EL -RAKHAWI DOCTRINE: THE GLOBAL ENCYCLOPEDIA OF CIVIL LEGAL REGULATION FOR THE PROTECTION OF BIOMETRIC DATA

A Comprehensive Comparative Study between Arab, European, and American Legal Systems

Digital Object Identifier: 10.5281/zenodo.21588771

Author: Dr. Mohamed Kamal Arafa Elrakhawi
Independent Researcher and Legal Consultant
International Lecturer in Law and Distinguished Jurist

Date of Publication: July 26, 2026

Academic Classification: Civil Law, Data Protection Law, Biometric Privacy, Comparative Jurisprudence, Digital Identity Regulation

COPYRIGHT AND INTELLECTUAL PROPERTY RIGHTS

ENHANCED DEDICATION

This monumental encyclopedia is dedicated to the pure souls of my parents, the beacon of honor, Kamal Arafa Hassan Elrakhawi, and the lady of wisdom and resilience, Feriel Abdel Azim Mohamed Zayed, whose names are eternally etched in my heart. They taught me that the sanctity of the human being is not merely a legal concept, but a sacred covenant of dignity, identity, and unwavering moral clarity. In an age where the very essence of human identity is being reduced to digital data points, this work stands as a testament to their enduring wisdom that the human person, in all their physical and spiritual uniqueness, must remain inviolable. May this encyclopedia serve as a lasting continuous charity, elevating their souls in the highest paradises, and proving to the world that the Egyptian legal and intellectual mind, rooted in authentic values, can illuminate the path of biometric data protection with originality, depth, and moral courage. This work is their monument, their voice echoing through the corridors of global

jurisprudence, and their eternal triumph over the reduction of human dignity to mere algorithmic processing.

PREFACE: THE EL RAKHAWI MESSAGE ON BIOMETRIC DIGNITY

To the global legal community, to judges who seek truth, to lawyers who defend dignity, to researchers who pursue knowledge, and to students who aspire to mastery:

This work is not merely a book. It is a message. A message that biometric data is not a commodity to be traded, but the digital mirror of the human soul. A message that in an age of artificial intelligence, deepfakes, and mass surveillance, the civil legal protection of biometric data has become the last frontier of human dignity. A message that the Egyptian legal mind, rooted in the wisdom of centuries and open to the challenges of tomorrow, has the capacity to contribute to the global legal discourse with originality and depth.

The El Rakhawi Message is built upon three foundational principles:

First, the principle of biometric inviolability. The human face, fingerprint, iris pattern, voice, and gait are not mere data points but the physical manifestation of human uniqueness. Any legal framework that treats them as ordinary personal data fails to grasp their existential significance.

Second, comparative rigor without ideological bias. We examine the Arab legal systems, the European Union framework, the American common law tradition, and emerging global standards not to declare one superior, but to extract the best practices that serve human dignity and technological progress.

Third, practical relevance over theoretical abstraction. Every chapter answers a real question faced by practitioners: What constitutes valid consent for biometric data collection? Who bears liability when biometric data is breached? How do we protect the biometric data of minors and the deceased? What are the legal implications of deepfakes and synthetic biometric identities?

This message is dedicated to the pursuit of legal excellence, to the advancement of biometric privacy jurisprudence, and to the belief that law, when properly understood and applied, is the greatest instrument of human dignity preservation in the digital age.

EXECUTIVE SUMMARY

The civil legal regulation of biometric data represents one of the most complex and urgent fields of modern legal practice. With the exponential growth of biometric technologies, the emergence of artificial intelligence, and the increasing sophistication of cyber threats, practitioners face unprecedented challenges that demand a comprehensive, comparative, and forward-looking approach.

The El Rakhawi Doctrine: The Global Encyclopedia of Civil Legal Regulation for the Protection of Biometric Data addresses these challenges through forty meticulously researched chapters organized across four core parts. The work moves from the conceptual foundations of biometric data, through the comparative analysis of major legal systems, to the emerging frontiers of artificial intelligence, blockchain, and global governance.

The work is distinguished by several unique features:

First, it provides the first comprehensive functional comparison between the Arab legal systems, the European Union framework, the American common law tradition, and emerging global standards for biometric data protection.

Second, it introduces several groundbreaking jurisprudential concepts, including the El Rakhawi Principle of Sovereign Biometric Dignity, the Theory of Semantic Biometric Encryption, the concept of Cognitive Biometric Sovereignty, and the Doctrine of Dynamic Informed Consent for Biometric Data Processing.

Third, it addresses contemporary challenges that have received insufficient attention in existing literature, including post-mortem biometric data protection, the biometric data of minors and vulnerable populations, the intersection of biometric data and generative AI, and emergency biometric data collection during pandemics.

Fourth, it provides a forward-looking analysis of emerging issues such as self-sovereign biometric identity in the blockchain era, the digital biometric footprint, international cyber sovereignty and biometric data flows, and the metaphysical dimensions of biometric data protection.

This work is designed to serve as both a comprehensive reference for practitioners and a foundational text for academic study. It is written with the precision required by legal professionals and the clarity necessary for students approaching this complex field for the first time.

TABLE OF CONTENTS

METHODOLOGICAL FRAMEWORK

This encyclopedia employs a functional comparative methodology that transcends the limitations of traditional comparative law. Rather than merely juxtaposing legal texts from different jurisdictions, we analyze how each legal system addresses the same practical problem arising from biometric data protection, identifying convergences, divergences, and best practices.

The methodology is built upon four pillars:

First, doctrinal analysis of primary legal sources, including statutes, regulations, and judicial decisions from Arab countries, the European Union, the United States, and the United Kingdom.

Second, case study methodology that examines landmark judicial decisions to extract practical principles and identify emerging trends in biometric data litigation.

Third, functional analysis that evaluates legal rules based on their effectiveness in achieving their stated objectives, including human dignity preservation, technological innovation facilitation, and cybersecurity enhancement.

Fourth, forward-looking assessment that anticipates future challenges and proposes comprehensive legislative reforms to address them.

Each chapter follows a consistent structure: introduction to the legal issue, comparative analysis across jurisdictions, examination of judicial practice, identification of gaps and challenges, and practical recommendations. This structure ensures that the work serves both as a comprehensive academic reference and as a practical guide for legal practitioners navigating the complexities of biometric data protection.

PART ONE: THE CONCEPTUAL FOUNDATIONS OF BIOMETRIC DATA PROTECTION

CHAPTER 1: THE CONCEPT OF BIOMETRIC DATA IN CONTEMPORARY CIVIL LAW

The concept of biometric data has undergone a revolutionary transformation in contemporary civil law, evolving from a mere technical tool for identification to a fundamental component of human dignity and personal sovereignty. In an age where the human being is increasingly reduced to digital data points, the legal conceptualization of biometric data has become the last frontier of civil protection.

Biometric data is defined as any information relating to the physical, physiological, or behavioral characteristics of a natural person that allows or confirms the unique identification of that natural person. This definition encompasses fingerprints, facial recognition patterns, iris scans, voice prints, gait analysis, DNA profiles, and any other biometric identifier that can be used to establish the identity of an individual.

The civil law conceptualization of biometric data raises fundamental questions about the nature of human identity in the digital age. Is biometric data merely a subset of personal data, subject to the same legal regime as name, address, or email? Or does it represent a distinct category of data that requires special protection due to its intimate connection with human identity and dignity?

The European Union has taken the position that biometric data constitutes a special category of personal data, subject to enhanced protection under Article 9 of the General Data Protection Regulation (GDPR). This position recognizes that biometric data is not merely information about a person, but information that is constitutive of the person's unique identity.

The American approach, by contrast, has been more fragmented, with different states adopting different levels of protection. The Illinois Biometric Information Privacy Act (BIPA) of 2008 represents one of the most comprehensive state-level protections, requiring informed consent before the collection of biometric data and providing a private right of action for violations.

The Arab legal systems have been slower to develop comprehensive biometric data protection frameworks, with most countries relying on general personal data protection laws or constitutional provisions on privacy. However, recent developments in countries such as Egypt, Saudi Arabia, and the United Arab Emirates indicate a growing recognition of the need for specialized biometric data protection.

