¹ In order to ensure a higher level of coherence between regulatory frameworks, strategies should be developed to define the different steps that need to be taken if the different MDAs are to reach the objectives set out in the regulations (such as increased data exchange and interoperability across the systems).

Sample assessment questions on regulation

- Do existing laws, regulations or policies govern the collection, processing and dissemination of crime and criminal justice statistics?
- Are the laws, regulations or policies in line with relevant international standards and guidelines?
- Do the laws, regulations or policies address data privacy and security issues?
- Is an independent oversight body responsible for monitoring the adherence to the regulations and ensuring data quality and integrity?
- How effectively are the regulations enforced and what mechanisms exist for addressing non-compliance?
- Have practical guidelines and handbooks been developed that translate legislative language into operational guidelines?

3.3 Coordination and cooperation

Coordination and cooperation are important for aligning and harmonizing efforts to enhance the value data has for society across the different MDAs within the criminal justice system. Coordination of data producers within the system is important for several reasons:⁵²

- To ensure comparability between the various outputs of the different institutions within the criminal justice system so that they can be meaningfully related to each other using a common vocabulary.
- To avoid duplication of efforts and undue burdening of respondents by collecting survey or additional administrative data when similar data already exist as part of administrative records of other MDAs.
- To ensure that official statistics cover all relevant subject areas for the monitoring of national crime and criminal justice trends and patterns, and for international reporting.
- To enhance the image of official crime and criminal justice statistics through branding and common release practices.
- To ensure that the best possible data are forwarded to international organizations.
- To facilitate the integration of information needs at the subnational level into the national programme in order to reduce the need for additional statistical surveys to be carried out at the subnational level.
- And, ultimately, to make crime prevention more efficient, humane and fair, and increase public safety and security.

Effective coordination among the various institutions in the criminal justice system is crucial for generating reliable and high-quality official statistics. While the constituent bodies of the criminal justice system, including the police, the prosecution service, the courts and the prison system, often fall under the same overarching organization, their inherent characteristics often grant them a significant level of autonomy. Additionally, within each of these institutions, territorial and sectorial decentralization is commonly observed, potentially leading to the existence of numerous independent

organizations within a single entity. Formal or informal collaboration and coordination mechanisms are thus essential for achieving data interoperability and generating relevant statistics.

As noted in the case study on Cameroon in the annex to the present guidelines, the country has faced difficulties in compiling reliable and accurate homicide statistics. In order to overcome issues related to the concepts used, management of data sources and the calculation method, the Cameroon National Institute of Statistics initiated a project in 2023, together with relevant stakeholders such as the national gendarmerie and the police, to raise awareness, train staff and produce an integrated database capable of generating high-quality statistics. While the work involved is largely of a technical nature (defining data collection standards and training staff), improved cooperation and coordination between the stakeholders is proving to be vital in improving the quality of homicide statistics (for further information, refer to the annex of the present guidelines).

3.3.1 Formal mechanisms

Many countries have created formal or semi-formal coordination mechanisms that bring together the different MDAs at regular intervals. The organization of a working group or task force or committee on crime and criminal justice statistics is common in many countries. The terms of reference for each such group may vary across countries, but the common thread is that different MDAs work together with the objective of improving data collection in the criminal justice system. The groups are typically led either by the Ministry of Justice (or equivalent organization) or by the NSO. It is common practice to have two types of working group, one at management level and one at a more operational level. Ideally, such formal mechanisms are clearly specified in the legal framework governing the criminal justice statistical system.

The advantages of formal cooperation mechanisms include the fact that they clearly define roles and responsibilities, promote the use of standardized data formats and definitions, typically have provisions for data security and provide a framework for sustained collaboration and data sharing over the medium to long term. Disadvantages include the fact that formal mechanisms can be overly bureaucratic, time-consuming to negotiate and approve, rigid and difficult to amend, and may limit data sharing to those institutions involved in the mechanism.

In the case of the Republic of Korea, the Information Consultation Body is composed of the second highest-ranking official from each of the institutions participating in the information system (the National Police Agency, the Supreme Prosecutors' Office, the Supreme Court of Korea and the Ministry of Justice), and the Task Force for the Integration of Criminal Justice Information System is composed of operational staff that are seconded from the same institutions.

In Kenya, of the two working groups, one is composed of managers from different institutions within the criminal justice system and beyond (Governance, Peace and Security Working Group) and the other group is composed of staff who code data in different institutions (Governance, Peace and Security Statistics Technical Working Group). While the management group oversees the process and participates in meetings and workshops, the operational group conducts training and capacity-building exercises.

In the Dominican Republic, the National Citizen Security System (SINSEC) is the main mechanism for cooperation and coordination.⁵³ Within this system, the Citizen Security Data Processing and Analysis Center (CADSECI) is the body responsible for collecting, processing and analysing crime data.⁵⁴ The technical unit of the body is made up of 12 institutions, including the Ministry of the Interior and Police (MIP), the National Police (PN), the Attorney General's Office (PGR), the National Institute of Forensic Sciences (INACIF) and the NSO (ONE). The objective is to obtain reliable, timely and representative

information on crimes at the national, regional, provincial and local levels in order to improve understanding of the situational context of crime and monitor the effectiveness of the institutional response. CADSECI also serves as technical support in the design and planning of programmes to MIP, implements monitoring and evaluation frameworks, and coordinates and supervises the local implementation units within the framework of SINSEC.

3.3.2 Informal mechanisms

In the absence of formal coordination mechanisms, countries can establish informal mechanisms between the MDAs that produce administrative data within the criminal justice system. These informal networks typically provide a forum to exchange data, knowledge and expertise between the different stakeholders. They are generally more flexible than formal mechanisms and involve direct communication between staff members, which facilitates the sharing of important information and data. Informal mechanisms can also be more cost-effective than formal ones as they often rely on existing relationships and communication channels. However, staff turnover can strongly affect informal cooperation and lead to fragmentation of the network when key people leave an organization. Moreover, informal networks may not follow standardized procedures, which can lead to variations in data formats and definitions.

Such informal networks exist in many countries. In the United Kingdom, for example, informal networks have proved to be effective for Sustainable Development Goal monitoring. The Sustainable Development Goals unit within the NSO, which oversees the collation of data from different government organizations, maintains informal relations with the different MDAs that provide this network with data and information that are used to populate the Sustainable Development Goal monitoring platform (see Box 9).

Box 9 Informal collaboration in the Open SDG platform in the United Kingdom

The Open SDG platform is an open source, free-to-(re)use platform for managing and publishing data and statistics related to the United Nations Sustainable Development Goals (SDGs).⁵⁵ The platform is built exclusively with open-source libraries and tools and can be hosted and maintained using free services. Open SDG is the result of collaboration between the United Kingdom Office for National Statistics (ONS), the United States Government, the non-profit Center for Open Data Enterprise (CODE) and members of the Open SDG community. It facilitates the gathering, dissemination and tracking of national and local data on the SDG indicators by countries and organizations and improves their access to official statistics and metadata.

Countries can use the platform to create their own SDG data portal. In the United Kingdom, for example, the NSO has built a site based on Open SDG to publish data related to all the SDGs.⁵⁶ Among the different SDGs, the site includes tables related to crime and criminal justice included within SDG 16 (Peace, Justice and Strong Institutions). Through the Open SDG platform, data and metadata are easily available for use and reuse and can be downloaded by anyone in various formats.

Intense coordination and collaboration enable the provision of all such information to the public. The NSO engages in informal collaboration with different MDAs in the United Kingdom in order to gather the necessary data and metadata. When needed, this information is harmonized so as to align with the methodologies and requirements of the different SDG indicators. The collaboration between the NSO and the different MDAs depends greatly on close, informal relationships that are

established with experts in each of the institutions that supply data. Every modification in the data can be tracked and the NSO provides all relevant details in a GitHub space accessible by the source experts.

3.3.3 Memoranda of understanding

If legal frameworks do not provide clear mechanisms, one way to formally improve cooperation is through memoranda of understanding (MoUs) that facilitate collaboration and data exchange. The NSO or the Ministry of Justice is typically the leading organization that initiates the development of MoUs. In order to facilitate the production of official statistics from crime and criminal justice administrative data, it is important that MoUs include provisions regarding data sharing and are as concrete as possible about specific data formats, timing of data sharing, defining roles and responsibilities along with focal points within the different institutions, and operationalizing the different steps involved in exchanging data. In some cases, MoUs also indicate coordination mechanisms between the institutions and either penalties or rewards for collaboration.⁵⁷

MoUs can foster cooperation and clearly define technical details on how data should be shared while respecting privacy and confidentiality. The main disadvantage is that they are usually one-to-one agreements rather than covering all MDAs in a given sector. Therefore, it is recommended to accompany MoUs with coordination mechanisms that bring together the different MDAs of the criminal justice system in order to align policies, standards and technical solutions. In this way, the sector can jointly move towards interoperability (legal, organizational, semantic and technical).

The use of MoUs within the criminal justice system is common in many countries. In Argentina for example, the National Criminal Information System (SNIC) is aimed at providing accurate and timely information on crime in the country and its territorial subunits in order to monitor trends and patterns. SNIC is regulated by law, but the country also relies on MoUs between the Ministry of Security and provincial law enforcement institutions. The latter oversee the collation of data from the local stations at the provincial level. Each province has its own independent data collection and management system and some provinces have independent data dissemination platforms.⁵⁸ MoUs ensure that the data that are sent to the federal level for the production of national-level official crime and criminal justice statistics follow the same standards, and are accompanied by a formal coordination mechanism that brings together all authorities responsible for collecting data at the provincial level. Regular meetings provide an opportunity to share the latest developments and showcase good practices in data management.

Box 10 Elements of a memorandum of understanding

Each context will require different considerations to be taken into account when designing a MoU to facilitate data sharing between stakeholders. However, a number of basic elements are typically part of any formal data sharing agreement. Based on the guidance provided by the Collaborative on Administrative Data, 12 elements are briefly presented for consideration below.⁵⁹ The guidance was developed by the collaborative in response to the need for a practical tool that can help formalize data sharing and exchange between agencies. Data sharing has many benefits, including efficient use of government resources and more comprehensive data sets for statistical production. In most cases, in particular when microdata are shared, the sharing needs to be regulated to help ensure confidentiality and privacy are maintained, giving citizens a clear indication that the data they provide are safely stored and handled.

1. **Parties:** Specifies the parties of the agreement.
2. **Purpose:** Sets out the intention of the agreement in general terms.
3. **Legal basis:** Refers to specific sections of relevant national acts that govern the exchange of data between government entities. If no such legislation exists, it is advisable to carefully review other documentation that may call for improved coordination and cooperation between public entities.
4. **Duration:** Specifies the term for which the data sharing agreement is valid.
5. **Obligations:** Lists the roles and responsibilities of each of the parties.
6. **Incentives:** A MoU can include incentives to foster data exchange (for example, staff training). Note that incentives require the use of resources and should be carefully considered.
7. **Focal points:** Designates focal points within each organization.
8. **Data:** Defines the scope and nature of the data to be shared, including its periodicity, format and the means of transmission.
9. **Quality standards:** Establishes quality standards that the data should comply with.
10. **Confidentiality and security:** Specifies the legal obligations in terms of confidentiality and data security, which is particularly relevant when sensitive microdata are shared.
11. **Amendments:** Specifies the procedure for amending the agreement.
12. **Use of information:** Specifies the use of the information collected from the data holder.

3.3.4 Use of standards⁶⁰

Setting standards that are applicable to all MDAs that collect, produce and disseminate crime and criminal justice data can be valuable for facilitating coordination. An important prerequisite is that the standards are developed in a participatory manner, with the involvement of the NSO, the data producers and, importantly, the data users (both internal and external). This process can be greatly facilitated by adopting standards established at the international level. The international statistical community has developed broad international standards concerning topics such as metadata, data transmission and the statistical business architecture that are generally applicable to all sectors producing official statistics.⁶¹

Content-oriented standards comprise classifications, terminology and definitions to be used across concrete statistical areas, with the purpose of ensuring that the same term is used for one concept across organizations. In some cases, national standard-setting consists mainly of aligning the terminology in the national languages in a way that corresponds best to the terminology used in an international standard. In the field of crime and criminal justice statistics, the International Classification of Crime for Statistical Purposes (ICCS) can be used to increase coordination in the collection, production and dissemination of administrative data. Box 11 provides a brief overview of ICCS and its implementation in Kenya.

Box 11 Implementation of the International Classification of Crime for Statistical Purposes (ICCS) in Kenya

Countries generally use a classification of criminal offences that is based on national criminal law when producing national crime and criminal justice statistics. Consequently, the definition of each offence will vary between countries and data will not be comparable across jurisdictions. ICCS is based on internationally agreed concepts, definitions and principles that enhance the consistency and international comparability of crime statistics and improve analytical capabilities at both the

national and international levels. ICCS provides a framework for the systematic production and comparison of statistical data across different jurisdictions. ICCS can also be used to harmonize data across domestic criminal justice institutions and standardize data from subnational entities that may have different statistical systems or legal frameworks. As such, ICCS can also be used as a standardization tool that enhances coordination at the national level.

In Kenya, the implementation process began with the mapping of ICCS against the national penal code and understanding how the different institutions were classifying their respective data. Two coordination bodies were then created, one composed of senior management and the other of the operational technicians in charge of coding crimes in all the key institutions of the criminal justice system in the country: the police, the prosecution service, the courts and the prison system. The two coordination bodies are tasked with ensuring that the decision-makers in each institution can share their ideas and work at the strategic level while those with a more technical role learn how to implement the new classification practically.

Operational actors were trained in the use of ICCS and its importance for improving crime and criminal justice statistics. The number of indicators reported nationally and internationally increased as a result of the process, as did the quality and comparability of statistics by aligning the coding procedures across different institutions. Although the implementation process is still ongoing, it has already increased coordination and cooperation among the different institutions, both at the senior management and operational levels.

Sample assessment questions on coordination and cooperation

- Are formal structures or committees in place to facilitate coordination among different MDAs involved in the collection, production and dissemination of crime and criminal justice statistics?
- Do these structures have representation from key stakeholders, such as the police, the prosecution service, the courts, the prison system and statistical agencies?
- Have mechanisms that simultaneously ensure data privacy and security been established for sharing data and information among the stakeholders?
- Are mechanisms in place to resolve conflicts or disputes that may arise during the exchange of data?
- Are formal or informal networks in place to facilitate knowledge exchange, encourage the sharing of best practices and promote collaboration in the field of crime and criminal justice statistics?

3.4 Data architecture

A common obstacle to data interoperability is the lack of agreement on how to represent data and metadata from different sources in a consistent way. Different organizations, or even different departments within a single organization, often decide how to structure their data and metadata assets on a case-by-case basis, adopting models of data collection, storage and exchange that respond only to their immediate operational needs, without considering interoperability and scalability needs across the broader data ecosystems of which they form part.⁶²

The term “data ecosystem” refers to the entire network of data collectors, data producers, data analysts and other data users that directly or indirectly collect, process, disseminate, analyse and/or otherwise consume data and associated services within a specified country, region or sector.⁶³

Such data models become silos because they focus almost exclusively on recording and updating information related to their day-to-day activities, prioritizing the integrity and accuracy of that information over the analytical needs of external users and the need to integrate their data with other sources of information. While this is partly an issue of data stewardship and coordination, it also reflects the lack of a coordinated focus on user needs at the technical and operational levels.

A way to overcome this issue is to develop a common statistical data architecture for the criminal justice system. A data architecture is composed of models, policies, rules and standards that govern which data are collected, how they are stored, processed, integrated and used in data systems. A well-designed data architecture can result in improved timeliness and more disaggregated statistics at higher frequencies. The data architecture must support quality, security and confidentiality and ensure access to data at any time in the data life cycle. The design of a data architecture includes policies and standards but can also include specific IT solutions that are used in organizations. This section highlights some key elements to consider when designing the data architecture of an organization.

A **data architecture** is composed of models, policies, rules and standards that govern which data are collected, how they are acquired, stored, processed, integrated and used in data systems.⁶⁴

It should be noted that while all countries have access to computers, digital capacities vary considerably from country to country. Even when digital resources are available in a country, they may not be widely available within the criminal justice system. Despite the great potential of automated data processing, many countries still rely on manual clerical operations. The introduction of major administrative computerized systems into government agencies, such as those involved in crime and justice operations and statistics, is a complex and costly process that may take several years to accomplish and requires a level of agreement between the different institutions that can take an equally long time to achieve.

3.4.1 Data standardization

For any data architecture, standards, classifications and vocabularies are crucial for ensuring semantic interoperability. Standard vocabularies and classifications help improve consistency in the description of data and metadata elements within a data set at the point of collection by providing a defined list of terms to systematically categorize or label information. This allows data producers to express the meaning of data without ambiguities and enables users to find and link related pieces of information, from the unit record level to the data set level, across different information systems or databases.⁶⁵

For more information on the standardized exchange of data and metadata, see the Statistical Data and Metadata eXchange (<https://sdmx.org/>). SDMX is an ISO standard designed to describe statistical data and metadata, normalize their exchange and improve the efficiency of sharing data across statistical and similar organizations. The exchange provides an integrated approach to facilitating statistical data and metadata exchange, enabling interoperable implementations within and between systems concerned with the exchange, reporting and dissemination of statistical data and their related meta-information. SDMX consists of technical standards, guidelines and tools that can support the harmonization and standardization of statistical data and metadata.

Box 12 Essentials of metadata

In general terms, metadata are data that define and describe other data. More specifically, they are data and other documentation that describe statistical data and statistical processes in a standardized way by providing information on data sources, methods, definitions, classifications and data quality. The use and management of metadata are essential for ensuring data quality and promoting efficient data exchange, a shared understanding of the data and data comparability. This is further underlined by principle 3 of the United Nations Fundamental Principles of Official Statistics, which states that, to facilitate a correct interpretation of the data, statistical agencies are to present information according to scientific standards on the sources, methods and procedures of the statistics.⁶⁶

A distinction can be made between structural and reference metadata. Structural metadata consist of identifiers and descriptors essential for organizing and processing a statistical data set, such as titles, variable names, descriptions, and more. Reference metadata, on the other hand, describe the statistical concepts and methodologies (for example, sampling, collecting methods, cleaning process) used for the collection and production of data and provide information on data quality (for example, timeliness and accuracy).

An example of structural metadata is the use of the variable “charge type” both by the police and the prosecution service. If both data providers collect data for this variable either by ICCS category or the unified national classification, this will facilitate the tracking of the number of charges registered by the police that lead to prosecution, which further enables the interoperability of (aggregated) data sets from different data providers. If the individual data providers utilize different methodologies for data collection and data aggregation, however, the data will not be directly comparable despite utilizing the same data structure, since the reference metadata differ. For example, the police could report “input statistics” that include all cases reported to the police or “output statistics” that only include confirmed criminal cases. Depending on the selected method of data collection, the reported numbers could differ substantially.