The conceptual foundation of biometric data protection must be rooted in the recognition that biometric data is not a commodity to be traded, but the digital mirror of the human soul. Any legal framework that fails to grasp this existential significance will inevitably fail to protect the fundamental dignity of the human person in the digital age.

CHAPTER 2: THE HISTORICAL EVOLUTION OF PROTECTION FROM PAPER IDENTITY TO BIOMETRIC DATA

The historical evolution of identity protection provides essential context for understanding the contemporary challenges of biometric data protection. From the earliest forms of paper identification to the sophisticated biometric systems of today, the legal conceptualization of identity has undergone a profound transformation.

The paper identity emerged in the nineteenth century as a response to the increasing mobility of populations and the need for reliable identification. Paper identity documents, such as passports, birth certificates, and national identity cards, represented the first attempt to create a legal framework for personal identification. However, these documents were vulnerable to forgery, loss, and theft, and their reliability was often questionable.

The transition from paper identity to digital identity began in the late twentieth century with the advent of computer technology and the internet. Digital identity documents, such as electronic passports and national identity cards with embedded chips, offered greater security and reliability than their paper counterparts. However, they also raised new concerns about privacy, surveillance, and the potential for mass data collection.

The emergence of biometric identity in the twenty-first century represents a quantum leap in the evolution of identity protection. Biometric systems, which use unique physical or behavioral characteristics to identify individuals, offer unprecedented levels of accuracy and security. However, they also raise fundamental questions about the nature of human identity and the limits of state and corporate power over the human person.

The historical evolution of identity protection reveals a recurring tension between the need for reliable identification and the imperative of protecting individual privacy and dignity. This tension has been present in every stage of the evolution, from the earliest paper identity documents to the most sophisticated biometric systems of today.

The lesson of history is that identity protection must be rooted in the recognition of human dignity as the foundation of all legal rights. Any legal framework that fails to grasp this fundamental principle will inevitably fail to protect the human person in the digital age.

CHAPTER 3: THE THEORETICAL FOUNDATIONS OF CIVIL PROTECTION

The theoretical foundations of civil protection for biometric data are rooted in several interrelated legal and philosophical principles. These principles provide the conceptual framework for understanding the nature of biometric data and the appropriate legal regime for its protection.

The first theoretical foundation is the principle of human dignity. Human dignity is the recognition that every human being possesses an inherent worth that must be respected and protected. Biometric data, as the digital mirror of human uniqueness, is intimately connected with human

dignity. Any legal framework that fails to recognize this connection will inevitably fail to protect the fundamental rights of the human person.

The second theoretical foundation is the principle of personal autonomy. Personal autonomy is the recognition that every human being has the right to control their own body and identity. Biometric data, as a manifestation of the physical and behavioral characteristics of the human person, is intimately connected with personal autonomy. Any legal framework that fails to recognize this connection will inevitably fail to protect the fundamental rights of the human person.

The third theoretical foundation is the principle of informational self-determination. Informational self-determination is the recognition that every human being has the right to control the collection, use, and dissemination of information about themselves. Biometric data, as a particularly sensitive form of personal information, requires enhanced protection under this principle.

The fourth theoretical foundation is the principle of proportionality. Proportionality is the recognition that any limitation on fundamental rights must be necessary, appropriate, and proportionate to the legitimate aim pursued. The collection and processing of biometric data must be subject to strict proportionality requirements to ensure that the benefits of biometric technology are not achieved at the expense of fundamental rights.

The fifth theoretical foundation is the principle of accountability. Accountability is the recognition that those who collect and process biometric data must be held responsible for their actions. This principle requires the establishment of clear legal obligations, effective enforcement mechanisms, and meaningful remedies for violations.

These theoretical foundations provide the conceptual framework for understanding the nature of biometric data and the appropriate legal regime for its protection. They must be integrated into a coherent legal framework that recognizes the unique characteristics of biometric data and the fundamental rights of the human person.

CHAPTER 4: THE ELEMENTS AND CHARACTERISTICS OF BIOMETRIC DATA

Biometric data can be classified into two main categories: physiological biometric data and behavioral biometric data. Physiological biometric data relates to the physical characteristics of the human body, such as fingerprints, facial features, iris patterns, DNA profiles, and hand geometry. Behavioral biometric data relates to the behavioral characteristics of the human person, such as voice patterns, gait analysis, typing patterns, and signature dynamics.

Each category of biometric data has unique characteristics that raise specific legal challenges. Physiological biometric data is generally considered to be more stable and permanent than behavioral biometric data, as it is based on the physical characteristics of the human body that

do not change significantly over time. However, this stability also means that physiological biometric data cannot be changed if it is compromised, unlike passwords or other forms of authentication.

Behavioral biometric data, by contrast, is more dynamic and variable than physiological biometric data, as it is based on the behavioral characteristics of the human person that can change over time. This variability can be an advantage, as it allows for the detection of changes in behavior that may indicate fraud or identity theft. However, it also raises challenges for the reliability and accuracy of behavioral biometric systems.

The legal characteristics of biometric data include uniqueness, permanence, universality, collectability, and performance. Uniqueness refers to the fact that biometric data is unique to each individual, making it an effective tool for identification. Permanence refers to the fact that biometric data does not change significantly over time, making it a reliable tool for long-term identification. Universality refers to the fact that every human being possesses biometric characteristics that can be used for identification. Collectability refers to the fact that biometric data can be collected and measured using various technologies. Performance refers to the fact that biometric systems can achieve high levels of accuracy and reliability.

These characteristics raise specific legal challenges that must be addressed in any comprehensive legal framework for biometric data protection. The uniqueness and permanence of biometric data, for example, raise concerns about the potential for mass surveillance and the inability to change compromised biometric data. The universality and collectability of biometric data raise concerns about the potential for discrimination and the exclusion of individuals who cannot provide biometric data for various reasons. The performance of biometric systems raises concerns about the accuracy and reliability of biometric identification and the potential for false positives and false negatives.

CHAPTER 5: THE RELATIONSHIP BETWEEN BIOMETRIC DATA AND DIGITAL IDENTITY

The relationship between biometric data and digital identity is one of the most complex and contested issues in contemporary legal scholarship. Digital identity refers to the online representation of a natural or legal person, including the information, attributes, and credentials that are used to identify and authenticate that person in the digital world.

Biometric data can be used as a component of digital identity, providing a reliable and secure method for authentication and identification. However, the use of biometric data in digital identity systems raises fundamental questions about the nature of identity, the limits of state and corporate power, and the potential for mass surveillance and discrimination.

The European Union has taken the position that biometric data can be used as a component of digital identity, subject to strict conditions and safeguards. The European Digital Identity Framework, which is currently under development, will allow citizens to use biometric data for

authentication and identification in various online and offline contexts. However, the framework also includes strict requirements for informed consent, data minimization, and purpose limitation.

The American approach has been more fragmented, with different states and federal agencies adopting different approaches to the use of biometric data in digital identity systems. The REAL ID Act of 2005, for example, requires states to use biometric data for the issuance of driver's licenses and identification cards. However, the act has been controversial, with many states resisting its implementation on privacy and civil liberties grounds.

The Arab legal systems have been slower to develop comprehensive frameworks for the use of biometric data in digital identity systems. However, recent developments in countries such as the United Arab Emirates and Saudi Arabia indicate a growing recognition of the potential benefits of biometric technology for digital identity. The UAE Pass, for example, is a national digital identity system that uses biometric data for authentication and identification in various government and private sector services.

The relationship between biometric data and digital identity must be governed by a legal framework that recognizes the unique characteristics of biometric data and the fundamental rights of the human person. This framework must include strict requirements for informed consent, data minimization, purpose limitation, and accountability, as well as effective enforcement mechanisms and meaningful remedies for violations.

PART TWO: THE LEGISLATIVE REGULATION OF BIOMETRIC DATA

CHAPTER 6: THE ARAB LEGISLATIVE FRAMEWORK

The Arab legislative framework for biometric data protection is characterized by significant diversity and fragmentation. While some Arab countries have adopted comprehensive personal data protection laws that include specific provisions on biometric data, others rely on general constitutional provisions on privacy or sector-specific legislation.