It is therefore essential to have a national consensus on the statistical classifications, concepts and methodologies applied – in line with international definitions, standards and norms whenever applicable – when collecting, producing and disseminating data. Always documenting and publishing this information as the official reference metadata is recommended. Only then can data comparability between different data providers and criminal justice institutions be guaranteed.

Several international organizations have drawn up guidelines and standards for documenting and exchanging metadata. Examples include:

- **Data Documentation Initiative (DDI)** is a standard for documenting statistical data sets to facilitate re-use. For more information, see <https://ddialliance.org/>.

- **ISO/IEC 11179** documents the standardization and registration of metadata to make data understandable and shareable.
- **Statistical Data and Metadata eXchange (SDMX)** is a set of technical standards to facilitate the exchange of data and metadata between organizations and computer systems. For more information, see <https://sdmx.org/>.
- **ISO 19115** defines the schema required for describing geographic information and services by means of metadata.

Semantic interoperability across the different institutions of the criminal justice system is thus essential for enabling the meaningful sharing of data and the production of comparable statistics to monitor crime and criminal justice at different territorial levels and across the different stages of the criminal justice system. To achieve this, it is important to assess whether the different institutions are using consistent and harmonized standards and classifications when collecting, storing and sharing the data.

Classifications

Classifications group and organize information meaningfully and systematically into a standard format. The preparation of a classification means creating an exhaustive and structured set of mutually exclusive and well-described categories, often presented as a hierarchy reflected by the numeric or alphabetical codes assigned to them.⁶⁷ As noted in the previous section, for the classification of criminal offences, ICCS is the internationally endorsed standard. Implementing ICCS typically requires a mapping between the national offence classification (for example, the penal code) and ICCS. The outcome of this exercise is the creation of a correspondence table that serves as the translation key between national offence data produced by the different institutions of the criminal justice system and ICCS-compliant criminal offence data that are comparable at the national, regional and global levels (for more information on ICCS implementation or technical assistance with the implementation process, contact UNODC at unodc-iccs@un.org).

An example is SDSKI (Satu Data Statistik Kriminal Indonesia (Indonesia One Crime Statistics Data)), which was initiated by BPS-Statistics Indonesia in 2021. SDSKI is aimed at enhancing the governance of crime data in Indonesia and improving the production of quality crime statistics. BPS has proposed a framework that mainly consists of information about data sources, classifications, principles, data utilization and expected outputs of SDSKI. Based on the framework, SDSKI will utilize both crime-related administrative data and survey-based data as its primary data sources, which will be standardized using ICCS to enhance interoperability and ensure international comparability. In addition, the data will be required to meet the Indonesia One Data Principles (for more details, see the case study in the annex to the present guidelines).

Frameworks

The other three guidelines in this series, which respectively focus on the production of statistical data by the police, the prosecution service and courts, and the prison system, also provide an avenue for further standardizing data collection processes. The guidelines offer concrete recommendations on the kind of data to collect in order to gain deeper insights into the workings of the criminal justice system and can be used to construct indicators that are deemed relevant for the national context. Partially or fully aligning the national data collection process with the guidelines and ensuring that those institutions are systematically collecting such data in a harmonized manner greatly facilitates data interoperability and the means of linking different data sets both within and across institutions using unique identifiers. In this manner, the value of administrative data is enhanced and institutions

can consider linking and exchanging microdata, within the limits set by regulation, for in-depth analysis rather than limiting the exchange to aggregated statistics for reporting purposes.

Unique identifiers

The use of unique identifiers plays a pivotal role in the data architecture as it promotes interoperability by allowing individual records to be accurately linked across data sets (i.e., data linkage). Unique identifiers are alphanumeric codes or numbers assigned to individuals, cases or entities within a system. As implied by the term “unique”, no two records should have the same identifier. When implementing unique identifiers within an institution, it is crucial to develop a standardized format with fixed naming conventions and implement robust validation checks to prevent the creation of invalid or duplicate identifiers. Clear guidance should also be in place regarding the management and retirement of unique identifiers.

When considering the broader criminal justice system, unique identifiers can be used to exchange data between the police, the prosecution service, the courts, the prison system and other relevant stakeholders. Such an interoperable system of administrative data can enable the tracking of individuals across the system and provide deeper insights into the workings of the criminal justice system. For example, it would become possible to track a specific offender in a case recorded by the police, better understand the decision to prosecute, and document information on the case duration and sentencing outcomes (which could be particularly relevant for research into recidivism). Such bespoke analyses could support decision-makers by more precisely highlighting what works and where programmes are producing the intended criminal justice outcomes – potentially improving effectiveness and saving costs simultaneously.

Data dictionaries

Lastly, a key step towards further standardization is the development of a data dictionary that specifies the basic components of the administrative data that can be used both within and across MDAs. A data dictionary is essentially a repository of metadata that provides a comprehensive description of the administrative data under review so that analysts can understand the data better. Some of the basic components to include in a data dictionary are listed in Table 2.

Table 2 **Basic data dictionary components**

Component	Description
Variable name	The name of the data element as it appears in the data set.
Variable description	A description of the data element, its purpose and context.
Data type	The type of data that can be stored in the data element, such as text, date or numeric.
Allowed values	Define the range of accepted values for the data element.
Source	Describes the source of the data element.
Validation rules	Describe any rules that need to be applied to validate the data element.

Box 13 Crime reporting in the United States

Provided by the Federal Bureau of Investigation (FBI) of the United States

In the United States, criminal offence data is collected through the Uniform Crime Reporting (UCR) programme in order to generate reliable statistics for use in law enforcement and provide information for researchers, the media and the public. Managed by the Federal Bureau of Investigation (FBI), the programme has been providing crime statistics since the 1930s.

Since 1 January 2021, the way data are reported to the programme has changed significantly. Data are no longer reported through the Summary Reporting System (SRS) – an aggregate monthly tally of crimes – but through the National Incident-Based Reporting System (NIBRS), which was developed in the 1980s. The most significant difference between NIBRS and the SRS system is the degree of detail in reporting. Through SRS, law enforcement agencies tallied the monthly counts of the number of crimes known to law enforcement for 10 offence categories based on the most serious offence reported for each crime incident. Through NIBRS, law enforcement agencies report data on each offence (up to 10 per incident) and arrest within 28 offence categories made up of 71 specific crimes called Group A offences. For each of the Group A offences that comes to its attention, law enforcement collects administrative, offence, property, victim, offender and arrestee information.⁶⁸

To ensure that these data are uniformly reported, the FBI provides contributing law enforcement agencies with a handbook explaining how to classify and score offences and provides uniform crime offence definitions. Acknowledging that offence definitions may vary from state to state, the FBI cautions agencies not to report offences according to local or state statutes but to the federal guidelines provided in the handbook. The accuracy of the statistics depends primarily on the adherence of each contributor to the established standards of reporting.

Participation in the FBI UCR programme is voluntary for state and local agencies. The FBI does not have the authority to mandate state and local agencies to report data to the UCR programme. Federal agencies, by contrast, have a statutory mandate to report data to the UCR programme.

By design, NIBRS data are generated as a by-product of a law enforcement agency's records management system. Therefore, an agency builds its system to suit its own individual needs, including all the information required for administration and operation, then only forwards the data required by NIBRS to the FBI UCR programme.

Throughout the transition from SRS to NIBRS, law enforcement agencies identified four main challenges impeding their move to the new reporting standard:

- **Funding:** Agencies reported that funding was not available to procure a records management system capable of capturing and reporting NIBRS data. Instead, funding was prioritized to meet other policing needs such as police equipment.
- **Staff shortages:** Agencies reported staff shortages that hindered the collection and submission of data.
- **Training:** Agencies reported that training insufficiencies resulted in delays in NIBRS implementation and reporting. This included personnel who were untrained in the fundamentals of NIBRS, such as correctly capturing and reporting NIBRS data within the records management system.

- **Public perception:** Agencies expressed concerns that there would be a public perception that crime significantly increased with the switch to NIBRS reporting. NIBRS can capture multiple criminal offences that occur during a single incident, unlike the older system, which only allowed for the most serious offence to be collected. As a result, an increase in offences was expected when agencies transitioned to NIBRS. The FBI addressed these concerns with a study that analysed the effects of NIBRS reporting on offence levels and showed only a nominal increase in crime reported via NIBRS.⁶⁹

To increase participation, the UCR programme partnered with the Bureau of Justice Statistics on the National Crime Statistics Exchange, working with advocacy groups to emphasize the importance of NIBRS data. In addition, the UCR programme has made resources available to help agencies address the cost of transitioning to the new system.

3.4.2 Statistical processes⁷⁰

Beyond sector-specific standards such as those defined in ICCS, many cross-sectoral models and standards developed by the international statistical community exist to support statistical production processes such as GAMS0, GSBPM and GSIM (see Table 3). As stated in *The Handbook on Management and Organization of National Statistical Systems*, standards are enablers of modernization through which statistical systems can be modernized and “industrialized”, enabling internationally comparable statistics to be produced more efficiently. Standards facilitate the sharing of data and technology in the development of internationally shared solutions and generate economies of scale. Standards provide benefits in the efficiency and quality of and trust in statistics, increase collaboration by providing a common language and foster innovation as they offer a solid basis for development.

Table 3 offers a brief description of selected frameworks. It is recommended to work closely with other institutions in the criminal justice system and the NSO when applying (parts of) these frameworks in order to improve crime and criminal justice statistical production processes.

Table 3 **Selected international models and standards for managing statistical processes**

Model	Description
Generic Activity Model for Statistical Organizations (GAMS0)	<p>The Generic Activity Model for Statistical Organizations (GAMS0) covers activities at the highest level of the statistical organization. It describes and defines the activities that take place within a typical organization that produces official statistics. The GAMS0 standard covers four broad areas of activity: production, strategy and leadership, capability management, and corporate support. As with related international standards, GAMS0 contributes towards creating a common vocabulary for these activities and a framework to support international collaboration activities. GAMS0 includes the management of the physical security of data and shared data infrastructures.</p> <p>For more information, refer to: https://unece.org/statistics/modernstats/gams0</p>

Generic Statistical Business Process Model (GSBPM)

The Generic Statistical Business Process Model (GSBPM) is a statistical model that provides a standard terminology for describing the different steps involved in the production of official statistics. GSBPM is applicable to all activities undertaken by statistical organizations that lead to statistical outputs. GSBPM covers the processes that cover specifying needs, building products, data collection, data processing, analysis, dissemination and evaluation.

For more information, refer to:

<https://unece.org/statistics/modernstats/gsbpm>

Generic Statistical Information Model (GSIM)

The Generic Statistical Information Model (GSIM) describes the information objects and flows within a statistical business process. GSIM is complementary to GSBPM and the framework enables descriptions of the definition, management and use of data and metadata throughout the statistical information process.

For more information, please refer to:

<https://unece.org/statistics/modernstats/gsim>

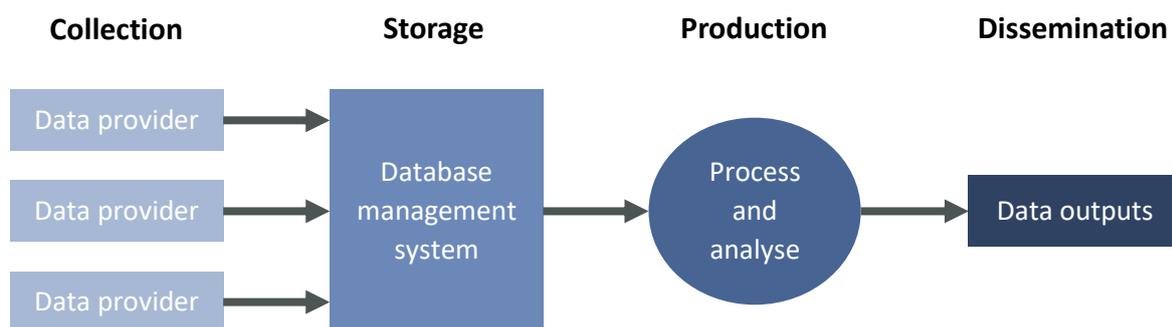
3.4.3 Managing the data life cycle

Beyond standards, a data architecture also involves the management of the data flows that support the statistical production process throughout the data life cycle. Vital elements of any data architecture are data sources and technical solutions for storing, processing, transforming, analysing and disseminating data and statistics. The adopted technological solutions (for example, cloud-based services for data hosting and analysis, data warehouses, data lakes, dashboards or application programming interfaces (APIs)) should support the policies, rules and standards defined within the criminal justice system and the NSS. Generally, countries do not create a data architecture from scratch but opt instead for re-engineering legacy data management practices and processes or adapting legacy data infrastructures.

The IT infrastructure will largely determine the degree of technical interoperability of administrative data and metadata within the criminal justice statistical system and its exchange, use and reuse. Technical interoperability is defined by different elements such as the basic structure of data sets, the format in which the data sets are made available and accessible and the availability of platforms for data exchange or data linkage. Many factors affect the type of IT infrastructure that is utilized, such as the distribution of responsibilities across different levels of government and institutions and the capacity and available resources of the different institutions. For instance, local-level police stations or courts may not have access to adequate digital tools, in particular those in remote rural areas. Each country has its own context that determines which IT solutions are currently employed and what kind of changes are possible going forward.

The crucial point when designing a data architecture is to be able to share administrative data and metadata across the different institutions of the criminal justice system and facilitate the production of high-quality official statistics on crime and criminal justice. A wide variety of different solutions have been adopted around the world, from highly complex database systems that require sources to be interoperable to more basic solutions such as simple spreadsheet-based solutions. Four key elements are identified here within the data life cycle: collection, storage, production and dissemination.

Figure 5 **Basic data flow diagram**



Source: UNODC.

Box 14 Improving the flow of crime data in Lebanon

Provided by the Internal Security Forces of Lebanon

By virtue of Law No. 17, dated 6/9/1990, the Internal Security Forces (ISF) of Lebanon are tasked with detecting and reporting crimes, collecting evidence and discovering, tracing, arresting and handing perpetrators over to competent judicial authorities. The ISF document their procedures and actions through reports under the supervision of the competent judiciary, which include information about the type of offence committed, the perpetrator, the victim, the modus operandi, the place and date of occurrence, and more. Analysing the content of these reports helps create a picture of the current crime situation in the country and the trends in and patterns of crime, which in turns helps formulate policy.

A copy of every judicial report drafted is referred to the Archives and Documents Bureau at the General Criminal Investigation Division of the Judicial Police Unit within ISF. Upon receipt of a report, the data are entered into an electronic system; however, experience has shown that the data do not always accurately express the content of the report and do not reflect all its components. To avoid errors and increase the accuracy of the data, an IT program was developed to collect data electronically after a report is drafted. ISF are currently working on implementing the software in their relevant units and connecting it directly to the Archives and Documents Bureau.

The main obstacle hampering implementation is ensuring a direct connection between the different ISF units and the IT network. ISF have started a comprehensive automation project called the Information Technology Automation Project (ITAP) to facilitate the effective analysis of data obtained from the reports, which will automate all the components of a report and link the different systems. ITAP is a centralized integration platform and reengineering effort that eliminates paper-based processes while providing a modern, simple and efficient computer-based workflow, reducing cost and curbing corruption. The project includes an application that allows the management of cases and enables users to enquire, manage data, conduct investigations, analyse crimes and submit reports. Ultimately, ITAP is aimed at improving the ability of ISF to fight crime, solve cases and interact with citizens.

Data collection

Any data collection produces a data set, which is a collection of data or information that generally has a predetermined structure (with a standardized format normally tabulated with rows and columns, much like a standard Excel spreadsheet). In the case of tabular microdata, each column of a table represents a particular variable (for example, the age of a victim) and each row corresponds to a particular record in the data set (for example, a specific court case with a unique identifier). Administrative data collections are generally stored in structured data sets that can have different formats, such as XML, CSV, SQL, XLSX or JSON, depending on the system in place in the relevant institution.

In this phase, as noted in the above section on data standardization, it is vital to determine which data are needed and according to what classification or standard they should be collected. The data collection should be aimed at effectively reducing collection costs, improving the availability of high-quality, interoperable data and following the principle of “collect once, use many times” so as to avoid the duplication of data collection efforts. This principle is at the core of India’s Interoperable Criminal Justice System (ICJS) project, for example, which is being implemented by the National Crime Records Bureau (NCRB) in association with the National Informatics Centre (NIC) during the period 2022/23 to 2025/26.⁷¹ ICJS is a national platform that will enable the seamless transfer of data among the police, courts, public prosecutors, prisons and forensic laboratories. The system will be made available through a dedicated and secure cloud-based infrastructure.

The mechanism by which administrative data and metadata are to be transferred should be clearly specified. Mechanisms differ between countries and even between different administrative authorities within a country, largely because of the level of maturity of the IT-system of the different data providers and the institution responsible for collecting official crime and criminal justice statistics (whether this is the NSO or another organization). The data providers may send data files to the responsible institution (electronically or hard copy) or the institution may extract the data directly from the administrative source database. As data providers further develop their IT systems and digitalize their processes, it will become easier to share and exchange data from administrative sources.

The transmission of data between institutions can benefit from the development of common standards and protocols applied across the criminal justice system or align with existing national standards. Providers of administrative data related to crime and criminal justice may also choose to align with existing international statistical standards for data and metadata exchange (for example, SDMX).

It can also be worthwhile to consider designing and implementing an extract, transform, load (ETL) pipeline.⁷² An ETL is a data integration process that combines data from multiple data sources into a single, consistent data store that is loaded into a data warehouse or other target system. Relevant data are extracted from the source database(s) and loaded into a staging area. Next, the data are transformed, which involves cleaning the data so they are better suited for analysis and putting them into a common format so they can be stored in a target system. In the final stage, the data are loaded into the target system where they can subsequently be used for analytical purposes. ETL is just one method as there are other data integration methods to facilitate data integration workflows, such as Change Data Capture (CDC), data virtualization and Stream Data Integration (SDI). The method that is best for a given organization depends on the availability of resources, data volumes and required levels of flexibility.

Data storage

Individual data sets can be stored either locally or in the cloud and can be linked through database management systems (DBMS) using unique identifiers. DBMS are used for creating, storing and connecting structured data and rapidly retrieving the data via a query language. Rules can be applied for data security, connecting data and enforcing referential integrity. This is vital for ensuring data quality, which cannot be guaranteed using unmanaged data stores such as Excel. Some of the commonly used commercial DBMS are Microsoft Access, Oracle Database and IBM Db2. Open-source software solutions are also available, including MySQL, MariaDB, MongoDB and PostgreSQL.

A database management system (DBMS) is a collection of programmes that manage the database structure and control access to data stored in a database.⁷³

In Estonia, for instance, the e-File system serves as a central information system where all relevant information and documents related to criminal cases are accessible to authorized parties, such as the police, prosecutors, judges and lawyers. It provides a secure and accessible platform to access case files, submit documents and track the progress of criminal proceedings. In essence, it is a system that enables the simultaneous exchange of information between different parties and databases. The system connects the data from different stakeholders through the X-Road solution, a secure and decentralized data exchange platform that facilitates seamless and reliable communication between various government and private sector organizations (Estonia's X-Road environment is known as "X-tee"). X-Road serves as the backbone of Estonia's digital infrastructure and underpins its successful e-Government initiatives (for further information, see the case study in the annex to the present guidelines).

In the Republic of Korea, KICS is the system connecting the Korean National Police, the Supreme Prosecutor's Office, the Supreme Court of Korea and the Ministry of Justice in order to enable them to perform their work through a standardized information system. KICS is an integrated IT system that facilitates the sharing of data on criminal cases between the agencies and with citizens. For information sharing and collaboration, the system enables authorized users from different criminal justice agencies to share information securely. It allows for the exchange of data, documents and messages related to investigations, court proceedings and corrections, promoting coordination and collaboration among agencies. At the criminal justice portal (www.kics.go.kr), the general public can electronically enquire about the progress of a case and about court records at any time and can electronically apply for civil services.

In both Estonia and the Republic of Korea, the system connects independent databases from the various institutions of the criminal justice system and allows for the seamless exchange of administrative data. In countries with more complex institutional settings that have a significant number of independent institutions at subnational level, each potentially with their own case management systems and different unique identifiers, it is substantially more challenging to achieve interoperability and connect the different systems. This is the case in the United States, for instance, where other solutions for collecting and collating information at aggregate levels (local, state or national) are adopted.

In the United States, approximately 18,000 independent law enforcement agencies (local, counties, special purpose, state and federal) collect their own data, each of which can have its own case management system and IT solutions. This degree of complexity poses a challenge to the achievement of full technical interoperability. For crime reporting under the National Incident-Based Reporting System (NIBRS), microdata are directly obtained from agencies or states. The United States Bureau of

Justice Statistics collects a broad range of additional information from the criminal justice system using survey instruments through programmes such as the Law Enforcement Core Statistics (LECS) programme and the National Corrections Reporting Programme (NCRP).

A key challenge in the United States is that state and local agencies are not obliged by federal law to share the data, but do so on a voluntary basis. Although this further complicates the production of crime and criminal justice statistics at the national level, it should be noted that voluntary reporting has certain advantages, such as reducing the cost of collection and potentially promoting the accuracy of the reported data⁷⁴ (for further information on crime reporting through the National Incident-Based Reporting System (NIBRS) in the United States, see Box 13).

Argentina stands somewhere in the middle of the above extremes of technical interoperability. The country's provinces are primarily responsible for the collection of data from law enforcement institutions. Although each province has developed its own case management system based on common semantic interoperability in order to achieve this, there is no technical interoperability at the national level between the different provincial systems. Instead, a separate federal system was created into which all provinces manually input the data they collect through their independent systems. Moreover, at the provincial level, the collection of administrative data is not handled by a digital system that connects local stations, but rather by a system based on summaries of each local case that are subsequently entered into the provincial digital case-management system.

Box 15 Modernizing IT infrastructure: Colombia and Senegal

The Data For Now initiative (<https://unstats.un.org/UNSDWebsite/capacity-development/data-for-now/>) is aimed at developing the capacity of countries to deliver the information needed by local and national policy and decision-makers for designing effective development strategies and policy programmes to achieve the 2030 Agenda for Sustainable Development and/or national goals that countries have identified as a priority. To this end, the initiative supports members of National Statistical Systems in participating countries to leverage innovative sources, technologies and methods for the streamlined production and dissemination of high-quality, more timely and disaggregated data. In this context, the initiative also supports effective collaboration between members of the National Statistical System, local, national and global partners from intergovernmental organizations, academia, civil society and the private sector.

Colombia

In Colombia, the initiative supported the National Statistical Office (DANE) in its efforts to modernize its IT architecture by providing guidance on architectural decisions through the recruitment of an IT expert and training on data engineering skills aimed at strengthening internal capabilities to maintain and operate the new infrastructure. One of the keys of the project was to ensure collaboration between the technical experts involved and the statistical production team. This ensured that existing gaps in data integration, storage and processing capabilities for statistical production were identified and provided a starting point to identify the main data integration and processing challenges.

One of the main challenges of the process was to develop new workflows and adapt existing statistical business processes in order to make optimal use of the new IT infrastructure. To address this challenge, DANE adopted an enhanced technological infrastructure and a robust Apache Hadoop ecosystem. After implementation, some processes take 90 per cent less time than they

used to and others are practically instantaneous, highlighting the substantial gains that can be obtained by modernizing the IT architecture that supports the statistical production process.

Senegal

In Senegal, the initiative prioritized a cross-cutting activity to establish and modernize its IT architecture. To achieve this, a series of consultations and meetings were held between the National Statistical Office (ANSD) and the Data for Now team in early 2021 to review the existing IT architecture. Based on the review, a practical list of solutions that fit the need of ANSD was identified and the discussions guided ANSD to not only modernize its IT architecture but also support its existing resources by automating some workflows.

Recommendations included components from the data lake architecture concept, which focuses on strengthening the overall data storage, processing, analysis and dissemination process. The recommendations also focused on sustainability along with increased reliability, scalability, flexibility and speed by automating data pipelines. After conducting an in-depth analysis of the technological infrastructure, the ANSD team agreed to implement the proposed data lake architecture through a pilot project on COVID-19 data. Some of the newly introduced tools included Apache NiFi for data ingestion, MinIO as a storage platform, Jupiter notebook/hub for data analysis/processing and Dagster for workflow automation and orchestration. Although an ongoing process, the pilot was a step forward and the activities will further support ANSD as it adopts the modern IT architecture and builds in-house capacity to manage and use these tools.

Another key consideration for data storage is deciding how long to store the data.⁷⁵ Older data may no longer be fit for purpose due, for example, to a change in methodology, or may be subject to legal and regulatory requirements that dictate a maximum retention period. The duration of data storage also depends on the relevance of the data to fulfil a specific function or purpose that will differ between stakeholders. If the data have outlived their shelf life, a further consideration is whether to archive or dispose of the data. When archived, data are moved to a separate storage medium or facility intended for the long-term retention of historical data, which can also include the removal of personally identifiable information. This ensures that historical data are still available for future analyses that can reveal new insights while safeguarding privacy rights. The destruction of data in line with relevant laws and regulations requires additional due diligence, as the action cannot be undone.

Data storage is also related to data sovereignty. A relatively new term and for which there is no single agreed definition to date, data sovereignty generally refers to control and ownership of data and its related infrastructure.⁷⁶ This can be particularly relevant when data are stored in the cloud and questions arise about storage, the jurisdiction under which they fall and how confidentiality will be ensured. For example, there may be a legal requirement to store certain data within national borders or there may be limitations on cross-border data transfers. Data sovereignty can also be interpreted as the right of the user to have control over their data. In this context, indigenous data sovereignty refers to the right of indigenous peoples to govern the collection, ownership and use of data about their peoples, lands and resources. An example is the First Nations Information Governance Centre in Canada, an independent non-profit operating with a special mandate from the Assembly of First Nations' Chiefs-in-Assembly (Resolution #48, December 2009) working to assert data sovereignty and support the development of information governance at the community level.⁷⁷

Data production

Almost every producer of official statistics uses one or more commercial or open-source software package in the production of statistical data, including for data processing (for example, data cleaning or validation) and analysis. Table 4 lists some of the more popular data analysis tools available today, without recommending any in particular. Each of the software packages has its strengths and user base, and the choice among them often depends on the specific needs, familiarity with the software and the type of analyses required. The selection of a data analysis tool is often path dependent as a particular tool may already be in use, making it difficult and time consuming to change existing processes and procedures. Whatever package is ultimately used, it is vital to document all the steps and procedures involved in conducting specific analyses to serve as a record and ensure that results can be reproduced and replicated in the future, even when using different analysis tools.

Table 4 Selected data analysis tools

Tool	Description
Python	<p>Python is a free, open-source programming language that is widely used in scientific and numeric computing. It can be extended with packages such as pandas, SciPy and NumPy that can help the user with data manipulation, cleaning and analysis.</p> <p>For more information, refer to: https://www.python.org/</p>
R	<p>R is a free, open-source language and software environment for data manipulation, statistical computing and graphical display and is highly extensible. It provides a wide range of tools and packages, such as tidyverse, for handling data, performing statistical analysis and generating visualizations.</p> <p>For more information, refer to: https://www.r-project.org/</p>
SAS	<p>SAS is a software suite used for statistical analysis, data management and predictive modeling. It was initially developed for use in research and academia but has been widely adopted in various industries for data analysis and reporting.</p> <p>For more information, refer to: https://www.sas.com/</p>

SPSS	<p>SPSS is a software package designed for statistical analysis and data management. It has become popular across various disciplines due to its user-friendly interface and versatile statistical capabilities.</p> <p>For more information, refer to: https://www.ibm.com/products/spss-statistics</p> <p>An open-source alternative is PSPP, which features similar functionality free of charge.</p> <p>For more information, refer to: https://www.gnu.org/software/pspp/</p>
SQL	<p>Structured Query Language (SQL) is a programming language for storing, updating, removing, searching, retrieving and processing information in large databases. SQL integrates well with different programming languages and is particularly well suited for dealing with structured databases.</p>
Stata	<p>Stata is an integrated software package that allows for data manipulation, visualization, statistics and automated reporting. It is commonly employed in research, academia and the social sciences.</p> <p>For more information, refer to: https://www.stata.com/</p>

Modern statistical software packages have made highly sophisticated techniques of analysis more accessible, but if there is no understanding of the underlying assumptions of those techniques and there is no guarantee that the design of the data series is consistent with the applied techniques, personnel untrained in statistics and analytics could draw incorrect or biased conclusions. Moreover, if the language used to communicate statistics is not in line with scientific principles and user-friendly, correct interpretation of the data may be hindered and trust in official statistics could be damaged.

It is therefore highly recommended to contract dedicated staff capable of conducting and explaining such advanced types of analysis, that is staff that can select, use and explain appropriate statistical techniques while understanding their inherent assumptions, strengths and limitations. If the requisite resources are unavailable, it is recommended to invest in data partnerships with third parties, such as the NSO, that provide data-related services ranging from technical advice and capacity-building to comprehensive data analysis facilitated through data-sharing agreements.

Data dissemination

Disseminating and utilizing data to analyse trends and answer pressing policy questions is a tangible benefit of the production of statistics. In addition, it is beneficial to disseminate metadata to help users understand the context in which the data were collected and processed, including details of revisions and corrections to the data and the contact details of the responsible statistician. This is useful for improving the usability of data and communicating data quality to data users. One of the key factors in overcoming challenges in data collection is to ensure that data providers see the utility of sharing their data at the (inter)national level. This allows them to monitor local trends over time or compare data with other agencies or jurisdictions for the first time as many may not have the time or resources to devote to data collection, production and dissemination. In this regard, the production and dissemination of data is one of the keys to garnering support from data providers. This is related to

the dissemination of data, which allows for the use and reuse of crime and criminal justice data by different stakeholders.

There are many ways to disseminate statistics on crime and criminal justice. This typically involves a press release, the presentation of general results and the release of a set of predefined data tables according to a predetermined release calendar that is communicated to the public well in advance. As a next step, agencies can consider releasing (part of) the underlying anonymized data and metadata. Countries with more advanced reporting systems typically allow aggregated data to be downloaded in user-friendly open formats, enabling the user to further analyse and process the data, fostering its reuse for research and other purposes. Data visualization tools, GIS solutions and APIs are other frequently used options for disseminating data and making results more actionable.

The NSO is not always the sole institution that disseminates data. In the case of Argentina, for example, the Ministry of Security hosts the National Criminal Information System, which provides a dashboard where the user can modify selection criteria to produce the desired tables and graphs.⁷⁸ The aggregated data can be download in various formats (Excel, CSV, Stata or SPSS) for further processing in statistical packages. In the United States, although the Bureau of Justice Statistics is the main institution for disseminating criminal justice data,⁷⁹ the FBI hosts the Crime Data Explorer.⁸⁰ This tool allows the user to manipulate interactive graphs and tables at either the federal or state level. The data available include information collected through NIBRS (for further details, see Box 13), as well as other data such as on hate crimes, the number of law enforcement employees and data on use-of-force incidents. The different summary data sets can be download for further analysis.

In other countries, the NSO plays an important role in disseminating crime and criminal justice data. In Norway, for example, the police collect the data, while the NSO is mainly responsible for dissemination of the data. The police have an IT system in place that allows the institution to disseminate annual reports on crime that are shared with the NSO, which produces different tables and reports based on the data that can be access by citizens.⁸¹ The Norwegian system allows the user to filter the data in a user-friendly manner and manipulate the output in order to customize it to their needs and download the results. One highlight is the quality of the associated metadata, which include information on the structure and quality of the data. In the case of Mexico, the role of the NSO in the dissemination of crime and criminal justice statistics is highlighted in Box 16.

Box 16 Mexico: National Census of State Law Enforcement (CNIJE)⁸²

The purpose of the National Census of State Law Enforcement (Censo Nacional de Impartición de Justicia Estatal) conducted by the NSO of Mexico, the National Institute of Statistics and Geography (INEGI), is to generate statistical and geographical information on the management and performance of the judicial branch in each state of the country, specifically in the functions of government, administration of justice, juvenile justice, alternative justice and/or alternative dispute resolution mechanisms and expert services, so that this information can be linked to governmental activities in the process of designing, implementing, monitoring and evaluating public policies at the national level. The census is one of 16 national government censuses conducted by INEGI, of which eight specifically provide data on the criminal justice system.

The census is comprised of six modules that together contain 753 questions: 1) organizational structure and resources; 2) delivery of justice in criminal matters; 3) juvenile justice; 4) delivery of justice in civil, family and commercial matters; 5) alternative justice and/or alternative dispute resolution mechanisms; and 6) expert services. To ensure data quality, several classifications are

used to standardize data collection, including the Technical Standard for the National Classification of Offences for Statistical Purposes, adopted by INEGI.

INEGI includes the following documentation in the census' dissemination package:

- Two documents containing general results for both justice delivery and expert services.
- All six modules of the data collection instrument in PDF format.
- A document that describes the methodological, conceptual and design aspects of the census. The purpose of the document is to facilitate the correct interpretation of information by users, and to support the processes by which they can link the information to the design, implementation, monitoring and evaluation of public policies, specifically in the corresponding areas.
- The metadata specifying the background of the census, thematic coverage, geographical coverage, producers and sponsors, details on the data collection process, questionnaire structure, data processing, microdata access policy and legal notices. The metadata released is in line with the Data Documentation Initiative (DDI) standard.
- An Excel document containing the conceptual outline for each of the six modules of the census.

In addition to this documentation, INEGI offers tabular data in a predefined format. This includes six Excel files that contain information on justice administration, resources, public defence, alternative dispute resolution mechanisms and more. Each file contains a range of predefined tables that offer a wide variety of data disaggregated by state. In addition, it is possible to download a series of open data files in CSV format containing raw data and metadata that enable data users to conduct their own analyses. Moreover, the data is offered in a mobile app (México en cifras), a range of online tools that offer dynamic graphs, and developers can access the data and metadata through the INEGI Indicators API, which allows users to create applications that display information directly from INEGI databases in real time.

Modern IT solutions allow for the dissemination of administrative data and official statistics through websites and data portals, the latter being web-based interfaces designed to make it easier to find, explore and use data. It is important to seek impartial expert advice when making an informed decision on selecting the appropriate data portal to meet organizational needs. It is important to be aware of the advantages and shortcomings of each system, its use of international standards or proprietary formats, its sustainability and real cost of its maintenance.

In the Estonian case mentioned above, the e-File system provides near real time dashboards for authorized users that allow for the visualization of statistical data based on the different connected databases (for more details, see the case study in the annex to the present guidelines). In the Republic of Korea, to disseminate crime and criminal justice statistics, in addition to the statistics produced by different institutions, there is a data hub independent of KICS hosted by the Korean Institute of Criminology. This dynamic database allows users to explore time-series data that include administrative data from the different institutions, as well as survey data (i.e., victimization surveys).

3.4.4 Data security

The present guidelines highlight the importance of data governance, assigning clear roles and responsibilities in relation to data and access to them, and collaboration between different agencies in full compliance with relevant data security and privacy laws and regulations. While these considerations are crucial in ensuring clarity about data collection, storage and access, analysis and dissemination, additional technical considerations need to be taken into account in order to prevent

unauthorized access to data. Given the sensitive nature of crime and criminal justice data, designing and building an appropriate data security architecture should be a primary consideration for all countries. Advice is widely available on the internet on a range of data security topics such as authentication, configuration management and cyber threats.⁸³ Moreover, readers can refer to the ISO/IEC 27001 standard on information security management systems.⁸⁴ This section briefly highlights data classification, privacy-enhancing technologies, access control, network security, data encryption and the human element in data security.

In general, data should be provided on a need-to-know basis, meaning that people only have access to the data they need to perform their duties or to achieve the purpose for which the data were shared. To determine who can access the data, what kind of rights they have over the data and how the data can be used, it is essential to be aware of the sensitivity of the data that is being housed and develop a data classification. For example, data could be divided into categories such as public, confidential and highly confidential, as highlighted in Table 5. Factors to consider are whether the data contain personally identifiable information (such as names or addresses), whether the data are in aggregate form, and the legal basis and purpose of holding the data. Once the data have been classified, appropriate security measures for each type can be designed and implemented.

Table 5 Example of data classification

Classification level	Considerations	Access
Highly confidential	Sensitive data that contain personally identifiable information. Unauthorized access may endanger the safety or security of individuals, or violate their rights.	Data access and use should be restricted and limited to authorized users with specific roles.
Confidential	Data that do not contain personally identifiable information (such as name, address or phone number) and are intended for internal use or use by a trusted third party under a data-sharing agreement.	Data access and use limited to authorized users or trusted third parties under a data-sharing agreement that clearly specifies intended use and data-sharing modalities.
Public	Aggregated data intended for unrestricted public use that cannot be directly or indirectly traced back to individuals.	No restrictions

A key element in assigning a data classification when handling sensitive and confidential data is how to mitigate privacy risks. Institutions in the criminal justice system are entrusted with data that has the potential to improve the delivery of justice for all, but these data can also contain personally identifiable information that, when linked to individuals, can have serious negative consequences. This is underlined by principle 6 of the United Nations Fundamental Principles of Official Statistics, which states that individual data collected for statistical compilation are to be strictly confidential and used exclusively for statistical purposes.⁸⁵ Hence, when publishing statistics based on administrative data, it is essential to mitigate privacy risks through, at a minimum, data anonymization and aggregation. More advanced methods include the application of the differential privacy method or the generation of synthetic data.⁸⁶

After cataloguing the available data and assigning a data classification, the next step is to implement policies that control access to the data in line with the classification. This involves developing and implementing policies that tackle a range of topics, such as those covered in Table 6.⁸⁷

Table 6 **Examples of access control policies**

Policy	Description
Account management	Defines which types of accounts are authorized to access the data and manage/monitor accounts accordingly.
Principle of least privilege	Gives users limited data access so that they can only accomplish assigned organizational tasks.
Unsuccessful login attempts	Enforce a limit on consecutive invalid login attempts, especially for users with access to the data.
System use notifications	Display a message to users before granting access to the data that provides relevant privacy and security notices until the user acknowledges the conditions.
Session termination	Automatically terminates a user session after a set period of inactivity expires or a specified event occurs.
Remote access	Establishes user restrictions and connection requirements for remote access to the data.