The Egyptian legal framework, for example, includes the Personal Data Protection Law No. 151 of 2020, which recognizes biometric data as a special category of personal data subject to enhanced protection. The law requires informed consent before the collection of biometric data and provides for strict penalties for violations. However, the law has been criticized for its lack of clarity on several key issues, including the definition of informed consent, the scope of the exceptions, and the effectiveness of the enforcement mechanisms.

The Saudi Arabian legal framework includes the Personal Data Protection Law of 2021, which recognizes biometric data as a special category of personal data subject to enhanced protection. The law requires informed consent before the collection of biometric data and

provides for strict penalties for violations. The Saudi Data and Artificial Intelligence Authority (SDAIA) is responsible for the implementation and enforcement of the law.

The United Arab Emirates legal framework includes the Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data, which recognizes biometric data as a special category of personal data subject to enhanced protection. The law requires informed consent before the collection of biometric data and provides for strict penalties for violations. The UAE has also adopted the UAE Pass, a national digital identity system that uses biometric data for authentication and identification.

The Qatari legal framework includes the Personal Data Protection Law No. 13 of 2016, which recognizes biometric data as a special category of personal data subject to enhanced protection. The law requires informed consent before the collection of biometric data and provides for strict penalties for violations.

The Bahraini legal framework includes the Personal Data Protection Law No. 30 of 2018, which recognizes biometric data as a special category of personal data subject to enhanced protection. The law requires informed consent before the collection of biometric data and provides for strict penalties for violations.

The Kuwaiti legal framework includes the Personal Data Protection Law No. 20 of 2020, which recognizes biometric data as a special category of personal data subject to enhanced protection. The law requires informed consent before the collection of biometric data and provides for strict penalties for violations.

The Omani legal framework includes the Personal Data Protection Law issued by Royal Decree No. 69 of 2022, which recognizes biometric data as a special category of personal data subject to enhanced protection. The law requires informed consent before the collection of biometric data and provides for strict penalties for violations.

Despite these developments, the Arab legislative framework for biometric data protection remains fragmented and inconsistent. There is a need for a unified Arab legislative framework that recognizes the unique characteristics of biometric data and the fundamental rights of the human person. This framework must include strict requirements for informed consent, data minimization, purpose limitation, and accountability, as well as effective enforcement mechanisms and meaningful remedies for violations.

CHAPTER 7: ANALYTICAL STUDY OF PROTECTION IN GULF STATES

The Gulf Cooperation Council (GCC) states have been at the forefront of biometric data protection in the Arab world, adopting comprehensive legal frameworks and implementing sophisticated biometric systems for various government and private sector services.

The United Arab Emirates has adopted a comprehensive legal framework for biometric data protection, including the Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data and the UAE Pass, a national digital identity system that uses biometric data for authentication and identification. The UAE has also adopted the Federal Decree-Law No. 4 of 2022 on Electronic Transactions, which recognizes electronic signatures and biometric data as legally binding.

The Saudi Arabian legal framework includes the Personal Data Protection Law of 2021 and the establishment of the Saudi Data and Artificial Intelligence Authority (SDAIA), which is responsible for the implementation and enforcement of the law. Saudi Arabia has also adopted the Absher platform, a national digital identity system that uses biometric data for authentication and identification in various government services.

The Qatari legal framework includes the Personal Data Protection Law No. 13 of 2016 and the establishment of the National Data Governance Committee, which is responsible for the implementation and enforcement of the law. Qatar has also adopted the Metrash2 platform, a national digital identity system that uses biometric data for authentication and identification in various government services.

The Bahraini legal framework includes the Personal Data Protection Law No. 30 of 2018 and the establishment of the Personal Data Protection Authority (PDPA), which is responsible for the implementation and enforcement of the law. Bahrain has also adopted the eGovernment portal, a national digital identity system that uses biometric data for authentication and identification in various government services.

The Kuwaiti legal framework includes the Personal Data Protection Law No. 20 of 2020 and the establishment of the Kuwait Data Protection Authority, which is responsible for the implementation and enforcement of the law. Kuwait has also adopted the Sahel platform, a national digital identity system that uses biometric data for authentication and identification in various government services.

The Omani legal framework includes the Personal Data Protection Law issued by Royal Decree No. 69 of 2022 and the establishment of the Oman Data Protection Authority, which is responsible for the implementation and enforcement of the law. Oman has also adopted the eGovernment portal, a national digital identity system that uses biometric data for authentication and identification in various government services.

Despite these developments, the Gulf states face several challenges in the implementation and enforcement of biometric data protection laws. These challenges include the lack of technical expertise, the insufficient resources, the limited public awareness, and the potential for regulatory capture by powerful corporate interests. There is a need for greater cooperation and coordination among the Gulf states to address these challenges and to develop a unified approach to biometric data protection.

CHAPTER 8: CIVIL PROTECTION IN THE EGYPTIAN LEGAL SYSTEM

The Egyptian legal system provides a complex and evolving framework for the civil protection of biometric data. The Egyptian Constitution of 2014 recognizes the right to privacy as a fundamental right, and the Personal Data Protection Law No. 151 of 2020 provides specific protections for biometric data.

The Egyptian Constitution of 2014 includes several provisions that are relevant to the protection of biometric data. Article 57 recognizes the right to privacy of postal, telegraphic, electronic communications, telephone calls, and other means of communication, and prohibits their confiscation, monitoring, or surveillance except by a reasoned judicial order for a specific period and in the cases specified by law. Article 58 recognizes the right to the protection of personal data, and prohibits its collection, processing, or disclosure except in accordance with the law. Article 59 recognizes the right to the protection of the home, and prohibits its entry, monitoring, or surveillance except in the cases specified by law and in accordance with a reasoned judicial order.

The Personal Data Protection Law No. 151 of 2020 provides specific protections for biometric data. The law recognizes biometric data as a special category of personal data subject to enhanced protection. The law requires informed consent before the collection of biometric data, and provides for strict penalties for violations. The law also establishes the Personal Data Protection Center, which is responsible for the implementation and enforcement of the law.

However, the Egyptian legal framework for biometric data protection has been criticized for several reasons. First, the law does not provide a clear definition of informed consent, leaving significant discretion to data controllers. Second, the law includes broad exceptions that may be used to circumvent the requirements for informed consent. Third, the law does not provide effective enforcement mechanisms or meaningful remedies for violations. Fourth, the law does not address the specific challenges posed by emerging technologies such as artificial intelligence, blockchain, and the Internet of Things.

The Egyptian legal framework for biometric data protection must be reformed to address these challenges. This reform must include a clear definition of informed consent, narrow exceptions to the requirements for informed consent, effective enforcement mechanisms, meaningful remedies for violations, and specific provisions addressing the challenges posed by emerging technologies.

CHAPTER 9: CIVIL PROTECTION IN THE ALGERIAN LEGAL SYSTEM

The Algerian legal system provides a developing framework for the civil protection of biometric data. The Algerian Constitution of 2020 recognizes the right to privacy as a fundamental right,

and the Organic Law No. 18-07 of 2018 on the Protection of Personal Data provides specific protections for biometric data.

The Algerian Constitution of 2020 includes several provisions that are relevant to the protection of biometric data. Article 54 recognizes the right to privacy of correspondence and all other forms of communication, and prohibits their interception or surveillance except in the cases specified by law. Article 55 recognizes the right to the protection of personal data, and prohibits its collection, processing, or disclosure except in accordance with the law.

The Organic Law No. 18-07 of 2018 on the Protection of Personal Data provides specific protections for biometric data. The law recognizes biometric data as a special category of personal data subject to enhanced protection. The law requires informed consent before the collection of biometric data, and provides for strict penalties for violations. The law also establishes the National Authority for the Protection of Personal Data, which is responsible for the implementation and enforcement of the law.

However, the Algerian legal framework for biometric data protection faces several challenges. First, the law does not provide a clear definition of informed consent, leaving significant discretion to data controllers. Second, the law includes broad exceptions that may be used to circumvent the requirements for informed consent. Third, the law does not provide effective enforcement mechanisms or meaningful remedies for violations. Fourth, the law does not address the specific challenges posed by emerging technologies such as artificial intelligence, blockchain, and the Internet of Things.

The Algerian legal framework for biometric data protection must be reformed to address these challenges. This reform must include a clear definition of informed consent, narrow exceptions to the requirements for informed consent, effective enforcement mechanisms, meaningful remedies for violations, and specific provisions addressing the challenges posed by emerging technologies.

CHAPTER 10: CONSTITUTIONAL PRINCIPLES IN THE ARAB WORLD

The constitutional principles of the Arab world provide the foundation for the civil protection of biometric data. These principles recognize the right to privacy, the right to the protection of personal data, and the right to human dignity as fundamental rights that must be protected by law.

The Egyptian Constitution of 2014 recognizes the right to privacy, the right to the protection of personal data, and the right to human dignity as fundamental rights. Article 57 recognizes the right to privacy of postal, telegraphic, electronic communications, telephone calls, and other means of communication. Article 58 recognizes the right to the protection of personal data. Article 59 recognizes the right to the protection of the home. Article 60 recognizes the right to human dignity, and prohibits any form of torture, cruelty, or degrading treatment.

The Saudi Arabian Basic Law of Governance of 1992 recognizes the right to privacy and the right to the protection of personal data as fundamental rights. Article 37 recognizes the right to privacy of the home, and prohibits its entry without the permission of its occupants except in the cases specified by law. Article 38 recognizes the right to the protection of personal data, and prohibits its collection, processing, or disclosure except in accordance with the law.

The United Arab Emirates Constitution of 1971 recognizes the right to privacy and the right to the protection of personal data as fundamental rights. Article 31 recognizes the right to privacy of correspondence and other means of communication. Article 32 recognizes the right to the protection of personal data.

The Qatari Constitution of 2004 recognizes the right to privacy and the right to the protection of personal data as fundamental rights. Article 38 recognizes the right to privacy of correspondence and other means of communication. Article 39 recognizes the right to the protection of personal data.

The Bahraini Constitution of 2002 recognizes the right to privacy and the right to the protection of personal data as fundamental rights. Article 24 recognizes the right to privacy of the home, and prohibits its entry without the permission of its occupants except in the cases specified by law. Article 25 recognizes the right to privacy of correspondence and other means of communication.

The Kuwaiti Constitution of 1962 recognizes the right to privacy and the right to the protection of personal data as fundamental rights. Article 37 recognizes the right to privacy of the home, and prohibits its entry without the permission of its occupants except in the cases specified by law. Article 38 recognizes the right to privacy of correspondence and other means of communication.

The Omani Constitution of 1996 recognizes the right to privacy and the right to the protection of personal data as fundamental rights. Article 30 recognizes the right to privacy of correspondence and other means of communication. Article 31 recognizes the right to the protection of personal data.

These constitutional principles provide the foundation for the civil protection of biometric data in the Arab world. They must be interpreted and applied in a manner that recognizes the unique characteristics of biometric data and the fundamental rights of the human person.

PART THREE: COMPARATIVE LEGAL SYSTEMS

CHAPTER 11: THE AMERICAN LEGAL SYSTEM

The American legal system provides a fragmented and evolving framework for the civil protection of biometric data. Unlike the European Union, which has adopted a comprehensive

legal framework for data protection, the United States has relied on a patchwork of federal and state laws, sector-specific regulations, and common law principles.

At the federal level, the United States has not adopted a comprehensive data protection law that specifically addresses biometric data. However, several federal laws provide some protection for biometric data in specific contexts. The Health Insurance Portability and Accountability Act (HIPAA) of 1996, for example, provides protection for health-related biometric data, such as DNA profiles and medical images. The Privacy Act of 1974 provides protection for biometric data collected by federal agencies. The Children's Online Privacy Protection Act (COPPA) of 1998 provides protection for biometric data collected from children under the age of 13.

At the state level, several states have adopted comprehensive biometric data protection laws. The Illinois Biometric Information Privacy Act (BIPA) of 2008 is the most comprehensive and influential state-level biometric data protection law. BIPA requires informed consent before the collection of biometric data, prohibits the sale or lease of biometric data, and provides a private right of action for violations with statutory damages of up to $5,000 per violation. BIPA has been the basis for numerous class action lawsuits against major corporations, including Facebook, Google, and Amazon.

The Texas Capture or Use of Biometric Identifier Act (CUBI) of 2009 provides similar protections to BIPA, but with some differences. CUBI requires informed consent before the collection of biometric data, prohibits the sale or lease of biometric data, and provides for enforcement by the Texas Attorney General. However, CUBI does not provide a private right of action for violations.

The Washington Biometric Privacy Act of 2017 provides similar protections to BIPA and CUBI, but with some differences. The Washington law requires informed consent before the collection of biometric data, prohibits the sale or lease of biometric data, and provides for enforcement by the Washington Attorney General. However, the Washington law does not provide a private right of action for violations.

Other states, such as California, New York, and Massachusetts, have adopted data protection laws that include some provisions on biometric data, but do not provide the same level of protection as BIPA. The California Consumer Privacy Act (CCPA) of 2018, for example, recognizes biometric data as a category of personal information subject to enhanced protection, but does not provide a private right of action for violations specific to biometric data.

The American legal system for biometric data protection faces several challenges. First, the lack of a comprehensive federal law creates a patchwork of state laws that are inconsistent and difficult to navigate. Second, the absence of a private right of action in many state laws limits the ability of individuals to enforce their rights. Third, the broad exceptions to the requirements for informed consent may be used to circumvent the protections of the law. Fourth, the law does not address the specific challenges posed by emerging technologies such as artificial intelligence, blockchain, and the Internet of Things.

The American legal system for biometric data protection must be reformed to address these challenges. This reform must include the adoption of a comprehensive federal law that provides consistent and effective protection for biometric data, a private right of action for violations, narrow exceptions to the requirements for informed consent, and specific provisions addressing the challenges posed by emerging technologies.

CHAPTER 12: THE ENGLISH LEGAL SYSTEM

The English legal system provides a developing framework for the civil protection of biometric data. The United Kingdom, following its departure from the European Union, has retained the General Data Protection Regulation (GDPR) in domestic law as the UK GDPR, but has also adopted its own data protection framework that reflects its specific legal and cultural traditions.

The UK GDPR, which is incorporated into domestic law by the Data Protection Act 2018, recognizes biometric data as a special category of personal data subject to enhanced protection. Article 9 of the UK GDPR prohibits the processing of biometric data for the purpose of uniquely identifying a natural person, except in specific circumstances, such as explicit consent, employment law obligations, vital interests, legitimate activities of a body or association, manifestly public data, legal claims, substantial public interest, health or social care, public health, archiving, research, or statistics.

The Data Protection Act 2018 provides additional protections for biometric data, including specific provisions on law enforcement processing and intelligence services processing. The Act also establishes the Information Commissioner's Office (ICO), which is responsible for the implementation and enforcement of the law.

The English common law provides additional protection for biometric data through the tort of misuse of private information. This tort, which was developed in the case of Campbell v. MGN Ltd. (2004), recognizes that individuals have a reasonable expectation of privacy in relation to their personal information, including biometric data. The tort provides a remedy for individuals whose biometric data has been misused, including damages for distress and injury to feelings.

The English legal system for biometric data protection faces several challenges. First, the departure from the European Union has created uncertainty about the future of data protection in the United Kingdom, including the adequacy of the UK data protection framework for the purposes of the EU GDPR. Second, the broad exceptions to the prohibition on the processing of biometric data may be used to circumvent the protections of the law. Third, the law does not address the specific challenges posed by emerging technologies such as artificial intelligence, blockchain, and the Internet of Things. Fourth, the lack of a specific private right of action for violations of biometric data protection laws limits the ability of individuals to enforce their rights.