Ensuring network security as a key component of any security architecture is related to these considerations. This includes a wide range of practices and technologies designed to protect the data and network resources. Before designing an on-site network, however, it is worthwhile to consider using existing products or services. For example, the use of cloud services transfers some of the responsibility for the management of the underlying technology and its security to the service provider.⁸⁸ Many cloud providers have invested heavily in security, including audit, authentication, physical security and operating procedures. When exploring this option, it is important to ensure that the service delivered by the cloud provider meets the needs of the organization and to seek guarantees regarding the use of the stored data to ensure that the provider does not use the data for their own purposes (for a brief discussion on data sovereignty, see section 3.4.3).

The following, non-exhaustive, overview of tools can be used to build secure network systems.⁸⁹

Table 7 **Examples of network security tools**

Tool	Description
Firewalls	Firewalls are barriers that stop suspicious traffic from entering or leaving a network while letting legitimate traffic through. They can be deployed on the entire network or used to divide the network into a smaller subnetwork (i.e., network segmentation). In this way,

	if one part of the network is compromised, the other parts remain inaccessible to the unauthorized user.
Intrusion detection and prevention systems	Deployed directly behind a firewall to scan incoming traffic for security threats, intrusion detection and prevention systems can automatically respond to potential threats, such as by blocking traffic or resetting the connection.
Network access control (NAC)	NAC acts like a gatekeeper that authenticates and authorizes users to determine who is allowed into a network and what they can do within it. NAC solutions are often used to enforce account management policies. For example, a junior user may only be able to view data, while a senior user may also have the right to edit data.
Virtual private networks (VPNs)	VPNs encrypt user traffic, allowing for secure communication over public networks and remote access to data assets.

A relatively new approach to network security involves the deployment of so-called zero trust networks.⁹⁰ Traditional networks focus on keeping threats from accessing the network. Once a user gains access, they are treated as trustworthy, but with the rise of decentralized networks and cloud services, perimeter-based security is becoming less effective. With a zero-trust architecture, the inherent trust in the network is removed and it is assumed that the network is hostile and each access request is verified based on an access policy. The right approach for an organization depends on its existing network architecture and security policies.

In addition to protecting data through access control and network security, encryption is another step that can be taken to ensure data security. Data encryption prevents unauthorized users from reading sensitive data, as it ensures that the data cannot be easily understood even if the unauthorized user accesses the data environment or captures the data while they are in transit. Encryption is the process of converting information (“plaintext”) into a series of unreadable, seemingly random characters (“ciphertext”) using an encryption algorithm. Associated with every encryption algorithm is a corresponding decryption algorithm that transforms the encrypted information into its original form.

A relevant standard on the topic is ISO/IEC 18033, which specifies encryption systems for the purpose of data confidentiality, including the Advanced Encryption Standard (AES) and Camellia block ciphers.⁹¹ Data encryption can be applied to data at rest and data in transit. Data at rest are data that are not actively moving from device to device or network to network, such as data stored on a hard drive or cloud storage. Encryption can be applied to data at rest using algorithms such as AES to safeguard the information from unauthorized access even if the storage medium is compromised. Data in transit refers to data actively being moved between systems or networks. Encrypting data in transit using a standardized protocol such as Transport Layer Security (TLS) or Internet Protocol Security (IPsec) is vital for preventing interception and tampering during data exchange.⁹²

Even with the most advanced security measures in place, however, there will always be a human element to data security. Cyberbreaches and attacks are most often caused by human error, not by failures of technical security standards. This is why it is important to foster a culture of security awareness among staff and invest in data security training, particularly for staff members with access to highly confidential data. Moreover, establishing and regularly communicating data security policies

to all staff can go a long way towards maintaining compliance and ensuring crime and criminal justice data are kept safe and secure.

3.4.5 Data quality

There is no single measure of data quality as it is a multidimensional concept that is strongly related to the needs of users. That said, access to high-quality data is a prerequisite for enabling evidence-based decision-making and meeting user needs. Collected and processed data also need to be consistent across the criminal justice institutions that supply the data. In short, collecting, producing and disseminating statistics can only offer added value if the underlying data quality is ensured.

The way to ensure data quality is to develop a quality assurance framework that fits national practice and circumstances. Multiple international organizations have developed generic frameworks for the assessment of data quality, which include the *United Nations National Quality Assurance Frameworks Manual for Official Statistics* and the *European Statistics Code of Practice*.⁹³

The *United Nations National Quality Assurance Frameworks Manual for Official Statistics* has five core recommendations and nine additional recommendations that are aimed at implementing specific fundamental principles. The core recommendations are focused on establishing a basis for the quality assurance of official statistics in a country. They call for a guaranteed legal and institutional framework, its application throughout the entire national statistical system and a commitment to the continual assessment of, improvement of and reporting on the quality of official statistics.

Regarding data output quality, the *United Nations National Quality Assurance Frameworks Manual for Official Statistics* lays out the six principles highlighted in Table 8.

Table 8 Principles for statistical output quality

Principle	Description	Requirements
1. Relevance	Statistics should meet the current and/or emerging needs or requirements of its users. The challenge is to balance the conflicting needs of different users and produce statistics that satisfy the most important needs within the given resource constraints.	<ul style="list-style-type: none"> 1.1 Procedures are in place to identify users and their needs and to consult them about the content of the statistical work programme. 1.2 Users' needs and requirements are balanced, prioritized and reflected in the work programme. 1.3 Statistics based on new and existing data sources are being developed in response to society's emerging information needs. 1.4 User satisfaction is regularly measured and systematically followed up.

2. Accuracy and reliability	Statistics should accurately and reliably portray reality.	<p>2.1 Source data, integrated data, intermediate results and statistical outputs are regularly assessed and validated.</p> <p>2.2 Sampling errors are measured, evaluated and documented. Non-sampling errors are described and, when possible, estimated.</p> <p>2.3 Studies and analyses of revisions are carried out and used to improve data sources, statistical processes and outputs.</p>
-----------------------------	--	---

3. Timeliness and punctuality	Statistics should be made available to users with the shortest delay possible and be delivered on the promised, advertised or announced dates.	<p>3.1 The timeliness of the statistical agency's statistics complies with international standards or other relevant timeliness targets.</p> <p>3.2 The relationship with data providers is managed with regard to timeliness and punctuality needs.</p> <p>3.3 Preliminary results can be released when their accuracy and reliability are acceptable.</p> <p>3.4 Punctuality is measured and monitored according to planned release dates, such as those set in a release calendar.</p>
-------------------------------	--	---

<p>4. Accessibility and clarity</p>	<p>Statistics should be easy to find and obtain, presented clearly and in a way that can be understood, and available and accessible to all users in line with open data standards.</p>	<p>4.1 Statistics are presented in a form that facilitates proper interpretation and meaningful comparison.</p> <p>4.2 A data dissemination strategy and policy exists and is made public.</p> <p>4.3 Modern IT is used for facilitating easy access to statistics.</p> <p>4.4 Access to microdata is allowed for research purposes, subject to specific rules and protocols on statistical confidentiality that are posted on the statistical agency's website.</p> <p>4.5 Mechanisms are in place to promote statistical literacy.</p> <p>4.6 The statistical agencies have a dedicated focal point that provides support and responds to inquiries from users in a timely manner.</p> <p>4.7 Users are kept informed about the quality of statistical outputs.</p>
<p>5. Coherence and comparability</p>	<p>Statistics should be consistent so as to make the combination and use of related data possible, including of data from different sources. Statistics should also be comparable over time and between areas.</p>	<p>5.1 International, regional and national standards are used with regard to definitions, units, variables and classifications.</p> <p>5.2 Procedures or guidelines are in place to ensure and monitor internal, intrasectoral and cross-sectoral coherence and consistency.</p> <p>5.3 Statistics are kept comparable over a reasonable period of time and between geographical areas.</p>

6. Metadata	Sufficient information should be made available to enable the user to understand all the attributes of the statistics, including their limitations. This includes information on the concepts and definitions applied, the variables and classifications used, the methodology of data collection and processing, and indications of data quality.	<p>6.1 The metadata management system of the statistical agency is well defined and documented.</p> <p>6.2 Metadata are documented, archived and disseminated according to internationally accepted standards.</p> <p>6.3 Staff training and development programmes are in place on metadata management and related information and documentation systems.</p>
-------------	--	--

The many methods and tools for quality assessment include assessing the quality of statistical outputs using the principles described above and can extend to assessing both the quality of the process and of the overall institutional environment. Quality indicators for statistical outputs can be developed that measure compliance with the above principles and allow for the description and comparison of quality among different statistical outputs and over time. In addition, regular consultation with data users through meetings or user satisfaction surveys can provide vital feedback about their analytical needs and perceptions of quality.

Going one step further, MDAs may choose to undergo an evaluation process. The goal of an evaluation is to identify possibilities for improvement in processes and products by referencing results against a standard model or framework. Evaluations can be undertaken by internal or external experts and, depending on the scope, take days to months to complete. Based on the result of the evaluation, an MDA may obtain a label or certificate after comparison with defined standards and requirements. A label can convey the extent to which a set of quality standards are met. For example, data outputs could be labelled as “official statistics” by the NSO after a successful evaluation.

As noted in the section on managing statistical processes, an improvement in the quality of statistical products requires the improvement of statistical processes. Frameworks such as the Generic Activity Model for Statistical Organizations (GSBPM) describe and define the processes needed to produce high-quality statistics. They establish a common language when referring to statistical processes and activities that take place within a statistical organization and are designed to be independent of the data source. Consequently, they can be used for the description and quality assessment of processes based on administrative data, surveys, censuses or mixed sources.

3.4.6 Use of open data standards

The *United Nations National Quality Assurance Frameworks Manual for Official Statistics* recommends data are made available in line with open data standards. While there is no agreed definition of open data, the International Open Data Charter defines digital data as data that are made available with the technical and legal characteristics necessary for them to be freely used, reused and redistributed by anyone, anytime, anywhere.⁹⁴ The International Open Data Charter emphasizes releasing data free of charge under an open and unrestrictive licence, in open and machine-readable formats, without mandatory registration on a central portal. Releasing crime and criminal justice data in such formats ensures that they can readily be used and reused by data users, increasing their value to society.

The term “open source” refers to software that has its source code made available under licence, which gives anyone the legal right to change and distribute the software freely and for any purpose.

In recent years, the adoption of open-source technologies has increased in NSOs as a replacement for commercial software products and there is a tendency to move away from in-house development towards collaboration. Indeed, open-source software is frequently developed in a collaborative public manner. Open-source technologies range from operating systems (for example, Linux), database management systems (for example, MySQL) and programming languages (for example, Python or R). International and regional bodies have been created to foster collaborative IT development, such as the High-Level Group for the Modernisation of Official Statistics (HLG-MOS), the Common Statistical Production Architecture (CSPA), the Statistical Information System Collaboration Community (SIS-CC) and the Statistical Data and Metadata eXchange (SDMX) toolkit.

The benefits of adopting open-source software include the flexibility to customize the software to suit specific needs, the transparency of the source code, lower costs and avoiding vendor lock-in. Challenges include a potential lack of official support, steep learning curves, dependency on community contributions and possible compatibility issues.

Box 17 X-Road: an open-source collaboration

Estonia's X-Road solution is a secure and decentralized data exchange platform that facilitates communication between various government and private sector organizations. It serves as the backbone of Estonia's digital infrastructure and underpins its successful e-Government initiatives. X-Road connects different information systems that may include a variety of services. In June 2023, 3,155 services were available in Estonia via X-Road (known as "X-tee" in Estonia).

X-Road was adopted by the Government of Estonia to promote interoperability between the many different systems that have been developed autonomously by different MDAs. The X-Road solution is open source and has been adopted by other Governments, such as those of Argentina, Finland, Iceland and Japan. X-Road not only allows national data exchange but also cross-border data exchange based on signed protocols and agreements. Estonia and Finland are currently exchanging information on business registers, taxation and population registers using X-Road.

In Argentina, the Ministry of Justice has developed a tool to improve the sharing of personal data in the context of judicial investigations using the central common interoperability platform (Interoperar). The tool allows registered users (for example, tribunals, prosecutors, courts) to request data from and between those data registers connected to the interoperability platform,⁹⁵ thereby speeding up data access and reducing the response time to citizens. Next steps for the platform include the implementation of the X-Road solution to allow for cross-border data exchange.

Box 18 Free and Open-Source Software: the Kingdom of the Netherlands⁹⁶ and Poland⁹⁷

Kingdom of the Netherlands

In 2010, Statistics Netherlands first approved R, a Free and Open-Source Software (FOSS) tool for use in the production of statistics. The adoption of R was picked up in a bottom-up fashion by a group of professionals who organized user group meetings, courses, software development standards and ran application management to support the process. Statistics Netherlands also adopted a FOSS policy that specified procedures for using, contributing to and developing FOSS products.

In 2012, Python was also approved for statistical production and a bottom-up approach again led to user meetings and knowledge exchange. Currently, R is the recommended tool for statistical work on data, while Python is recommended for orchestration and process management. The major strengths of Python over R were the ability to integrate with (web) services and a strong tradition of machine learning and text mining. The strengths of R over Python were visualization, data processing and management, its strong statistical libraries and a strong package management system (CRAN). Apart from the difference in the maturity of package management, R and Python can now be considered roughly equivalent in most of these areas.

Using and contributing to open-source software has been an essential part of the development of Statistics Netherlands over the past decade or so. Moreover, the open-source way of working has lowered the barrier to collaboration internationally, within the official statistics community or beyond, to the point where that barrier has all but vanished.

Poland

Statistics Poland is adapting to the new digital world by using available technologies and data in an innovative, safe and affordable way. Considering the benefits to society and the economy from the use of open-source software, and taking into account the law and applicable rules and standards for statistical production, the President of Statistics Poland issued the Being Open manifesto. Based on the manifesto, Statistics Poland is committed to using open-source software in the statistical production process and to actively participating in the work of communities creating open-source software.

Open-source software is used by statistics Poland in almost all areas – from technical infrastructure (operating systems, servers and network monitoring), through programming, data processing and analysis, data sharing, project management, geospatial information, and internet application security, to minor utility programs supporting daily work. Some examples of FOSS are:

- **Docker:** Open-source software used to implement virtualization at the operating system level (known as “containerization”) in order to create, deploy and run distributed applications.
- **PostgreSQL:** A relational database management system used in the information portal.
- **R-Studio:** Used primarily to compare data sets and create tables, charts and summaries when analysing data, this provides a good solution for large databases, as it allows many operations to be performed quickly. Its benefit is the ease with which it reads CSV, XLS and XLSX files.
- **Shiny:** A development environment for R language for creating web applications, used for testing data analyses and creating interactive charts.

- **Python:** A programming language used to write scripts related to Big Data analysis.
- **GitLab:** A version control system and software supporting project management based on Git.
- **Inkscape:** A program for editing vector graphics (for example, related to graphical data visualization in a range not available in Microsoft Excel).

Sample assessment questions on data architecture

- Have data standards, classifications and coding schemes been developed that are consistently applied across different institutions?
- Are guidelines or manuals for ensuring consistent data collection and reporting practices available?
- Is a mechanism in place to regularly train staff on the proper application of data and metadata standards?
- Is a data quality assessment mechanism in place that requires regular evaluation of data outputs against defined quality standards and requirements?
- Has a robust and secure IT infrastructure been developed for supporting the collection, storage, processing, analysis and dissemination of criminal justice data?
- Is a database management system in place for managing the database structure and controlling access to data?
- Are mechanisms in place for regularly backing up and protecting the data from loss or unauthorized access?
- Are adequate resources – including hardware, software and human and financial resources – available for managing and maintaining the data infrastructure in a sustainable manner?
- Has a data-sharing platform or portal been developed that allows authorized users to access and utilize crime and criminal justice microdata for research, policy analysis and decision-making purposes?
- Are aggregate statistics released in open and machine-readable formats on a central portal that does not require registration?

4 Conclusions and recommendations

Core data for the production of statistics in the criminal justice system can be extracted from administrative records kept by the police, prosecutors, courts, prison administrations and other MDAs. Such administrative data are essential for the effective and efficient operation of the criminal justice system and serve to strengthen public trust and confidence in the sector. The present guidelines provide an overview of the nature of administrative data, the associated benefits and challenges, and highlights how the collection, production and dissemination of administrative data for statistical purposes are shaped by the specificities of the criminal justice system in each country.

One of the main findings is that there are no one-size-fits all solutions for achieving greater data interoperability and improving data governance of administrative data on crime and criminal justice. Countries are constrained by the degree of (de)centralization, regulatory frameworks, past practices and procedures as well as the availability of skilled personnel, technical resources, funds and the level of political commitment. Nevertheless, the present guidelines introduce four basic building blocks that can be used to improve the ability to collect, produce and disseminate relevant crime and criminal justice statistics, namely leadership and vision, regulations, coordination and cooperation, and data architecture.

Assessment

The first step in the improvement of the collection, production and dissemination of administrative data for statistical purposes in the criminal justice system is to assess the current state of data governance arrangements. Each of the four main sections of chapter 3 offer a series of sample assessment questions that are meant to provide a starting point for evaluating the maturity of any system of criminal justice statistics. Countries are encouraged to customize the questions according to their specific contexts and needs and expand on them when deemed relevant. In addition, Table 9 offers a means of assessing the level of maturity of the data governance system using the four elements in the present guidelines.