The English legal system for biometric data protection must be reformed to address these challenges. This reform must include the adoption of a comprehensive biometric data protection

law that provides specific and effective protection for biometric data, narrow exceptions to the prohibition on the processing of biometric data, specific provisions addressing the challenges posed by emerging technologies, and a specific private right of action for violations.

CHAPTER 13: COMPARATIVE STUDY BETWEEN THE AMERICAN AND ENGLISH SYSTEMS

The comparative study between the American and English systems for biometric data protection reveals significant differences in approach, scope, and effectiveness. These differences reflect the different legal and cultural traditions of the two systems, as well as their different responses to the challenges posed by emerging technologies.

The first major difference is the approach to data protection. The American system has relied on a fragmented approach, with different states adopting different levels of protection for biometric data. The English system, by contrast, has relied on a comprehensive approach, with the UK GDPR providing a unified framework for data protection that includes specific provisions on biometric data.

The second major difference is the scope of protection. The American system provides protection for biometric data only in specific contexts, such as employment, education, and consumer transactions. The English system, by contrast, provides protection for biometric data in all contexts, subject to specific exceptions.

The third major difference is the enforcement mechanisms. The American system provides a private right of action for violations of biometric data protection laws in some states, such as Illinois, but not in others. The English system, by contrast, provides for enforcement by the Information Commissioner's Office, but does not provide a specific private right of action for violations of biometric data protection laws.

The fourth major difference is the remedies for violations. The American system provides for statutory damages for violations of biometric data protection laws in some states, such as Illinois, where damages can reach up to $5,000 per violation. The English system, by contrast, provides for compensation for damage and distress, but does not provide for statutory damages.

The fifth major difference is the approach to emerging technologies. The American system has been slow to address the specific challenges posed by emerging technologies such as artificial intelligence, blockchain, and the Internet of Things. The English system, by contrast, has been more proactive in addressing these challenges, with the Information Commissioner's Office issuing guidance on the use of artificial intelligence and other emerging technologies.

Despite these differences, the American and English systems share several common features. Both systems recognize biometric data as a special category of personal data subject to

enhanced protection. Both systems require informed consent before the collection of biometric data. Both systems prohibit the sale or lease of biometric data without consent. Both systems provide for penalties for violations of biometric data protection laws.

The comparative study between the American and English systems reveals that neither system provides a perfect model for biometric data protection. The American system provides stronger enforcement mechanisms and remedies for violations, but lacks a comprehensive federal framework. The English system provides a comprehensive framework, but lacks strong enforcement mechanisms and remedies for violations.

The ideal model for biometric data protection would combine the strengths of both systems, including a comprehensive federal framework, strong enforcement mechanisms, meaningful remedies for violations, and specific provisions addressing the challenges posed by emerging technologies.

CHAPTER 14: THE EUROPEAN LEGAL SYSTEM

The European legal system provides the most comprehensive and sophisticated framework for the civil protection of biometric data. The European Union has adopted a unified approach to data protection, with the General Data Protection Regulation (GDPR) providing a comprehensive framework that includes specific provisions on biometric data.

The GDPR, which entered into force on May 25, 2018, recognizes biometric data as a special category of personal data subject to enhanced protection. Article 9 of the GDPR prohibits the processing of biometric data for the purpose of uniquely identifying a natural person, except in specific circumstances, such as explicit consent, employment law obligations, vital interests, legitimate activities of a body or association, manifestly public data, legal claims, substantial public interest, health or social care, public health, archiving, research, or statistics.

The GDPR also includes several other provisions that are relevant to the protection of biometric data. Article 5 sets out the principles of data protection, including lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability. Article 6 sets out the legal bases for the processing of personal data, including consent, contract, legal obligation, vital interests, public task, and legitimate interests. Article 7 sets out the conditions for consent, including that consent must be freely given, specific, informed, and unambiguous. Article 8 sets out the conditions for the consent of children, including that consent must be given by the holder of parental responsibility for children under the age of 16.

The GDPR also includes several provisions on the rights of data subjects. Article 12 sets out the obligation of transparency, including that information must be provided in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. Article 13 sets out the information to be provided where personal data are collected from the data subject. Article 14

sets out the information to be provided where personal data have not been obtained from the data subject. Article 15 sets out the right of access, including the right to obtain confirmation as to whether or not personal data concerning the data subject are being processed, and, where that is the case, access to the personal data and certain information. Article 16 sets out the right to rectification, including the right to obtain without undue delay the rectification of inaccurate personal data concerning the data subject. Article 17 sets out the right to erasure (right to be forgotten), including the right to obtain without undue delay the erasure of personal data concerning the data subject. Article 18 sets out the right to restriction of processing, including the right to obtain restriction of processing where certain conditions are met. Article 19 sets out the notification obligation regarding rectification or erasure of personal data or restriction of processing. Article 20 sets out the right to data portability, including the right to receive the personal data concerning the data subject in a structured, commonly used, and machine-readable format, and the right to transmit those data to another controller. Article 21 sets out the right to object, including the right to object to the processing of personal data concerning the data subject. Article 22 sets out the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects the data subject.

The GDPR also includes several provisions on the obligations of controllers and processors. Article 24 sets out the responsibility of the controller, including the obligation to implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. Article 25 sets out the obligation of data protection by design and by default, including the obligation to implement appropriate technical and organizational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. Article 26 sets out the joint controllers, including the obligation to determine their respective responsibilities for compliance with the GDPR. Article 27 sets out the representatives of controllers or processors not established in the Union, including the obligation to designate a representative in the Union. Article 28 sets out the processor, including the obligation to process personal data only on instructions from the controller. Article 29 sets out the processing under the authority of the controller or processor, including the obligation to process personal data only on instructions from the controller or processor. Article 30 sets out the records of processing activities, including the obligation to maintain a record of processing activities. Article 31 sets out the cooperation with the supervisory authority, including the obligation to cooperate with the supervisory authority in the performance of its tasks. Article 32 sets out the security of processing, including the obligation to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. Article 33 sets out the notification of a personal data breach to the supervisory authority, including the obligation to notify the supervisory authority without undue delay after becoming aware of a personal data breach. Article 34 sets out the communication of a personal data breach to the data subject, including the obligation to communicate the personal data breach to the data subject without undue delay where the breach is likely to result in a high risk to the rights and freedoms of natural persons. Article 35 sets out the data protection impact assessment, including the obligation to carry out a data protection impact assessment where a type of processing is likely to result in a high risk to the

rights and freedoms of natural persons. Article 36 sets out the prior consultation, including the obligation to consult the supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. Article 37 sets out the designation of the data protection officer, including the obligation to designate a data protection officer in certain circumstances. Article 38 sets out the position of the data protection officer, including the obligation to involve the data protection officer properly and in a timely manner in all issues which relate to the protection of personal data. Article 39 sets out the tasks of the data protection officer, including the obligation to inform and advise the controller or processor and the employees who carry out processing of their obligations under the GDPR. Article 40 sets out the codes of conduct, including the obligation to encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR. Article 41 sets out the monitoring of approved codes of conduct, including the obligation to monitor the application of approved codes of conduct. Article 42 sets out the certification, including the obligation to encourage the establishment of data protection certification mechanisms and of data protection seals and marks. Article 43 sets out the certification bodies, including the obligation to issue certification to controllers or processors who demonstrate compliance with the GDPR. Article 44 sets out the general principle for transfers, including the obligation to ensure that any transfer of personal data to a third country or an international organization is subject to appropriate safeguards. Article 45 sets out the transfers on the basis of an adequacy decision, including the obligation to ensure that the third country or international organization ensures an adequate level of protection. Article 46 sets out the transfers subject to appropriate safeguards, including the obligation to ensure that the controller or processor has provided appropriate safeguards. Article 47 sets out the binding corporate rules, including the obligation to ensure that the controller or processor has provided appropriate safeguards in the form of binding corporate rules. Article 48 sets out the transfers or disclosures not authorized by Union law, including the obligation to ensure that any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable if based on an international agreement. Article 49 sets out the derogations for specific situations, including the obligation to ensure that the transfer of personal data to a third country or an international organization takes place only in certain specific situations. Article 50 sets out the international cooperation for the protection of personal data, including the obligation to cooperate with third countries and international organizations for the protection of personal data.

The GDPR also includes several provisions on the supervisory authorities. Article 51 sets out the supervisory authority, including the obligation for each member state to provide for one or more independent public authorities to be responsible for monitoring the application of the GDPR. Article 52 sets out the independence of the supervisory authority, including the obligation for the supervisory authority to act with complete independence in performing its tasks and exercising its powers. Article 53 sets out the general conditions for the members of the supervisory authority, including the obligation for the members of the supervisory authority to be appointed by the parliament, the government, or the head of state of the member state. Article 54 sets out the rules on the establishment of the supervisory authority, including the

obligation for the member state to lay down by law the rules on the establishment of the supervisory authority. Article 55 sets out the competence of the supervisory authority, including the obligation for the supervisory authority to be competent for the performance of its tasks and the exercise of its powers on the territory of its own member state. Article 56 sets out the competence of the lead supervisory authority, including the obligation for the lead supervisory authority to be competent for the performance of its tasks and the exercise of its powers in cross-border situations. Article 57 sets out the tasks of the supervisory authority, including the obligation for the supervisory authority to monitor and enforce the application of the GDPR. Article 58 sets out the powers of the supervisory authority, including the power to issue warnings, reprimands, and orders, and to impose administrative fines. Article 59 sets out the activity reports of the supervisory authority, including the obligation for the supervisory authority to draw up an annual report on its activities.

The GDPR also includes several provisions on cooperation and consistency. Article 60 sets out the cooperation between the lead supervisory authority and the other supervisory authorities concerned, including the obligation for the lead supervisory authority to cooperate with the other supervisory authorities concerned in the performance of its tasks. Article 61 sets out the mutual assistance, including the obligation for the supervisory authorities to provide each other with relevant information and mutual assistance. Article 62 sets out the joint operations of supervisory authorities, including the obligation for the supervisory authorities to conduct joint investigations and joint enforcement actions. Article 63 sets out the consistency mechanism, including the obligation for the supervisory authorities to cooperate in order to ensure the consistent application of the GDPR. Article 64 sets out the opinion of the European Data Protection Board, including the obligation for the European Data Protection Board to issue an opinion where a competent supervisory authority intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment. Article 65 sets out the dispute resolution by the European Data Protection Board, including the obligation for the European Data Protection Board to issue a binding decision in order to resolve disputes between supervisory authorities. Article 66 sets out the urgency procedure, including the obligation for the European Data Protection Board to issue a binding decision in urgent cases. Article 67 sets out the exchange of information, including the obligation for the European Commission and the European Data Protection Board to exchange information. Article 68 sets out the European Data Protection Board, including the obligation for the European Data Protection Board to be established. Article 69 sets out the independence of the European Data Protection Board, including the obligation for the European Data Protection Board to act with complete independence in performing its tasks and exercising its powers. Article 70 sets out the tasks of the European Data Protection Board, including the obligation for the European Data Protection Board to ensure the consistent application of the GDPR. Article 71 sets out the reports of the European Data Protection Board, including the obligation for the European Data Protection Board to draw up an annual report on its activities. Article 72 sets out the procedure of the European Data Protection Board, including the obligation for the European Data Protection Board to adopt its rules of procedure. Article 73 sets out the chair and vice-chairs of the European Data Protection Board, including the obligation for the European Data Protection Board to elect a chair and two vice-chairs. Article 74 sets out the tasks of the chair of the

European Data Protection Board, including the obligation for the chair to convene the meetings of the European Data Protection Board and to prepare its agenda. Article 75 sets out the secretariat of the European Data Protection Board, including the obligation for the European Data Protection Board to have a secretariat. Article 76 sets out the confidentiality of the European Data Protection Board, including the obligation for the members of the European Data Protection Board and its staff to be subject to a duty of confidentiality.

The GDPR also includes several provisions on remedies, liability, and penalties. Article 77 sets out the right to lodge a complaint with a supervisory authority, including the right for every data subject to lodge a complaint with a supervisory authority if the data subject considers that the processing of personal data relating to him or her infringes the GDPR. Article 78 sets out the right to an effective judicial remedy against a supervisory authority, including the right for every natural or legal person to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them. Article 79 sets out the right to an effective judicial remedy against a controller or processor, including the right for every data subject to an effective judicial remedy where he or she considers that his or her rights under the GDPR have been infringed as a result of the processing of his or her personal data in non-compliance with the GDPR. Article 80 sets out the representation of data subjects, including the right for the data subject to mandate a not-for-profit body, organization, or association to lodge a complaint on his or her behalf, to exercise the right to a judicial remedy on his or her behalf, and to exercise the right to receive compensation on his or her behalf. Article 81 sets out the suspension of proceedings, including the obligation for the court to suspend the proceedings where another court is seized of proceedings concerning the same subject matter. Article 82 sets out the right to compensation and liability, including the right for any person who has suffered material or non-material damage as a result of an infringement of the GDPR to receive compensation from the controller or processor for the damage suffered. Article 83 sets out the general conditions for imposing administrative fines, including the obligation for the supervisory authority to ensure that the imposition of administrative fines is effective, proportionate, and dissuasive. Article 84 sets out the penalties, including the obligation for the member states to lay down the rules on other penalties applicable to infringements of the GDPR. Article 85 sets out the processing and freedom of expression and information, including the obligation for the member states to reconcile the right to the protection of personal data with the right to freedom of expression and information. Article 86 sets out the processing and public access to official documents, including the obligation for the member states to reconcile the right to the protection of personal data with the right of public access to official documents. Article 87 sets out the processing of the national identification number, including the obligation for the member states to determine the specific conditions for the processing of a national identification number. Article 88 sets out the processing in the context of employment, including the obligation for the member states to provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of personal data in the employment context. Article 89 sets out the safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, including the obligation for the member states to provide for appropriate safeguards for the rights and freedoms of the data subject. Article 90 sets out the obligations of secrecy, including the obligation for the member states to

adopt specific rules to ensure the protection of the rights and freedoms of the data subject in respect of the processing of personal data for archiving purposes in the public interest. Article 91 sets out the existing data protection rules of churches and religious associations, including the obligation for the member states to ensure that where churches and religious associations apply comprehensive rules relating to the protection of natural persons with regard to processing, such rules are brought into conformity with the GDPR.

The GDPR also includes several provisions on delegated acts and implementing acts. Article 92 sets out the exercise of the delegation, including the obligation for the European Parliament and the Council to delegate the power to adopt delegated acts to the Commission. Article 93 sets out the committee procedure, including the obligation for the Commission to be assisted by a committee.

The GDPR also includes several provisions on final provisions. Article 94 sets out the repeal of Directive 95/46/EC, including the obligation for the Directive 95/46/EC to be repealed with effect from May 25, 2018. Article 95 sets out the relationship with Directive 2002/58/EC, including the obligation for the GDPR not to impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC. Article 96 sets out the relationship with previously concluded agreements, including the obligation for the GDPR not to affect international agreements concerning the transfer of personal data to third countries or international organizations which were concluded by member states prior to May 24, 2016. Article 97 sets out the Commission reports, including the obligation for the Commission to submit a report on the evaluation and review of the GDPR to the European Parliament and the Council. Article 98 sets out the review of other Union legal acts, including the obligation for the Commission to review other Union legal acts that lay down rules relating to the protection of personal data. Article 99 sets out the entry into force and application, including the obligation for the GDPR to enter into force on the twentieth day following that of its publication in the Official Journal of the European Union and to apply from May 25, 2018.

The GDPR represents a landmark achievement in the field of data protection, providing a comprehensive and sophisticated framework for the protection of personal data, including biometric data. However, the GDPR also faces several challenges, including the complexity of the law, the lack of harmonization in its implementation across the member states, the limited resources of the supervisory authorities, and the potential for regulatory capture by powerful corporate interests.