Table 9 Data governance maturity assessment

	Ad hoc	Basic structure	Continuous improvement
Vision and leadership	No data strategy for criminal justice system in place	Data strategy for criminal justice system developed through an inclusive process	Data strategy fully integrated into organizational strategies with feedback mechanisms in place and data stewardship roles assigned
Regulations	No regulatory framework on official statistics or data privacy and security in place	Basic regulatory framework in place, not consistently enforced	Regulatory framework in place, compliance mechanisms developed and consistently enforced, implementation guidelines available

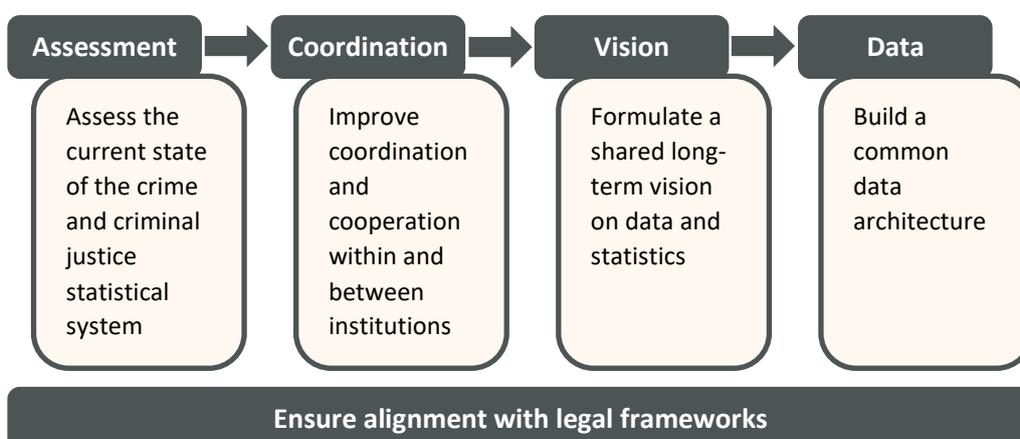
Coordination and cooperation	Work takes place in silos	Basic coordination mechanism in place with partial/inconsistent participation	Formalized coordination mechanism in place with seamless cooperation across all criminal justice system stakeholders
Data architecture	No defined data management rules in place, leading to inconsistent processes and outputs; data (partially) still collected on paper	Basic data architecture principles identified with standardized processes in place for data collection, storage, analysis, dissemination and security	Optimized data architecture where data availability, quality and security are proactively managed, data are available in open and machine-readable formats and emerging technologies are seamlessly adopted

Source: UNODC.

Road map for the improvement of data governance

Working on any one of the four elements introduced in the present guidelines can improve the collection, production, dissemination and use of relevant, high-quality crime and criminal justice statistics. While there is no fixed order in which countries should tackle each of the elements, an ideal starting point after the initial assessment is to work on improving coordination and cooperation. To guarantee the timely collection of harmonized administrative data within and between institutions, it is essential to have both formal and informal collaboration mechanisms in place that involve the key stakeholders among the many involved in the production of crime and criminal justice statistics. Ways to formally improve cooperation include the adoption of binding frameworks that provide for the production of criminal justice data or memoranda of understanding that facilitate collaboration and data exchange between institutions.

Figure 6 Road map for the improvement of data governance



Source: UNODC.

Once cooperation between different MDAs has been established, work on formulating a long-term vision for administrative data and statistics in the criminal justice system can be initiated. To ensure alignment of the relevant stakeholders, both within and outside the criminal justice system, it is vital to organize an inclusive process that sets clear and achievable priorities during this phase. Assigning key roles and responsibilities will further ensure that the strategic vision is translated into the everyday practice of relevant staff.

The focus can then shift to building a common data architecture and breaking down existing data silos. A well-designed data architecture will facilitate the collection, production, dissemination and use of crime and criminal justice statistics at the technical level. The data architecture must support quality, security and confidentiality, as well as access to data at any time in the data life cycle. The design of a data architecture includes policies and standards, but can also include specific IT solutions that are used in organizations. The present guidelines highlight data standardization, statistical processes, the data life cycle, data security, data quality and open data standards as priority areas.

Throughout the process it is vital to ensure alignment with existing legislation, rules and guidelines that provide frameworks for the collection of data, their quality and security, and specify limits on the use and reuse of data. This will protect privacy, promote transparency and foster public trust in the data. If existing legislative frameworks are outdated or lacking in specific areas, it may be worthwhile to pursue the adoption of new or revised legislation in the medium to long term as this can be a lengthy and complex process.

Incremental change

The primary objective of the present guidelines is to facilitate the collection, production, dissemination and use of high-quality crime and criminal justice statistics that effectively serve the needs of data users. Although improving interoperability and data governance is the ultimate long-term goal, countries face different circumstances and contexts that may make the realization of such a goal seem like an insurmountable challenge. For this reason, starting small with one of the elements and building on what works is highly recommended. As a practical step, it is worthwhile evaluating existing systems and solutions beforehand in order to review what has already been done before designing a new system from scratch. It may be possible to retain elements that already function well and move the system forward from there.

In the short term, smaller incremental changes can be made to improve the current governance of administrative data for statistical purposes using any of the four elements highlighted in the present guidelines. The more drastic or rapid the change, the greater the burden on individual institutions and budgets – substantially increasing the cost of failure. Incremental improvements are typically easier to implement, involve fewer risks and building on the success of incremental changes, while time consuming, increases the chance of long-term success. For example, a country may opt to standardize data on intentional homicide collected by the police and use this as a first step in paving the way for more and better administrative data and statistics on crime and criminal justice. This can be used to champion data and showcase their utility throughout the criminal justice system.

Human resources

In addition to the technical elements discussed throughout the present guidelines, the management of human resources is key to improving the governance of administrative data in the criminal justice system. The survey conducted as part of the research for the preparation of the present guidelines highlighted the fact that a limited number of professional staff and a lack of technical skills are two of the most important constraints to the production of statistics on crime and criminal justice.

Therefore, it is highly recommended to hire staff for key data-related positions (for example, data stewards) and include dedicated data units within organizational charts so that they are less vulnerable to staff rotation or political and administrative changes. Moreover, investment in the training of new and current staff is recommended on topics such as data literacy, data standardization, data security and data-related legislation, as is promoting the exchange of experiences with administrative data for statistical purposes across the different institutions of the criminal justice system and beyond.

Interoperable future

Data are a key strategic asset, not just a by-product of daily operations. They are increasingly necessary not only for the basic operation of the criminal justice system but also for planning, the development of policies and budgets, and improving performance. Developing an interoperable system of administrative data for statistical purposes within the criminal justice system is not an easy task, however, as it requires significant investment, the harmonization of systems and due consideration to be given to data security and privacy. Policies should also be able to address current needs and be flexible enough to adapt to the changes that inevitably arise. The development of a data governance framework capable of guiding the development of an interoperable system will be an ongoing, lengthy and iterative task.

That said, an interoperable system offers enhanced efficiency and collaboration both within and between the MDAs of the criminal justice system. A key benefit is the seamless exchange of real-time information and statistics not only within each individual institution but also between the police, the prosecution service, the courts, the prison system and other relevant stakeholders. This facilitates quicker decision-making, enables authorities to respond promptly to emerging threats and places greater emphasis on meeting the needs of individual justice users. Moreover, an interoperable system can provide nuanced and highly disaggregated statistics, thereby aiding in the development of targeted crime prevention strategies and the optimization of resources. Such a system promotes transparency and accountability within the criminal justice system, fostering public trust and offering a pathway to a fairer, more inclusive, efficient and effective system.

Annex: Case Studies

Cameroon: Improving homicide statistics

Provided by the National Institute of Statistics (INS) of Cameroon

In line with the implementation of the National Strategies for the Development of Statistics 2021–2030 (Stratégies Nationales de Développement de la Statistique), the National Statistical Information System (Système National d'Information Statistique (SNIS)) of Cameroon has seen significant development, enabling it to respond to the national and international demand for statistical information. Although improvements in the volume and quality of statistical production are perceptible, much remains to be done for improving the monitoring and evaluation of development policies and strategies, including the Sustainable Development Goals. In particular, monitoring indicator 16.1.1 (Number of victims of intentional homicide per 100,000 population, by sex and age) requires quality information on intentional homicides. To bridge this information gap, SNIS has initiated, with the technical support of UNSD and UNODC, a profound reform to improve the quality of the indicator.

Currently, indicator 16.1.1 poses numerous problems due to the concepts used, the management of data sources and calculation method difficulties that stem from the lack of a common database for all homicide data. The solution is therefore to create an individual database on intentional homicides that integrates data from the two main sources: the national gendarmerie and the police. The database should make it possible to address the usual problems of coverage and double counting and, above all, clearly distinguish intentional from non-intentional homicides. The approach will be implemented in five stages: i) diagnosis of the existing system; ii) awareness raising among the main stakeholders; iii) staff training; iv) production of an integrated database during the pilot phase; v) preparation of a report analysing the data from the pilot phase and evaluation of the project.

1. Diagnosis of existing system

The diagnosis work was completed through a number of exchanges with the main stakeholders, namely the national gendarmerie, the police, the Ministry of Justice, the Ministry of Women's Empowerment and the Family, the Ministry of Territorial Administration and the National Statistical Office. The exchanges concluded with a national workshop that identified difficulties in measuring the indicator, which were mainly linked to coordinating the actions of the different stakeholders, the absence of a national database, coverage, double counting, consistency of sources and the calculation methodology.

2. Awareness raising

In addition to open discussions with the stakeholders who regularly handle homicide data at the national level, a high-level meeting was organized with decision-makers, which made it possible to share the merits of the production of quality indicators for monitoring national and international development policies and strategies. Emphasis was placed on the effective use of data for planning, programming, budgeting and, above all, the monitoring and evaluation of actions. Civil society actors were also involved in the discussions, mainly as users of statistical information.

3. Staff training

This took the form of a workshop led by a team from UNODC and UNSD. Topics covered included the definition of concepts, harmonization and disaggregation of data, the quality of administrative data, an assessment of the quality of existing data on intentional homicides and the main challenges involved in producing homicide statistics. As a result, a road map was developed to help steer the project through to its final phase, consisting of the evaluation of the analysis report of the pilot data.

4. Production of an integrated database

After the workshop, the main stakeholders involved in the issue of intentional homicide met several times with the NSO to implement the road map. To this end:

- A data collection sheet was designed and developed in Excel in a participatory manner.
- The national gendarmerie and police personnel responsible for compiling homicide data were trained to fill in the sheet using the physical archives available in their departments. Considered a pilot case, the focus was on data for the year 2022, the idea being to develop the mechanisms for quality control in order to make it operational by 2024.
- Data collection was subsequently undertaken by the national gendarmerie and the police and the two files obtained will be merged to create a single national file that will be processed and used to produce indicator 16.1.1.

5. Data analysis report and project evaluation

With the participation of all stakeholders, a data analysis report of the pilot phase will be produced using the database obtained for the year 2022, which will then be presented and discussed at the evaluation seminar planned for early 2024. An objective assessment will be made of the work carried out and final adjustments to the overall approach may be recommended before the effective implementation of the database planned for 2024, with the possibility of reconstructing, as far as possible, the time series on intentional homicides in Cameroon.

During the course of the project, new attitudes and habits have been acquired by SNIS stakeholders and are beginning to be implemented in practice. Specific organizational measures will be taken at the NSO level to ensure better coordination and continuous improvement of the system.

Ecuador: Special Statistical Commission on Security, Justice, Crime and Transparency

Provided by the National Institute of Statistics and Censuses (INEC) of Ecuador

History of the commission

Article 13 of the Statistics Law of Ecuador empowers the National Institute of Statistics and Censuses (INEC) to create Special Statistical Commissions that function as auxiliary and advisory bodies of INEC comprised of delegates of the institutions producing and using statistics in a certain sector. Moreover, article 10 of the same law states that INEC is responsible for "coordinating the operation of the special statistical commissions" and "coordinating and supervising the execution of the statistical programs and work plans to be carried out by the other institutions of the National Statistical System".

The Special Statistical Commissions have a mandate to propose the design, development and implementation of statistical plans and projects aimed at closing information gaps, standardizing methodologies, incorporating new data sources, preparing sectoral statistical programmes, and the overall improvement of official statistical production within the National Statistical System.

The generation of statistical information on crime in Ecuador began around 2000, a time when there was no process in place to guarantee quality, timely and reliable data. Several actors were producing information in an idiosyncratic and isolated manner, but the need to integrate citizen security statistics into a single system had not yet been conceived. From this starting point, there was a need to strengthen information capture processes, to have manuals documenting the activities carried out, to improve the administration of standardized crime classifiers, and to improve the use of technological tools for managing information with databases.

In order to address the need to strengthen the statistical production process in the crime and criminal justice system, in June 2010 INEC established a Special Inter-institutional Commission on Citizen Security and Justice Statistics.⁹⁸ Its original objective was limited to coordinating and standardizing the methodology for the production of official information on citizen security and justice statistics through the synergy of relevant institutions. The commission was to serve as a systematic and transparent input for an adequate design, execution and evaluation of security policies.

However, just a year after the commission's creation, the President of Ecuador broadened its scope in response to the urgent need for standardized figures for such a sensitive sector.⁹⁹ INEC then broadened its objective to the development and standardization of guidelines, technical criteria and methodological schemes for the production of official information on citizen security and justice statistics.¹⁰⁰ Consequently, the commission became the foundation stone on which to build the evidenced-based National System of Violence and Citizen Security.

The commission has been undergoing further developments and improvements ever since. In December 2012, it created a Technical Subcommittee for Validation aimed at supporting the commission's decision-making. In the period 2016/17, INEC created further technical subcommittees linked to the National Development Plan 2017–2021 and the 2030 Agenda for Sustainable Development. More recently, INEC has undertaken restructuring and optimization processes to streamline the works of its Special Statistical Commissions. As a result, the commission has been revamped as the Special Statistical Commission on Security, Justice, Crime and Transparency, the objective of which is: "to promote the production and strengthening of information on security, justice, crime and transparency through the design, development and implementation of statistical

plans and projects to ensure compliance with the national agenda for development, sectoral and territorial agendas, and international development plans".¹⁰¹

Structure of the Special Statistical Commission on Security, Justice, Crime and Transparency

The commission is steered through a strategic group, made up of the heads or high-level delegates of nine entities.¹⁰² Additionally, the work of the commission is distributed among technical groups, formed by the member institutions according to their areas of competence and based on their needs. The chairmanship of the commission falls on INEC, both in the strategic group and in the technical groups.

Current technical groups include:

- Technical Group for the Statistical Strengthening of Security and Justice Indicators
- Technical Group on Corruption and Transparency
- Technical Group on Road Safety Statistics

At present, the commission is comprised of the heads or delegates of 36 institutions, including members from the crime and criminal justice system, planning agencies, education, defence, financial, health and social security institutions.

Achievements of the Special Statistical Commission on Security, Justice, Crime and Transparency

National level

- Contributing to the creation of statistical projects such as the First Survey on Victimization and Perception of Insecurity (2011) and the First National Survey on Family Relations and Gender Violence against Women (2011).
- Identifying single sources of information for reporting statistics on citizen security.
- Defining the methodological process for the creation, validation and processing of statistics on crime reports based on the administrative records of the Attorney General's Office.
- Defining the most socially significant crimes to be monitored periodically.
- Defining the process to officialize statistical information on Citizen Security.
- Standardizing data production for the Sustainable Development Goal indicators.
- Developing, validating and updating the Statistical Registry of Intentional Homicides of Women and Femicide.
- Developing and updating methodological documents that contribute to the continuous improvement and standardization of data production processes.

International level

- Participating in the development and piloting of the International Classification of Crime for Statistical Purposes (ICCS) developed by UNODC.
- Participating in the development and review of the Latin America and the Caribbean Crime Victimization Survey Initiative (LACSI) developed by the UNODC-INEGI Center of Excellence in Statistical Information on Government, Crime, Victimization and Justice and the Center of Excellence of INEGI, through the INEC Regional System of Standardized Indicators of Coexistence and Citizen Security (SES) project.
- Participating in the piloting of the Statistical Framework for Measuring the Gender-related Killing of Women and Girls (also referred to as femicide/feminicide).

Finally, as Special Statistical Commissions are periodically evaluated and their continuity is determined depending on their results, the Special Statistical Commission on Security, Justice, Crime and Transparency has proved its relevance, validity and effectiveness time and again. It is one of the most active and longest-standing inter-institutional spaces coordinated by INEC, its contributions are evident nationwide and have had significant impacts on the statistical processes carried out by its member entities. It is expected to continue working as a valuable asset throughout the security sector in the years to come.

Estonia: e-Justice system and interoperability

Based on an interview with the Centre of Registers and Information Systems (RIK) of Estonia

Description

Estonia's e-File system is a digital platform that allows for the efficient handling of criminal proceedings within the country. The implementation of the e-File system has significantly improved the efficiency and transparency of criminal case management in Estonia and has reduced administrative burdens, minimized paperwork and enhanced the speed of information exchange among relevant parties.

The e-File system serves as a centralized database where all relevant information and documents related to criminal cases are stored electronically. It provides a secure and accessible platform for prosecutors, judges, defence attorneys and other authorized parties to access case files, submit documents and track the progress of criminal proceedings. Different information systems (for prosecutors, police or courts) are connected to e-File, which serves as a backend for the different systems.

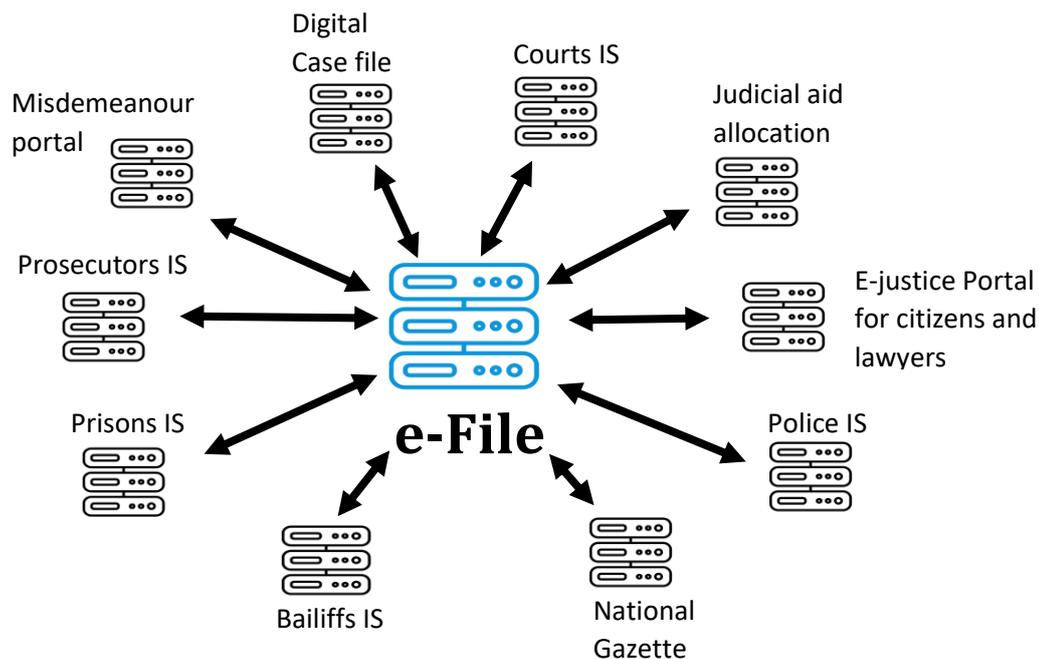
Key features of the system include:

- **Digital case management:** The e-File system allows for the creation, organization and management of criminal cases in a digital format. This includes storing details such as case identifiers, parties involved, charges and court decisions.
- **Document submission:** Users can submit various types of documents related to criminal cases electronically, including petitions, motions, evidence and other supporting materials. The system ensures the integrity and authenticity of the documents through digital signatures and encryption.
- **Notifications and reminders:** The e-File system enables automatic notifications and reminders for upcoming hearings, deadlines and other important events related to the case. This ensures that all parties involved stay informed and facilitates timely actions and responses.
- **Access control and security:** The system incorporates strict access controls and encryption protocols for data transfer in order to safeguard sensitive information. Only authorized individuals, such as judges, prosecutors and lawyers, can access the case files, ensuring data privacy and security.
- **Integration with other systems:** Estonia's e-file system is designed to integrate seamlessly with other components of the e-Justice system. This allows for the exchange of information and data between different legal entities and stakeholders involved in the criminal justice process.

The most important components of the e-File system are Public e-File (for citizens and lawyers), Prosecutors IS (for prosecutors and staff), Court IS (for judges and staff) and Police IS (for police). Public e-File is a system integrated into e-File that enables citizens both to initiate civil, administrative, judicial and misdemeanour proceedings and monitor them, as well as submit documents. Public e-File is the part of e-File that is visible to citizens and lawyers involved in a specific case. It enables parties and their representatives to submit proceedings documents to the court electronically and monitor the progress of the related court proceedings. Citizens and their representatives can also dispute claims and decisions as well as make enquiries in the Criminal Records Database regarding themselves and others.

Public e-File is connected with other information systems within the criminal justice system. The Prosecutors Information System is the case management system for all prosecutors in Estonia (293 officials, including 191 prosecutors) and the Court Information System is the case management system for all the courts (243 judges and 750 staff). The court system includes a videoconferencing solution and automated transcriptions that are used in court hearings. Every court case has a unique identifier and consists of at least one charge. Case documents can be viewed either by the different individual charges in the case or the case as a whole. The Police Information System consists of a web-based solution used by officers to access all information and is connected with the other e-File systems.

Figure 7 e-File central case management system in Estonia



Source: Centre of Registers and Information Systems (RIK), unpublished PowerPoint presentation.

This interoperable system allows for the linking of different information systems and the creation of near real time statistics on many different aspects of the criminal justice system. This includes elements linked to the inputs into the system and its functioning – such as staffing levels or average time needed for each service (for example, court proceeding) – and to output elements – such as average conviction time or the type of weapon used in crimes. Beyond the creation of statistics, the system’s high level of interoperability lets actors have access to information in real time. Prosecutors can share information with courts and the police, those engaged in trials can check information concerning their proceedings, and citizens can check every procedure scheduled by each court in Estonia through the Digital State Gazette, with all information about hearings stored in the e-File system. The regular use of secure digital authentication and electronic signatures (eID) by most of the population allows easy access to e-services and enables information exchange between government entities and the public.

The different components of e-File (Prosecutors IS, Court IS, Police IS) are connected with other government systems (tax and customs, population register, business register, land register, etc.) using X-Road, and can retrieve information for the proceedings. The e-File system has mostly been developed by a state agency (RIK) under the Ministry of Justice, which has 16 development teams and around 250 staff. Apart from e-File, RIK is also in charge of other e-government systems such as the e-

Business Register, European Business Register, e-Land register, e-Financials, Criminal Records Database, State Gazette, Official Announcements, the Courts Information System and the Prosecutors Information System.

X-road basis

Estonia's X-Road solution is a secure and decentralized data exchange platform that facilitates seamless and reliable communication between various government agencies and private sector organizations. X-Road serves as the backbone of Estonia's digital infrastructure, underpins its successful e-Government initiatives and connects different information systems that may include a variety of services. In June 2023, 3,155 services could be used in Estonia via X-Road.

Adopted by the Government of Estonia to promote interoperability between the many different systems that were developed independently by different MDAs, X-Road uses standardized data formats and protocols that ensure reliable and seamless communication between entities. X-Road also provides a highly secure environment for data exchange between different organizations by using advanced encryption and authentication mechanisms to protect the confidentiality and integrity of the transmitted data. Moreover, X-Road incorporates a robust access rights management system that allows organizations to define and control access privileges for different data categories, ensuring that only authorized personnel can access and utilize specific information.

The X-Road solution is open source and has been adopted by other Governments, such as those of Argentina, Finland, Iceland and Japan. X-Road not only enables national data exchange but also cross-border data exchange based on signed protocols and agreements. For example, Estonia and Finland are exchanging information on business registers, taxation and population registers.

Challenges

Rather than technical, the greatest challenge for the Estonian system has been securing cooperation among the different ministries and entities involved. Not only are different departments connected through e-File, they can also directly share and exchange information. Although many countries have developed digital case management systems for individual institutions, such as the police, it is much rarer for a single case management system to be deployed across multiple institutions, like in Estonia, as this requires a degree of cooperation and willingness to share data that may not be feasible in different contexts.

An early challenge was resistance from a limited number of staff to the transition to a fully digital and interoperable environment. The Estonian system is designed to be an almost entirely paperless one in which all documents can be directly attached to case files and viewed at any moment. For staff accustomed to paper-based processes, this was a significant change that required a period of adjustment. To address this, RIK introduced the system in an incremental manner, beginning with criminal offences, and on an optional basis for users. As users became accustomed to the system and experienced its benefits, it became easier to expand the scope to civil and administrative offences and eventually make use of the system mandatory.

Recommendations

To connect different government services and build an interoperable platform that connects different systems, a high level of political support is required. This requires strategic and long-term thinking, documented ideally in an official development road map that should set clear strategic priorities and specify deliverables, including realistic timelines. The road to developing a well-functioning and

interoperable system of criminal justice statistics is a long and winding one that also requires a degree of flexibility. As a practical step, it is a good idea to evaluate existing systems and solutions before moving to design a new system from scratch as it may be possible to retain existing elements that function well and take the system forward from there.

It is unlikely that “off-the-shelf” IT solutions are available and Governments may need to develop their own solutions, either using internal or external developers. Depending on the department and the need and structure of the public system, the use of external or internal staff may be preferred.

Way forward

Although Estonia already has an advanced system of criminal justice statistics, work to improve the system further is ongoing. For example, since some data records in the system, such as case descriptions, are in plain text format, RIK is currently developing a machine-learning solution for reading them and taking all the necessary information from the text, including locations and offender characteristics, in order to further codify the text from each case. Furthermore, all files uploaded into the system will be indexed and directly searchable through the use of key terms.

RIK is also developing a data warehouse for the Ministry of Justice that will take in all the information from the e-Justice system and offer data analytics functionalities to make it straightforward for officials to review the anonymized data and generate statistics. The use of this system will be facilitated through a dashboard that will allow users to create custom graphs, tables and reports. The data contained in this data warehouse will be regularly updated to guarantee access to (quasi-) real-time information, and will be open to authorized criminal justice actors, including prosecutors, judges, court staff and Ministry of Justice analysts.

Resources

e-File:

<https://www.rik.ee/en/e-file>

<https://www.rik.ee/en/international/public-e-file>

X-Road:

<https://e-estonia.com/solutions/interoperability-services/x-road/>

<https://x-road.global/xroad-world-map>

e-Government:

<https://e-estonia.com/solutions/>

Indonesia: One Data Initiative and criminal justice statistics

Provided by the Crime Stats Team, Directorate of Resilience Statistics, BPS-Statistics Indonesia

Background

Not just an important benchmark for public security, crime statistics also serve as a basis for the preparation of national development planning for public security and improving public welfare. Aside from national considerations, crime statistics are also relevant at the international level. They are used to meet the data requirements of the United Nations Crime Trend Survey (UN-CTS) and are an essential part of achieving the Sustainable Development Goals. This is particularly the case for Goal 16, which is aimed at promoting peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels.

To meet this growing demand, Indonesia is continually working to improve its crime statistics, although challenges related to the availability and quality of crime data remain in the country. This includes a lack of data to calculate certain international crime indicators and differences in the way crimes are classified between different law enforcement agencies within the country.

Collecting crime data in Indonesia

Crime statistics are produced in Indonesia both through the use of administrative data and surveys conducted by the National Statistical Office of Indonesia (BPS-Statistics Indonesia). Several surveys conducted by BPS are related to crime and complement administrative data, including Susenas (the National Socioeconomic Survey) and Podes (the Village Potential Statistics), and the victimization survey pilot through SPTK (the Happiness Level Measurement Survey).

In addition, BPS collects crime-related administrative data from law enforcement agencies in Indonesia. Crime-related administrative data are collected annually for multiple purposes, such as producing the annual Crime Statistics report, filling out the UN-CTS questionnaire and reporting on Sustainable Development Goal indicators related to crime.

To produce crime statistics, BPS requires the cooperation of criminal justice institutions. Based on Law Number 16 of 1997, concerning Statistics, BPS has the role of supervising the collection and production of statistics carried out by government agencies. Furthermore, the President of Indonesia issued Presidential Regulation Number 39 on 12 June 2019, which concerns the Indonesia One Data initiative. The initiative constitutes a government data governance policy for producing accurate, updated, integrated and accountable data that are easily accessible and shared between central government agencies and regional agencies through the realization of data standards, metadata, data interoperability and use of reference codes and master data.

In 2021, to operationalize the One Data Initiative, BPS initiated Satu Data Statistik Kriminal Indonesia (SDSKI). SDSKI is aimed at enhancing the governance of crime data in Indonesia in order to produce high-quality crime statistics based on the Indonesia One Data principles, as follows:

- Data must meet data standards
- Data must have metadata
- Data must comply with data interoperability rules
- Data must use the reference code and/or master data

To improve the quality of existing crime data in Indonesia and implement SDSKI, the following six activities have been initiated:

1. BPS organized a kick-off webinar to raise awareness among all parties, especially agencies involved in jointly building SDSKI. This webinar was held online on 8 September 2021 and was attended by more than 2,000 participants.
2. BPS created a road map that specifies the data sources, data classification, data principles and expected outputs of SDSKI. SDSKI will utilize both administrative and survey data that are to be aligned with the International Classification of Crime for Statistical Purposes (ICCS) and must meet the One Data principles highlighted above. SDSKI is expected to disseminate crime statistics through a publicly accessible dashboard.
3. BPS mapped the availability of crime data in Indonesia. Results showed that 16 out of 24 crime-related Sustainable Development Goal indicators still need to be developed in order to meet global indicator standards and that Indonesia was only able to fill 36 out of 162 UN-CTS indicators in 2022.
4. Multiple meetings were organized with affected agencies to discuss future plans and technical matters regarding SDSKI. These discussions included BPS, KemenkoPolhukam (Coordinating Ministry for Political, Legal and Security Affairs), Bappenas (Ministry of National Development Planning/National Development Planning Agency), the Indonesian National Police, the Supreme Court of the Republic of Indonesia, the Attorney General of the Republic of Indonesia, the Correction–Ministry of Law and Human Rights, and the department of criminology of the University of Indonesia.
5. To standardize the concepts and definitions of crime among criminal justice institutions, BPS is championing the implementation of ICCS. BPS and the involved criminal justice institutions, with the help of academics, have already mapped the Indonesian penal code into the ICCS categories. An agreement regarding the concepts, definitions and the classification has not yet been achieved, however.
6. BPS and the institutions involved in the SDSKI collaboration have received technical assistance regarding crime statistics from several organizations, including UNODC and the Australian Bureau of Statistics (ABS). In early 2023, UNODC provided assistance on how to implement ICCS. In July 2023, representatives of BPS and several law enforcement agencies visited ABS to learn best practices from Australian counterparts on the governance of crime statistics and their experience in implementing the Australian and New Zealand Standard Offence Classification.

Key challenges and opportunities of improving crime statistics

Currently, the main concern for collecting crime data in Indonesia, especially administrative data, is the lack of official collaboration between BPS and the criminal justice institutions that produce the data. Since there is no regulation directly covering such a collaboration, law enforcement agencies are reluctant to provide crime data and coordinate efforts. This obstructs the management and coordination of crime statistics between BPS and those institutions. As a result, BPS is restricted in its provision of sectoral assistance and improving the quality of crime data for statistical purposes.

BPS has started looking for new opportunities to solve this collaboration problem. Based on information obtained during meetings, BPS has determined that criminal justice institutions have established a collaboration with KemenkoPolhukam and Bappenas in order to build an integrated system for exchanging crime data, called the Information Technology-Based Integrated Criminal Justice System (SPPT-TI). SPPT-TI records the flow of crime incidents from the police to the prosecution service and courts and eventually the prison system. An integrated system among criminal justice institutions, SPPT-TI will facilitate the collaboration process, which BPS expects to be able to join in

order to monitor data quality, extract aggregated data to produce crime statistics and ensure that the data meet the Indonesia One Data principles.

Future plans

- Establish a memorandum of understanding between BPS and relevant criminal justice institutions. BPS is aiming to join the existing SPPT-TI collaboration in order to facilitate the sharing and exchange of crime data.
- Strengthen the collaboration between BPS and criminal justice institutions for producing more reliable crime statistics.
- Schedule regular meetings between BPS and relevant criminal justice institutions for following up on the implementation of SDSKI.
- Develop the SDSKI Dashboard as a platform for disseminating crime statistics.

Resources

Indonesia One Data portal:

<https://data.go.id/home>

Presidential Regulation Number 39 of 2019:

<https://peraturan.bpk.go.id/Details/108813/perpres-no-39-tahun-2019>

Republic of Korea: Korea Information System of Criminal Justice Services (KICS)

Based on an interview with the Ministry of Justice of the Republic of Korea

Description

Within the broader e-government approach of the Republic of Korea, KICS connects the various agencies involved in the criminal justice system, including the police, the prosecution service, the courts and the Ministry of Justice. KICS serves as a central repository for storing and managing data related to criminal investigations, prosecutions, court proceedings and offender management. The integrated IT system allows for the sharing of digital information on criminal cases between the criminal justice agencies. For information sharing and collaboration, the system enables authorized users from the different agencies to share information securely. KICS allows for the exchange of data, documents and messages related to investigations, court proceedings and corrections – promoting coordination and collaboration among the agencies. By facilitating the exchange of data and promoting interoperability, the system helps enhance the overall effectiveness and efficiency of the Korean criminal justice system.

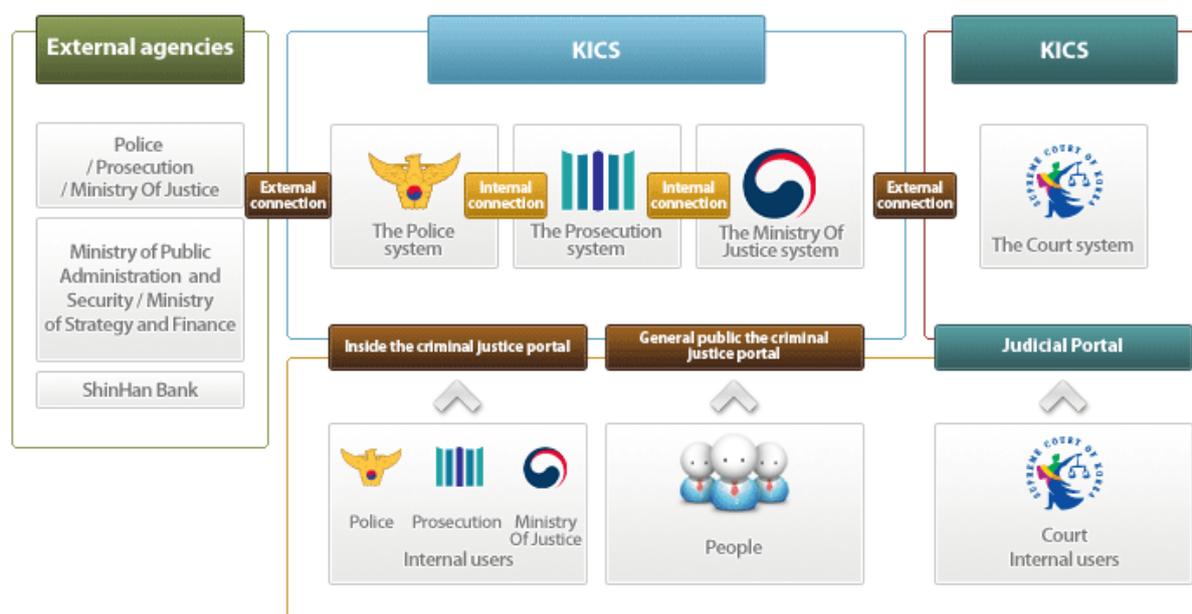
The development of KICS started in 2005, when the Government of the Republic of Korea recognized the need for an integrated information system to streamline and improve the management of criminal justice-related data across multiple agencies. The system was launched in 2010, with different modules and functionalities being added gradually. As technology advanced and new requirements emerged, KICS underwent updates and enhancements to meet the evolving needs of the Korean criminal justice system. The system was developed to digitalize the criminal justice system, which was paper-based prior to the implementation of KICS, with the objective of gaining efficiency and accuracy in all processes.

Prior to the implementation of KICS, prosecutors received paper case records from the police and each agency (prosecution service and courts) entered the information independently into their own case management system. Moreover, to search for information on cases or civil complaints, citizens and their representatives had to log into the system of each individual agency. KICS allowed for the creation of an integrated system that connected the different information systems, with significant efficiency gains for the agencies, citizens and society as a whole, for example, the substantial reduction of paper consumption.

The flow of information in KICS is mostly digital and shared between the different actors involved. An investigation typically starts at the police level, after which the case is transferred to the prosecution service. If a charge is filed, the case is transferred to the courts for trial and then sentencing is executed under the authority of Ministry of Justice.

As noted, KICS connects all four institutions within the criminal justice system, but also allows for integration with external agencies. Two types of external entities are currently connected to KICS: private companies, including mobile network operators, insurance companies and banks, from which the system obtains information that may be important for investigations; and other government or public institutions beyond the criminal justice system, including the Ministry of Finance, the Ministry of Labour and Employment, and the Ministry of Public Administration.

Figure 8 Structure of the Korean Information System of Criminal Justice Services (KICS)



Source: Ministry of Justice of the Republic of Korea. Available at <https://fgn.kics.go.kr/en/jsp/kics/structure.jsp>.

Note: This figure reflects the composition of KICS in September 2022. In November 2022, the Corruption Investigation Office for High-ranking Officials joined KICS.

In practice, each of the four agencies maintains its own IT system and operates its own server, meaning that the police have their digital system and operate a KICS server, while the other agencies do the same for their respective areas. In addition to these four systems, an integrated system has been built that enables the sharing of information in a secure manner among the different sub-systems.

A total of 394 types of information are used. The police provide 74 types of information, such as transfer reports and crime history data. The prosecution service provides 160 types of information, such as written arraignments, indictment decisions and various warrant claims. The courts provide 95 types of information, such as warrant issuance, trial date information and written judgments. Finally, the Ministry of Justice provides 65 types of information, such as details on imprisonment and information on probation.