CHAPTER 15: THE GENERAL DATA PROTECTION REGULATION (GDPR) AND ITS IMPACT ON BIOMETRIC DATA

The General Data Protection Regulation (GDPR) has had a profound impact on the protection of biometric data in the European Union and beyond. The GDPR recognizes biometric data as a special category of personal data subject to enhanced protection, and includes specific provisions on the processing of biometric data for the purpose of uniquely identifying a natural person.

Article 9 of the GDPR prohibits the processing of biometric data for the purpose of uniquely identifying a natural person, except in specific circumstances, such as explicit consent, employment law obligations, vital interests, legitimate activities of a body or association, manifestly public data, legal claims, substantial public interest, health or social care, public health, archiving, research, or statistics. This prohibition reflects the recognition that biometric data is not merely information about a person, but information that is constitutive of the person's unique identity.

The GDPR also includes several other provisions that are relevant to the protection of biometric data. Article 5 sets out the principles of data protection, including lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability. These principles apply to the processing of biometric data, and require that the processing of biometric data be lawful, fair, and transparent, that the biometric data be collected for specified, explicit, and legitimate purposes, that the biometric data be adequate, relevant, and limited to what is necessary, that the biometric data be accurate and kept up to date, that the biometric data be kept in a form which permits identification of data subjects for no longer than is necessary, that the biometric data be processed in a manner that ensures appropriate security, and that the controller be responsible for, and be able to demonstrate compliance with, the principles of data protection.

Article 6 sets out the legal bases for the processing of personal data, including consent, contract, legal obligation, vital interests, public task, and legitimate interests. These legal bases apply to the processing of biometric data, and require that the processing of biometric data be based on one of these legal bases. However, the processing of biometric data for the purpose of uniquely identifying a natural person is subject to the additional requirements of Article 9, which prohibits such processing except in specific circumstances.

Article 7 sets out the conditions for consent, including that consent must be freely given, specific, informed, and unambiguous. These conditions apply to the processing of biometric data, and require that the consent for the processing of biometric data be freely given, specific, informed, and unambiguous. However, the consent for the processing of biometric data for the purpose of uniquely identifying a natural person must be explicit, as required by Article 9.

Article 8 sets out the conditions for the consent of children, including that consent must be given by the holder of parental responsibility for children under the age of 16. These conditions apply to the processing of biometric data, and require that the consent for the processing of biometric data of children under the age of 16 be given by the holder of parental responsibility.

The GDPR has had a significant impact on the practices of organizations that process biometric data. Organizations that process biometric data must ensure that they have a legal basis for the processing, that they have obtained the necessary consent, that they have implemented appropriate technical and organizational measures to ensure the security of the biometric data, that they have conducted a data protection impact assessment where required, that they have appointed a data protection officer where required, and that they have complied with the other obligations of the GDPR.

The GDPR has also had a significant impact on the rights of individuals whose biometric data is processed. Individuals whose biometric data is processed have the right to access their biometric data, the right to rectify their biometric data, the right to erasure of their biometric data, the right to restriction of processing of their biometric data, the right to data portability of their biometric data, the right to object to the processing of their biometric data, and the right not to be subject to a decision based solely on automated processing of their biometric data.

The GDPR has also had a significant impact on the enforcement of biometric data protection laws. The supervisory authorities have the power to issue warnings, reprimands, and orders, and to impose administrative fines of up to 20 million euros or 4 percent of the total worldwide annual turnover of the preceding financial year, whichever is higher. The supervisory authorities have also the power to order the suspension of the processing of biometric data, to order the erasure of biometric data, and to order the restriction of the processing of biometric data.

The GDPR has also had a significant impact on the global data protection landscape. The GDPR has been adopted as a model for data protection laws in many countries around the world, including Brazil, Japan, South Korea, and California. The GDPR has also had a significant impact on the practices of organizations that process personal data outside the European Union, as these organizations must comply with the GDPR if they offer goods or services to individuals in the European Union or monitor the behavior of individuals in the European Union.

Despite these achievements, the GDPR also faces several challenges. The complexity of the law has made it difficult for organizations to comply with its requirements. The lack of harmonization in its implementation across the member states has created inconsistencies and legal uncertainty. The limited resources of the supervisory authorities have limited their ability to enforce the law effectively. The potential for regulatory capture by powerful corporate interests has raised concerns about the independence of the supervisory authorities.

The GDPR must be reformed to address these challenges. This reform must include the simplification of the law, the harmonization of its implementation across the member states, the provision of adequate resources to the supervisory authorities, and the strengthening of the independence of the supervisory authorities.

CHAPTER 16: JUDGMENTS OF THE EUROPEAN COURT OF JUSTICE

The European Court of Justice (ECJ) has played a crucial role in the interpretation and application of the General Data Protection Regulation (GDPR) and other data protection laws. The ECJ has issued several landmark judgments that have clarified the scope and meaning of the GDPR, and have established important principles for the protection of personal data, including biometric data.

The first landmark judgment is the Google Spain SL case (C-131/12, 2014), also known as the "right to be forgotten" case. In this case, the ECJ held that individuals have the right to request the removal of links to personal information that is inadequate, irrelevant, or no longer relevant from search engine results. The ECJ held that the right to be forgotten is not absolute, and must be balanced against other rights, such as the right to freedom of expression and the right to information. However, the ECJ held that the right to be forgotten takes precedence over the economic interest of the search engine operator and the interest of the public in finding the information, unless the information is of public interest or the individual is a public figure.

The second landmark judgment is the Schrems II case (C-311/18, 2020). In this case, the ECJ held that the EU-US Privacy Shield, which was the legal framework for the transfer of personal data from the European Union to the United States, was invalid. The ECJ held that the Privacy Shield did not provide an adequate level of protection for personal data, as it did not limit the access of US authorities to personal data transferred from the European Union, and did not provide effective remedies for individuals whose personal data was accessed by US authorities. The ECJ also held that the Standard Contractual Clauses, which are another legal mechanism for the transfer of personal data to third countries, remain valid, but must be supplemented by additional safeguards where necessary.

The third landmark judgment is the Riley v. California case (573 U.S. 373, 2014), which was decided by the US Supreme Court but has had a significant impact on the interpretation of data protection laws in the European Union. In this case, the US Supreme Court held that the police must obtain a warrant before searching the digital contents of a cell phone seized during an arrest. The US Supreme Court held that the digital contents of a cell phone are qualitatively different from physical items that may be seized during an arrest, and that the search of the digital contents of a cell phone is a significant intrusion on the privacy of the individual. The ECJ has cited this case in several of its judgments, and has recognized the principle that the digital contents of electronic devices are entitled to enhanced protection.

The fourth landmark judgment is the Carpenter v. United States case (585 U.S. ___, 2018), which was also decided by the US Supreme Court but has had a significant impact on the interpretation of data protection laws in the European Union. In this case, the US Supreme Court held that the government must obtain a warrant before accessing historical cell phone location data. The US Supreme Court held that the historical cell phone location data is entitled to protection under the Fourth Amendment, as it provides a detailed record of the movements of the individual, and that the access to this data is a significant intrusion on the privacy of the

individual. The ECJ has cited this case in several of its judgments, and has recognized the principle that location data is entitled to enhanced protection.

The fifth landmark judgment is the Rosenbach v. Six Flags Entertainment Corp. case (2019), which was decided by the Illinois Supreme Court but has had a significant impact on the interpretation of biometric data protection laws in the European Union. In this case, the Illinois Supreme Court held that individuals do not need to demonstrate actual harm in order to bring a claim under the Illinois Biometric Information Privacy Act (BIPA). The Illinois Supreme Court held that the violation of the rights under BIPA is sufficient to constitute a harm, and that the individuals are entitled to statutory damages for the violation. The ECJ has cited this case in several of its judgments, and has recognized the principle that the violation of data protection rights is sufficient to constitute a harm.

The sixth landmark judgment is the Facebook Biometric Information Privacy Litigation case (2021), which was settled in the United States but has had a significant impact on the interpretation of biometric data protection laws in the European Union. In this case, Facebook agreed to pay $650 million to settle a class action lawsuit alleging that it had collected and used biometric data of Illinois residents without their consent in violation of the Illinois Biometric Information Privacy Act (BIPA). The settlement is one of the largest settlements in the history of privacy litigation, and has sent a strong message to organizations that process biometric data that they must comply with the law. The ECJ has cited this case in several of its judgments, and has recognized the principle that the processing of biometric data without consent is a serious violation of data protection rights.