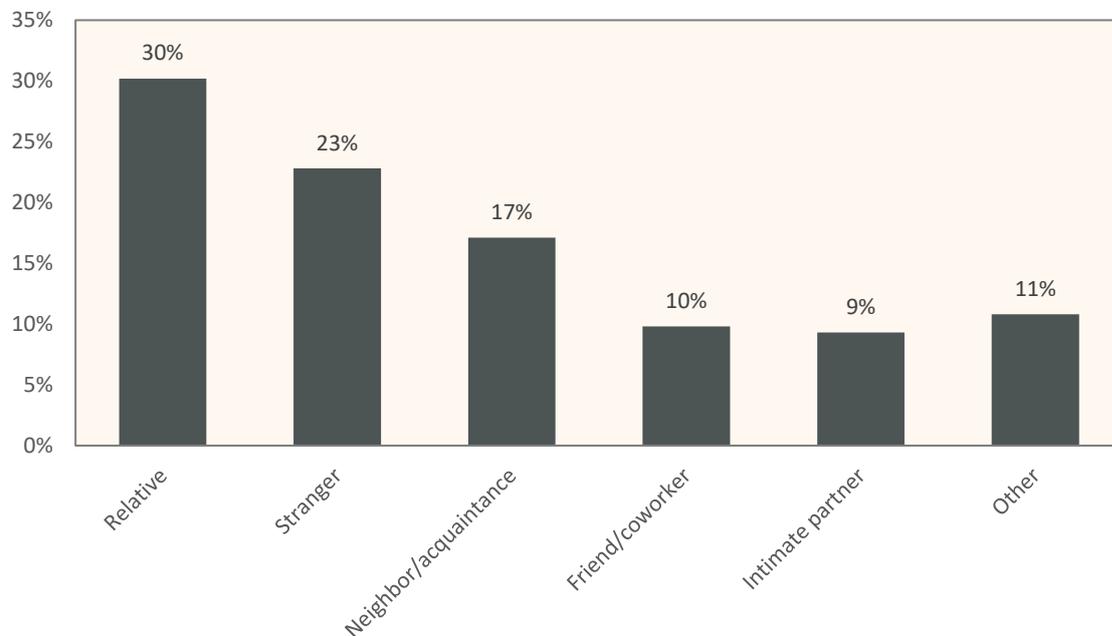
In addition to important cost savings, the system has improved services by acting as a one-stop-shop both for the involved agencies and citizens. The system can be used either through a mobile phone or computer. Three types of services are offered: searches (case search, penalty search, deposit refund search and criminal compensation payment search); civil affairs services (79 different types of service, including civil affairs filing, certificate issuance and courts records and notification); and crime victim support services.

Use of KICS by the Supreme Prosecutor's Office

The Supreme Prosecutor's office uses the administrative data generated in KICS to produce and disseminate statistical reports on a variety of topics related to crime analysis, crime trends and trends in criminal cases. Statistics available on the office's website include an analysis of the major crime types, such as homicide, robbery, sexual violence, arson, assault, theft and fraud. Figure 9 highlights some of the data related to intentional homicide collected in 2021, during which a total of 692 intentional homicides occurred. The available data are broken down by type of intentional homicide, time of occurrence, gender and age of both the victim and the offender, relationship between the

victim and offender, among others. Such detailed data can provide an improved understanding of the dynamics of major crime types, giving policymakers the evidence they need to design more effective policies and improve the safety of communities.

Figure 9 **Victim-perpetrator relationship in intentional homicide, Republic of Korea, 2021**
(Percent)



Source: Supreme Prosecutor’s Office, “Characteristics of each major crime type in 2021”, *Crime Analysis*. Available at <https://www.spo.go.kr/site/spo/crimeAnalysis.do>.

Challenges

The greatest challenge during the development process of KICS was to create consensus among the different institutions. The creation of coordination bodies and the development of legislative acts to enforce data sharing across different institutions were key factors in overcoming the limited level of cooperation prior to the implementation of KICS.

Coordination among the different criminal justice agencies takes place at two levels – senior management and technical. Comprised of senior managers, the Information Consultation Body meets twice a year and discusses future cooperation among the institutions. At the technical level, the establishment of the integrated Criminal Justice System Task Force helped steer the operational work. Responsible for providing the internal business process portals for each of the agencies, the task force is a permanent body with staff seconded from all participating institutions. The five-year period between the initiation of the project and the launch of KICS was crucial for reaching long-lasting agreements between the four agencies involved in the development of the system: the police, the prosecution service, the courts and the Ministry of Justice.

Another enabler of the system was legislation, which began with the Act on Promotion of the Digitalization of the Criminal Justice Process (originally enacted in 2008; Act No. 18653). This act was followed by other legislative developments, such as the Act on the Use of the Electronic Documents on the Summary Proceedings (originally enacted in 2010; Act No. 17354), together with memoranda of understanding between individual agencies. The most recent act to be enacted is the Act on the Use of Electronic Documents in Criminal Justice Procedures (originally enacted in 2021; Act No.

18485), the objective of which is to achieve 100 per cent digitalization of the processes of the criminal justice system.

Recommendations

This case study shows that securing strong commitment from top government officials is recommended. The development of KICS was part of a broader vision to develop the e-government system in the Republic of Korea that, together with strong leadership, was instrumental in creating institutional consensus and finding compromises among different institutions.

Way forward

Plans are in place to further develop KICS and funds have been secured for the Next-Generation Korea Information System of Criminal Justice Services (KICS) project. The objective is to increase trust in the criminal justice system among citizens and improve transparency and innovation in service provision on criminal justice. The detailed work plan highlights the following key improvements: the development of a remote video-conferencing system to serve investigations and an intelligent criminal justice assistant chat-bot; the expansion of the digitalization of criminal justice procedures, and the introduction of the mobile KICS application for agents operating in the field.

Resources

Korea Information System of Criminal Justice Services (KICS):

<https://www.kics.go.kr/> (Korean)

<https://fgn.kics.go.kr/en/> (English)

United Kingdom: Long-term strategic data vision

Based on an interview with the Ministry of Justice of the United Kingdom

The criminal justice statistical system of the United Kingdom is a paradigmatic case of a highly developed criminal justice statistical system. Showing the importance of a forward-looking approach that tries to anticipate future developments, this case study also depicts a complex criminal justice system that manages to generate high-quality statistics despite its complexity. As in many other Member States, the criminal justice system in the United Kingdom is highly decentralized, both territorially and at the institutional level. Additional complexity is created by the high demand for data from the public and information to be used in policymaking and research purposes. A partnership between different universities, financed by the Economic and Social Research Council, funds a project from a government department to link data from various public administrative registers. The objective of this project is to increase the use of administrative data for research and demonstrates the importance of data to society and the push for government to share data openly.

Description

Within the Ministry of Justice, there have been three important developments in the data landscape: i) intense work at the strategic level, ii) the implementation of concrete projects to improve access to and linking and dissemination of data, and iii) data infrastructure improvements.

At the strategic level, a data strategy has been recently developed for the Ministry of Justice. This was followed by the creation of a data strategy team and a Data Improvement Programme to enhance data governance across the criminal justice system. The Ministry employs roughly 600 staff who work directly with data (both operational and analytical data), but the programme is targeted at the entire 50,000 staff employed in the organization, including those in operational positions and strategic positions.

With external support, the programme has defined several stages in its advancement towards a data-driven organization with good data governance. The first stage is the discovery phase, for identifying the gaps in data governance, understanding the wider concepts, providing clarity on how the programme fits within the organization, and producing a list of potential solutions. The second stage is the alpha phase, for testing and refining the solutions in the real world with the objective of scaling them across the whole organization. The programme focuses on three key elements: i) the creation of an operating model to be implemented within the Ministry of Justice, which will define how to govern and manage data and metadata; ii) the definition of data stewardship roles; iii) the creation of a data catalogue and tools that define data quality standards and procedures.

The second development is the implementation of concrete projects that will help convince different parts of the criminal justice system to jointly improve data governance. Rather than comprehensive strategic developments, these are concrete projects with concrete outputs. One example is the Better Outcomes through Linked Data programme (BOLD) aimed at improving the connectedness of government data in England and Wales.¹⁰³ Thematically, the initial focus of BOLD was on reducing homelessness, supporting victims of crime, reducing substance misuse and reducing reoffending. Another example is the Data First project, a data-linking programme led by the Ministry of Justice and funded by Administrative Data Research UK (ADR UK). Data First is aimed at unlocking the potential of the wealth of data already recorded by the Ministry of Justice by linking administrative data sets from across the justice system and enabling accredited researchers from within government and academia to access the data in an ethical and responsible way.¹⁰⁴ Through Data First, the Ministry of Justice has developed a free and open-source software library, Splink, to enable data linkage.

The third development concerns data infrastructure and digital solutions. The digital strategy of the Ministry of Justice sets three key objectives: being more flexible, driven by data and led by users. One of the tools under development in response to the strategy is a data platform that is intended as a one-stop-shop for high-quality and well-governed data for the criminal justice system. Other IT solutions have been developed as part of successful projects mentioned above, such as Splink. At the same time, individual organizations within the Ministry of Justice have also worked on creating several solutions that could serve the institutions and citizens. The solutions catalogue contains several applications and IT tools that can be used freely.

In parallel to these three developments within the Ministry of Justice, there have also been strategic achievements at different levels of government. The police, for example, has created its own strategy to improve the experience of citizens and the use of digital solutions within the institution. At the same time, at the national level, there have been strategic developments in improving data governance and IT solutions more broadly, which comprise documents such as the National Data Strategy. One example, recently developed by the Central Digital and Data Office, is the Data Maturity Assessment for Government tool,¹⁰⁵ which is a voluntary self-assessment framework that helps public sector organizations to measure, improve and maintain the health and strength of their data ecosystems. Together with the framework, an informal data maturity group brings together different MDAs that meet regularly.

Challenges

The data revolution in the United Kingdom is affecting all organizations, both public and private. The Government is taking strategic and proactive steps at different levels, with successful projects that link data and develop IT solutions and applications useful to their staff and the public. The national strategy for a data-driven public sector is being developed while, simultaneously, organizations within the criminal justice system such as the Ministry of Justice, the police, the prosecution service and other MDAs are working on implementing their own strategic data-related plans.

The most important challenge, therefore, may be the coordination of the parallel efforts being undertaken both within the different MDAs of the criminal justice system and at the broader national level. Without such coordination, the process could result in different data governance models and interoperability standards across different criminal justice institutions. Moreover, if certain MDAs within the criminal justice system align with national efforts but others do not, interoperability within the sector will remain limited.

In an ideal world, strategic-level policy and guidance should be developed as the foundation for both national and sector-level data governance efforts prior to the development of concrete analytical and IT tools. In the United Kingdom, these two processes are partially running in parallel. There are positive elements to this approach, such as the buy-in effect that successful projects stimulate both among the staff and the public using them. This favours the inclusion of incremental changes in how data is used and governed, but there are also potential challenges related to this approach, not least regarding the creation of multiple parallel solutions and reduced efficiency.

Resources

National Data Strategy:

<https://www.gov.uk/government/publications/uk-national-data-strategy>

Central Digital and Data Office – Digital and Data Roadmap 2022-2025:

<https://www.gov.uk/government/publications/roadmap-for-digital-and-data-2022-to-2025>

Central Digital and Data Office – Data Maturity Assessment for Government:

<https://www.gov.uk/government/publications/data-maturity-assessment-for-government-framework>

Ministry of Justice – Digital Strategy 2025:

<https://www.gov.uk/government/publications/ministry-of-justice-digital-strategy-2025>

Ministry of Justice – Data First:

<https://www.gov.uk/guidance/ministry-of-justice-data-first>

Ministry of Justice – Better Outcomes through Linked Data (BOLD):

<https://www.gov.uk/government/publications/ministry-of-justice-better-outcomes-through-linked-data-bold>

Ministry of Justice – Splink:

<https://www.gov.uk/government/publications/joined-up-data-in-government-the-future-of-data-linking-methods/splink-mojs-open-source-library-for-probabilistic-record-linkage-at-scale>

National Policing Digital Strategy:

<https://pds.police.uk/national-policing-digital-strategy-2020/>

Results of the survey on criminal justice statistical systems

As part of the research for the present guidelines, a short survey was conducted among a limited number (17) of Member States that were invited to participate based on two criteria: i) geographical distribution and ii) UN-CTS submission record. The aim of the survey was to collect information on the functioning of criminal justice statistical systems in different Member States. Administered online to representatives of the institutions that are responsible for the production of crime and criminal justice statistics, the survey was completed by 41 respondents in the 17 countries (Albania, Argentina, Belgium, Ecuador, Estonia, Finland, Italy, Kenya, Lithuania, Mauritius, Mexico, Morocco, Philippines, Republic of Korea, Slovenia, United Kingdom, United States). The data were collected between April and June 2023. The questionnaire was split into two sections: one section for central reporting agencies (National Statistical Office, Ministry of Justice, etc.); another section for reporting institutions (the police, the prosecution service, the courts and the prison system). Selected results from the survey are presented below.

Table 10 Number of survey participants, by country

<i>Country</i>	<i>Participants</i>
Albania	1
Argentina	7
Belgium	2
Ecuador	4
Estonia	1
Finland	5
Italy	3
Kenya	1
Lithuania	4
Mauritius	1
Mexico	1
Morocco	1
Philippines	5
Republic of Korea	1
Slovenia	2
United Kingdom	1
United States	1
Total	41

The survey results indicate that the institutional setting for the production of crime and criminal justice statistics is typically well established. Respondents in 12 of the 17 countries reported that legislation is in place in their countries that outlines the roles and responsibilities for the production and use of administrative data on crime and criminal justice, including how access to such data can be controlled.

In addition, respondents in 10 countries indicated the existence of an active national statistics council, board or committee that meets regularly to discuss the production of official statistics related to crime and criminal justice. However, respondents in five countries indicated that although legislation exists, it requires updating.

Most respondents indicated that the general statistical system is either partially or fully decentralized and typically includes a coordination mechanism/authority for effective collaboration. The statistical system is centrally organized around a single national office responsible for all types of statistics in only one of the countries. Respondents in seven countries indicated that a formal data governance framework on crime and criminal justice data is in place, while respondents in four countries indicated that no data governance framework exists at all.

Collaboration between the central institution in charge of producing statistics on crime and criminal justice and the data providers tends to be well developed in the countries responding to the questionnaire. Only one country indicated that there is little cooperation between the institutions involved, leading to the duplication of work, errors in statistics and incomplete analyses. Respondents in all the other countries indicated that either formal or informal collaboration mechanisms are in place between the institutions, resulting in regular meetings and open communication about data.

Despite the high degree of collaboration, the technical integration of IT systems and related protocols remains limited in most of the countries. Respondents from the central reporting agency in just five countries indicated that information-sharing protocols are in place between the institutions involved and data are shared electronically. Often data are compiled and exchanged manually, in part because of inadequate IT systems that prevent the automatic linking and exchange of data (see Table 11).

Table 11 Level of technical interoperability

	<i>Frequency</i>	<i>Percentage</i>
Yes, IT systems were developed to ensure full integration of the police, prosecution, courts and prison/correction database systems.	4	24
IT systems were developed independently of one another and at different times, making integration impossible. However, data are transferred from each institution to the central reporting facility through a software interface that recognizes different codes for extracting relevant data, linking the databases.	5	29
None of the IT systems are linked. Some data may be exchanged but they are compiled and transferred manually.	8	47

Note: Distribution of responses to the question “Are data directly accessible through linkages or integration of database systems across different departments and/or agencies?”.

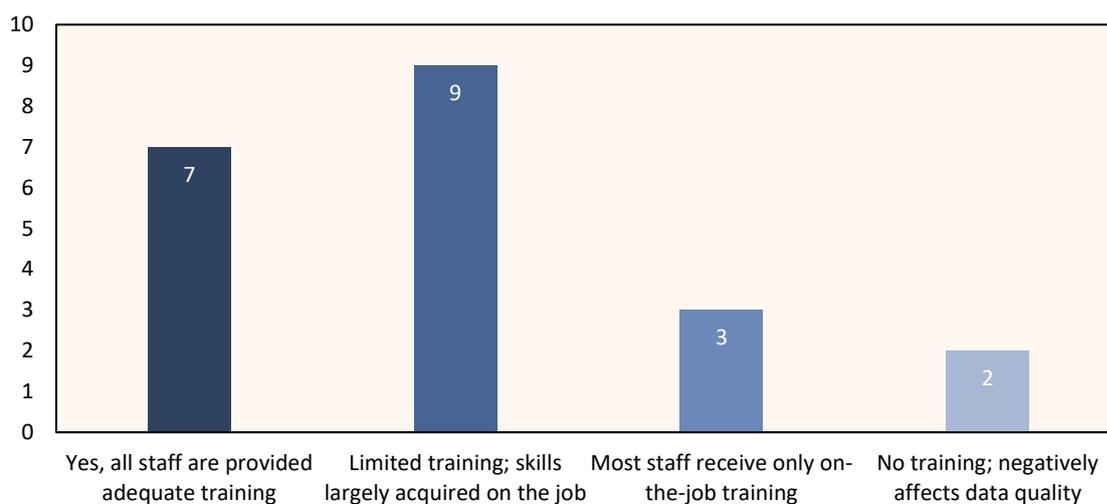
Moreover, respondents from the central reporting authority in seven countries indicated that the system is still (partially) paper based. It is quite common for local offices to continue to use paper records that are sent to regional offices that have intranet or web-/cloud-based electronic systems for inputting the data, which can be viewed at the national office. Records from local offices are scanned or entered electronically at the regional office and sent to the national office, often relying on a web-/cloud-based platform for transfer.

Most respondents indicated that demand for crime and criminal justice data is quite high, with key staff using data to determine whether targets and goals have been achieved and researchers regularly requesting anonymized raw (micro) data. Moreover, respondents indicated that administrative data on crime and criminal justice are used to inform planning (for example, allocation of resources based

on needs) and strategic decision-making (for example, development of new specialized units based on trends) at the local, district, state, regional and national levels. Although the data are typically produced at a monthly frequency, in some cases this only occurs once a quarter or once a year.

At the level of the reporting institutions, most respondents indicated that the level of training received by staff responsible for data is not entirely sufficient. Many respondents indicated that staff receive some training, but most of the relevant skills are either picked up on the job or staff members simply never learn them. This can differ between the different reporting institutions within a single country, however.

Figure 10 Adequacy of staff training



Note: Distribution of responses to the question “Do the staff at the central reporting facility who are responsible for data extraction, coding, organization and analysis (where relevant) receive adequate training to carry out their functions?”.

The availability of supplies and equipment such as forms, pens, phones and computers is generally judged adequate, with respondents in only four countries indicating the unavailability of such supplies to be a serious constraint. Moreover, a lack of a basic ICT infrastructure with stable internet service does not pose a major challenge according to most respondents.

A major constraint to data standardization in many countries seems to be a lack of written codebooks with a single definition for each data variable and specifications for data collection methods, codes, transmission and use. Respondents in only half of the countries indicated that such codebooks exist and can be found in each institution/office/court/department at the local, district, state, regional and national levels. In the other countries, such codebooks either do not exist or can only be found at the national level.

The three most critical constraints identified both by central reporting authorities and reporting institutions in the production of statistical data on crime and criminal justice are the number of professional staff available, the technical skills of available staff, and the availability of software solutions. By contrast, respondents indicated being least concerned about the demand for statistics and their use for planning purposes.

UNODC would like to express gratitude to all respondents for taking the time to complete the survey. Their responses were used to structure the present *Guidelines for the Governance of Statistical Data in the Criminal Justice System* and identify some of the key issues that needed to be covered.

End notes

- ¹ United Nations, “Report of the United Nations Office on Drugs and Crime and the National Institute of Statistics and Geography of Mexico on Crime and Criminal Justice Statistics,” E/CN.3/2022/14 (United Nations Statistical Commission, 2022).
- ² Ibid.
- ³ United Nations, *Manual for the Development of a System of Criminal Justice Statistics*, Studies in Methods, Series F No. 89 (United Nations publication, 2003).
- ⁴ “Kyoto Declaration on Advancing Crime Prevention, Criminal Justice and the Rule of Law: Towards the Achievement of the 2030 Agenda for Sustainable Development” (United Nations publication, 2021).
- ⁵ United Nations, *United Nations National Quality Assurance Frameworks Manual for Official Statistics*, Series M, No. 100 (United Nations publication, 2019).
- ⁶ United Nations, *Manual for the Development of a System of Criminal Justice Statistics*.
- ⁷ Based on United Nations, *United Nations National Quality Assurance Frameworks Manual for Official Statistics*; United Nations, *The Handbook on Management and Organization of National Statistical Systems*, 4th ed. (United Nations publication, 2022).
- ⁸ United Nations, *Manual on Victimization Surveys* (United Nations publication, 2010).
- ⁹ United Nations Office on Drugs and Crime, *Guidelines for the Production of Statistical Data by the Police* (United Nations publication, 2022).
- ¹⁰ *The Status and Role of Prosecutors—A United Nations Office on Drugs and Crime and International Association of Prosecutors Guide*, Criminal Justice Handbook Series (United Nations publication, 2014).
- ¹¹ United Nations Office on Drugs and Crime, *Guidelines for the Production of Statistical Data by the Prosecution Service and the Courts* (United Nations publication, 2023).
- ¹² United Nations Office on Drugs and Crime, *Guidelines for the Production of Statistical Data by the Prison System* (United Nations publication, 2023).
- ¹³ Based on United Nations, *Manual for the Development of a System of Criminal Justice Statistics*.
- ¹⁴ United Nations, *The Handbook on Management and Organization of National Statistical Systems*.
- ¹⁵ Australian Bureau of Statistics, “Crime and Justice,” accessed August 10, 2023, <https://www.abs.gov.au/statistics/people/crime-and-justice>.
- ¹⁶ United Nations, *The Handbook on Management and Organization of National Statistical Systems*.
- ¹⁷ United Nations, *Fundamental Principles of Official Statistics*, A/RES/68/261, 2014.
- ¹⁸ Based on United Nations, *Manual for the Development of a System of Criminal Justice Statistics*.
- ¹⁹ United Nations, *United Nations National Quality Assurance Frameworks Manual for Official Statistics*.
- ²⁰ United Nations Statistics Division, “Collaborative on the Use of Administrative Data for Statistics,” accessed July 18, 2023, <https://unstats.un.org/capacity-development/admin-data/>.
- ²¹ UNODC-INEGI Center of Excellence in Statistical Information on Government, Crime, Victimization and Justice, “El Sistema de Gestión de Seguridad Pública (SGSP) Del Ministerio Del Interior de La República Oriental Del Uruguay,” Publication Series on Good Practices for Statistical Quality (Mexico, 2021), <https://www.cdeunodc.inegi.org.mx/unodc/wp-content/uploads/2021/04/SGSP-Uruguay-web.pdf>.
- ²² Task Force on Data Stewardship, “Data Stewardship and the Role of National Statistical Offices in the New Data Ecosystem,” ECE/CES/2023/2 (Conference of European Statisticians, 2023).
- ²³ Luis Gerardo González Morales and Tom Orrell, *Data Interoperability: A Practitioner’s Guide to Joining up Data in the Development Sector* (2018).
- ²⁴ United Nations, *The Handbook on Management and Organization of National Statistical Systems*.
- ²⁵ European Commission, *European Interoperability Framework – Implementation Strategy*, COM/2017/0134 final, 2017.
- ²⁶ United Nations, *Manual for the Development of a System of Criminal Justice Statistics*.
- ²⁷ Organisation for Economic Co-operation and Development, *The Path to Becoming a Data-Driven Public Sector* (OECD, 2019); Task Force on Data Stewardship, “Data Stewardship and the Role of National Statistical Offices in the New Data Ecosystem.”
- ²⁸ World Bank, *World Development Report 2021: Data for Better Lives* (World Bank, 2021).
- ²⁹ Ireland, “Criminal Justice Sectoral Strategy 2022-2024,” accessed November 24, 2023, <https://www.gov.ie/en/publication/ca8bf-criminal-justice-sectoral-strategy-2022-2024>.
- ³⁰ Paris21, “Guidelines for National Strategy for the Development of Statistics (NSDS),” accessed November 29, 2023, <https://new.nsdsguidelines.paris21.org/>.

-
- ³¹ United Kingdom, “National Data Strategy,” accessed July 20, 2023, <https://www.gov.uk/guidance/national-data-strategy>.
- ³² United Kingdom, “Ministry of Justice Digital Strategy 2025,” accessed July 20, 2023, <https://www.gov.uk/government/publications/ministry-of-justice-digital-strategy-2025>.
- ³³ United Kingdom, “National Policing Digital Strategy – Police Digital Service,” accessed July 20, 2023, <https://pds.police.uk/national-policing-digital-strategy-2020/>.
- ³⁴ Colombia, Instituto Nacional de Estadística y Censos, “Comisión de Seguridad Justicia Crimen y Transparencia,” accessed July 19, 2023, <https://www.ecuadorencifras.gob.ec/comision-de-seguridad-justicia-crimen-y-transparencia/>.
- ³⁵ Organisation for Economic Co-operation and Development, *Digital Government Review of Argentina: Accelerating the Digitalisation of the Public Sector*, OECD Digital Government Studies (OECD, 2019).
- ³⁶ David Plotkin, *Data Stewardship: An Actionable Guide to Effective Data Management and Data Governance*, Second edition (Academic Press, 2020).
- ³⁷ Task Force on Data Stewardship, “Data Stewardship and the Role of National Statistical Offices in the New Data Ecosystem.”
- ³⁸ Diane Robinson and Sarah Gibson, “Data Governance Policy Guide” (National Center for State Courts, 2019).
- ³⁹ United Nations, *Fundamental Principles of Official Statistics*.
- ⁴⁰ United Nations, *The Handbook on Management and Organization of National Statistical Systems*.
- ⁴¹ Based on chapter 4 of Organisation for Economic Co-operation and Development, *The Path to Becoming a Data-Driven Public Sector*.
- ⁴² United Nations Economic Commission for Europe, *Generic Law on Official Statistics for Eastern Europe, Caucasus and Central Asia* (United Nations publication, 2016); United Nations Economic Commission for Latin America and the Caribbean, *Generic Law on Official Statistics for Latin America* (United Nations publication, 2020); United Nations Economic and Social Commission for Western Asia, *Generic Law for Official Statistics in the Arab Countries* (United Nations publication, 2021).
- ⁴³ Mexico, Instituto Nacional de Estadística y Geografía, “INEGI - About us,” accessed July 21, 2023, <https://en.www.inegi.org.mx/inegi/contenido/instituto.html>.
- ⁴⁴ Mexico, Sistema Nacional de Información Estadística y Geográfica, “Sesiones inductivas al SNIEG,” accessed August 9, 2023, <https://www.snieg.mx/sesiones-inductivas/>.
- ⁴⁵ United Nations, *Fundamental Principles of Official Statistics*.
- ⁴⁶ United Nations, *The Handbook on Management and Organization of National Statistical Systems*.
- ⁴⁷ The European Parliament and the Council of the European Union, “Directive (EU) 2016/680 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data” (2016), <https://data.europa.eu/eli/dir/2016/680/oj/eng>.
- ⁴⁸ Commission nationale de l’informatique et des libertés, “CNIL,” accessed August 21, 2023, <https://www.cnil.fr/fr/particulier>.
- ⁴⁹ Personal Data Protection Commission, “PDPC,” accessed August 21, 2023, <https://www.pdpc.gov.sg/>.
- ⁵⁰ Amelia Bleeker and Abdullahi Abdulkadri, “A Review of Caribbean National Statistical Legislation in Relation to the United Nations Fundamental Principles of Official Statistics,” *Studies and Perspectives* (United Nations Economic Commission for Latin America and the Caribbean, 2020).
- ⁵¹ Organisation for Economic Co-operation and Development, *The Path to Becoming a Data-Driven Public Sector*.
- ⁵² United Nations, *The Handbook on Management and Organization of National Statistical Systems*.
- ⁵³ President of the Dominican Republic, “Decreto 645-21 Sistema Nacional de Seguridad Ciudadana,” Pub. L. No. 645–21 (2021), <https://mip.gob.do/wp-content/uploads/marcolegal/Decretos/DECRETO%20645-21%20que%20crea%20el%20Sistema%20Nacional%20de%20Seguridad%20Ciudadana%20.pdf>.
- ⁵⁴ CADSECI, “Centro de Análisis de Datos de La Seguridad Ciudadana,” accessed December 6, 2023, <https://cadseci.gob.do/index.php/en/>.
- ⁵⁵ Open SDG, “Open SDG,” accessed August 21, 2023, <https://open-sdg.org/>.
- ⁵⁶ United Kingdom, “U.K. Indicators For The Sustainable Development Goals,” accessed August 21, 2023, <https://sdgdata.gov.uk/>.
- ⁵⁷ For details on MoUs, see for instance the UNSD guide on memoranda of understanding for coordination and cooperation (2021), <https://unstats.un.org/UNSDWebsite/capacity-development/admin-data/tools/mou>.

-
- ⁵⁸ This is the case, for instance, of the province of Santa Cruz, which provides local statistics (<http://www.policiaedesantacruz.gob.ar/index.php/es/servicios/estadisticas>) on crime and criminal justice that complement the national statistical platform (<https://www.argentina.gob.ar/seguridad/estadisticascriminales>).
- ⁵⁹ Collaborative on Administrative Data, “Guidance and Template for Developing a Memorandum of Understanding” (United Nations Statistics Division, 2022). Available at https://unstats.un.org/UNSDWebsite/resourceCatalog/documents/MoUGuidelines_v5_EN.pdf.
- ⁶⁰ This section is based on United Nations, *The Handbook on Management and Organization of National Statistical Systems*.
- ⁶¹ See, for example, United Nations Statistics Division, “Expert Group on International Statistical Classifications,” accessed October 17, 2023, <https://unstats.un.org/unsd/classifications/expertgroup/>; United Nations Statistics Division, “List of International and Multinational Classifications,” accessed October 17, 2023, <https://unstats.un.org/unsd/classifications/Family/ListByName>.
- ⁶² González Morales and Orrell, “Data Interoperability: A Practitioner’s Guide to Joining up Data in the Development Sector.”
- ⁶³ United Nations, *The Handbook on Management and Organization of National Statistical Systems*.
- ⁶⁴ Ibid.
- ⁶⁵ González Morales and Orrell, “Data Interoperability: A Practitioner’s Guide to Joining up Data in the Development Sector.”
- ⁶⁶ United Nations, *Fundamental Principles of Official Statistics*.
- ⁶⁷ United Nations, *The Handbook on Management and Organization of National Statistical Systems*.
- ⁶⁸ United States Department of Justice, “National Incident-Based Reporting System User Manual,” accessed November 24, 2023, <https://le.fbi.gov/file-repository/nibrs-user-manual.pdf/view>.
- ⁶⁹ United States Department of Justice, Federal Bureau of Investigation, “Effects of NIBRS on Crime Statistics,” accessed October 17, 2023, https://ucr.fbi.gov/nibrs/2014/resource-pages/effects_of_nibrs_on_crime_statistics_final.pdf.
- ⁷⁰ Based on Chapter 14 of United Nations, *The Handbook on Management and Organization of National Statistical Systems*.
- ⁷¹ Government of India, “Interoperable Criminal Justice System,” accessed November 27, 2023, <https://static.pib.gov.in/WriteReadData/specificdocs/documents/2022/jun/doc202262367401.pdf>.
- ⁷² IBM, “What Is ETL (Extract, Transform, Load)?,” accessed November 17, 2023, <https://www.ibm.com/topics/etl>.
- ⁷³ United Nations, *The Handbook on Management and Organization of National Statistical Systems*.
- ⁷⁴ Brian A. Harris-Kojetin and Constance F. Citro, eds., *Principles and Practices for a Federal Statistical Agency: Seventh Edition* (Washington, D.C.: National Academies Press, 2021), <https://doi.org/10.17226/25885>.
- ⁷⁵ International Organization for Migration (IOM) and United Nations Office on Drugs and Crime (UNODC), “Making Each Case Count: Leveraging Administrative Data on Trafficking in Persons,” 2023, https://www.unodc.org/documents/data-and-analysis/tip/2023/Making_each_case_count_Sep-19.pdf.
- ⁷⁶ Patrik Hummel et al., “Data Sovereignty: A Review,” *Big Data & Society* 8, no. 1 (January 1, 2021): 2053951720982012, <https://doi.org/10.1177/2053951720982012>.
- ⁷⁷ “The First Nations Information Governance Centre,” The First Nations Information Governance Centre, accessed December 6, 2023, <https://fnigc.ca/>.
- ⁷⁸ Argentina, “Estadísticas criminales de la República Argentina,” accessed August 9, 2023, <https://www.argentina.gob.ar/seguridad/estadisticascriminales>.
- ⁷⁹ United States, Department of Justice, Bureau of Justice Statistics, “Data Analysis Tools,” accessed October 17, 2023, <https://bjs.ojp.gov/data/data-analysis-tools>.
- ⁸⁰ United States, Federal Bureau of Investigation, “Crime Data Explorer,” accessed August 9, 2023, <https://cde.ucr.cjis.gov/>.
- ⁸¹ Statistics Norway, “Offences and Victims Reported to the Police,” accessed August 9, 2023, <https://www.ssb.no/en/statbank/table/08631>.
- ⁸² Instituto Nacional de Estadística y Geografía (INEGI), “Censo Nacional de Impartición de Justicia Estatal 2023,” accessed December 4, 2023, <https://www.inegi.org.mx/programas/cnije/2023/>.
- ⁸³ For instance, see European Union, “European Union Agency for Cybersecurity,” accessed November 24, 2023, <https://www.enisa.europa.eu>; United Kingdom, “National Cyber Security Centre,” accessed November 24, 2023, <https://www.ncsc.gov.uk/>; United States, “Cybersecurity & Infrastructure Security Agency,” accessed November 24, 2023, <https://www.cisa.gov/>.

-
- ⁸⁴ IEC, “International Electrotechnical Commission,” accessed November 24, 2023, <https://www.iec.ch/homepage>; “ISO/IEC 27001 Standard – Information Security Management Systems,” ISO, accessed November 24, 2023, <https://www.iso.org/standard/27001>.
- ⁸⁵ United Nations, *Fundamental Principles of Official Statistics*.
- ⁸⁶ United Nations, *United Nations Guide on Privacy-Enhancing Technologies for Official Statistics*, United Nations Committee of Experts on Big Data and Data Science for Official Statistics (New York, 2023).
- ⁸⁷ Joint Task Force Interagency Working Group, “Security and Privacy Controls for Information Systems and Organizations,” Revision 5 (National Institute of Standards and Technology, September 23, 2020), <https://doi.org/10.6028/NIST.SP.800-53r5>.
- ⁸⁸ National Cyber Security Centre, “Architecture and Configuration,” accessed November 24, 2023, <https://www.ncsc.gov.uk/collection/10-steps/architecture-and-configuration>.
- ⁸⁹ IBM, “What Is Network Security?,” accessed October 18, 2023, <https://www.ibm.com/topics/network-security>.
- ⁹⁰ National Cyber Security Centre, “Introduction to Zero Trust,” accessed October 18, 2023, <https://www.ncsc.gov.uk/collection/zero-trust-architecture/introduction-to-zero-trust>.
- ⁹¹ “ISO/IEC 18033 - Information Security and Encryption Algorithms,” ISO, accessed November 24, 2023, <https://www.iso.org/standard/76156.html>.
- ⁹² National Cyber Security Centre, “Device Security Guidance,” accessed November 24, 2023, <https://www.ncsc.gov.uk/search>.
- ⁹³ United Nations, *United Nations National Quality Assurance Frameworks Manual for Official Statistics*; Eurostat, ed., *European Statistics Code of Practice* (Luxembourg: Publications Office of the European Union, 2018), <https://doi.org/10.2785/914491>.
- ⁹⁴ Open Data Charter, “Principles,” accessed August 3, 2023, <https://opendatacharter.net/principles/>.
- ⁹⁵ Organisation for Economic Co-operation and Development, *Digital Government Review of Argentina: Accelerating the Digitalisation of the Public Sector*.
- ⁹⁶ Statistics Netherlands, “Free and Open-Source Software at Statistics Netherlands,” ECE/CES/2023/20 (Conference of European Statisticians, 2023).
- ⁹⁷ Statistics Poland, “Open-Source Solutions at Statistics Poland,” ECE/CES/2023/22 (Conference of European Statisticians, 2023).
- ⁹⁸ Resolution No. 102-DIRG-2010 of 24 June 24, 2010.
- ⁹⁹ Official Letter No. DPR-011-0024 of 28 March 2011.
- ¹⁰⁰ Resolution No. 124- DIRG-2011 of 29 July 2011.
- ¹⁰¹ Resolution No. 005-DIREJ-DIJU-NT-2019 of 4 February 2019.
- ¹⁰² Members of the Strategic Group: Security Sector Council, Habitat, Infrastructure and Natural Resources Sector Council, SENPLADES, MDI, CPCCS, MTOP, ECU 911, ANT and INEC.
- ¹⁰³ United Kingdom, Ministry of Justice, “Better Outcomes through Linked Data (BOLD),” GOV.UK, November 15, 2023, <https://www.gov.uk/government/publications/ministry-of-justice-better-outcomes-through-linked-data-bold>.
- ¹⁰⁴ United Kingdom, Ministry of Justice, “Ministry of Justice: Data First,” accessed August 9, 2023, <https://www.gov.uk/guidance/ministry-of-justice-data-first>.
- ¹⁰⁵ United Kingdom, Ministry of Justice, Central Digital and Data Office, “Data Maturity Assessment for Government: Framework,” GOV.UK, accessed December 8, 2023, <https://www.gov.uk/government/publications/data-maturity-assessment-for-government-framework>.



UNODC

United Nations Office on Drugs and Crime