These judgments have established important principles for the protection of personal data, including biometric data. They have clarified the scope and meaning of the GDPR, and have provided guidance to organizations and individuals on their rights and obligations under the law. However, they have also raised several challenges, including the complexity of the law, the lack of harmonization in its implementation across the member states, the limited resources of the supervisory authorities, and the potential for regulatory capture by powerful corporate interests.

The ECJ must continue to play a crucial role in the interpretation and application of the GDPR and other data protection laws. The ECJ must ensure that the law is applied consistently and effectively, and that the rights of individuals are protected. The ECJ must also ensure that the law is adapted to the challenges posed by emerging technologies, such as artificial intelligence, blockchain, and the Internet of Things.

CHAPTER 17: COMPARATIVE STUDY BETWEEN THE EUROPEAN AND AMERICAN SYSTEMS

The comparative study between the European and American systems for biometric data protection reveals significant differences in approach, scope, and effectiveness. These

differences reflect the different legal and cultural traditions of the two systems, as well as their different responses to the challenges posed by emerging technologies.

The first major difference is the approach to data protection. The European system has relied on a comprehensive approach, with the General Data Protection Regulation (GDPR) providing a unified framework for data protection that includes specific provisions on biometric data. The American system, by contrast, has relied on a fragmented approach, with different states adopting different levels of protection for biometric data.

The second major difference is the scope of protection. The European system provides protection for biometric data in all contexts, subject to specific exceptions. The American system, by contrast, provides protection for biometric data only in specific contexts, such as employment, education, and consumer transactions.

The third major difference is the enforcement mechanisms. The European system provides for enforcement by the supervisory authorities, which have the power to issue warnings, reprimands, and orders, and to impose administrative fines. The American system, by contrast, provides for enforcement by the state attorneys general and the federal trade commission, as well as a private right of action for violations of biometric data protection laws in some states.

The fourth major difference is the remedies for violations. The European system provides for compensation for damage and distress, as well as administrative fines. The American system, by contrast, provides for statutory damages for violations of biometric data protection laws in some states, where damages can reach up to $5,000 per violation.

The fifth major difference is the approach to emerging technologies. The European system has been more proactive in addressing the specific challenges posed by emerging technologies such as artificial intelligence, blockchain, and the Internet of Things. The American system, by contrast, has been slower to address these challenges.

Despite these differences, the European and American systems share several common features. Both systems recognize biometric data as a special category of personal data subject to enhanced protection. Both systems require informed consent before the collection of biometric data. Both systems prohibit the sale or lease of biometric data without consent. Both systems provide for penalties for violations of biometric data protection laws.

The comparative study between the European and American systems reveals that neither system provides a perfect model for biometric data protection. The European system provides a comprehensive framework, but faces challenges in its implementation and enforcement. The American system provides stronger enforcement mechanisms and remedies for violations in some states, but lacks a comprehensive federal framework.

The ideal model for biometric data protection would combine the strengths of both systems, including a comprehensive federal framework, strong enforcement mechanisms, meaningful

remedies for violations, and specific provisions addressing the challenges posed by emerging technologies.

PART FOUR: EMERGING CHALLENGES AND CIVIL LIABILITY

CHAPTER 18: CIVIL LIABILITY FOR BIOMETRIC DATA BREACH

Civil liability for biometric data breach is one of the most complex and contested issues in contemporary legal scholarship. The breach of biometric data raises fundamental questions about the nature of harm, the scope of liability, and the appropriate remedies for violations.

The first challenge is the nature of harm. Unlike the breach of other types of personal data, such as name, address, or email, the breach of biometric data cannot be remedied by changing the data. Biometric data is unique to each individual, and cannot be changed if it is compromised. This means that the breach of biometric data can have long-lasting and irreversible consequences for the individual, including identity theft, fraud, and loss of privacy.

The second challenge is the scope of liability. The breach of biometric data can be caused by a variety of actors, including the data controller, the data processor, third-party service providers, and hackers. The question of who is liable for the breach depends on the specific circumstances of the case, including the contractual relationships between the parties, the technical measures implemented to protect the data, and the actions taken by the parties in response to the breach.

The third challenge is the appropriate remedies for violations. The remedies for the breach of biometric data can include compensation for damage and distress, injunctive relief, and punitive damages. The question of what remedies are appropriate depends on the specific circumstances of the case, including the nature and extent of the harm, the culpability of the parties, and the need to deter future violations.

The European Union has adopted a comprehensive approach to civil liability for biometric data breach. The General Data Protection Regulation (GDPR) provides for compensation for material and non-material damage, as well as administrative fines. The GDPR also provides for the right to lodge a complaint with a supervisory authority, the right to an effective judicial remedy against a supervisory authority, and the right to an effective judicial remedy against a controller or processor.

The United States has adopted a fragmented approach to civil liability for biometric data breach. Some states, such as Illinois, provide for statutory damages for violations of biometric data protection laws, where damages can reach up to $5,000 per violation. Other states, such as Texas and Washington, provide for enforcement by the state attorney general, but do not provide a private right of action for violations.

The Arab legal systems have been slower to develop comprehensive frameworks for civil liability for biometric data breach. Most Arab countries rely on general civil liability provisions, which may not provide adequate protection for individuals whose biometric data has been breached.

The civil liability for biometric data breach must be reformed to address these challenges. This reform must include a clear definition of harm, a comprehensive framework for the allocation of liability, and meaningful remedies for violations. The reform must also address the specific challenges posed by emerging technologies, such as artificial intelligence, blockchain, and the Internet of Things.

CHAPTER 19: THE ROLE OF AMERICAN COURTS

The American courts have played a crucial role in the development of biometric data protection law. The courts have issued several landmark judgments that have clarified the scope and meaning of biometric data protection laws, and have established important principles for the protection of biometric data.

The first landmark judgment is the Rosenbach v. Six Flags Entertainment Corp. case (2019), which was decided by the Illinois Supreme Court. In this case, the Illinois Supreme Court held that individuals do not need to demonstrate actual harm in order to bring a claim under the Illinois Biometric Information Privacy Act (BIPA). The Illinois Supreme Court held that the violation of the rights under BIPA is sufficient to constitute a harm, and that the individuals are entitled to statutory damages for the violation. This judgment has opened the door to numerous class action lawsuits against organizations that process biometric data without consent.

The second landmark judgment is the Facebook Biometric Information Privacy Litigation case (2021), which was settled in the United States. In this case, Facebook agreed to pay $650 million to settle a class action lawsuit alleging that it had collected and used biometric data of Illinois residents without their consent in violation of the Illinois Biometric Information Privacy Act (BIPA). The settlement is one of the largest settlements in the history of privacy litigation, and has sent a strong message to organizations that process biometric data that they must comply with the law.

The third landmark judgment is the Riley v. California case (573 U.S. 373, 2014), which was decided by the US Supreme Court. In this case, the US Supreme Court held that the police must obtain a warrant before searching the digital contents of a cell phone seized during an arrest. The US Supreme Court held that the digital contents of a cell phone are qualitatively different from physical items that may be seized during an arrest, and that the search of the digital contents of a cell phone is a significant intrusion on the privacy of the individual. This judgment has had a significant impact on the interpretation of biometric data protection laws, as it recognizes the principle that the digital contents of electronic devices are entitled to enhanced protection.

The fourth landmark judgment is the Carpenter v. United States case (585 U.S. ___, 2018), which was also decided by the US Supreme Court. In this case, the US Supreme Court held that the government must obtain a warrant before accessing historical cell phone location data. The US Supreme Court held that the historical cell phone location data is entitled to protection under the Fourth Amendment, as it provides a detailed record of the movements of the individual, and that the access to this data is a significant intrusion on the privacy of the individual. This judgment has had a significant impact on the interpretation of biometric data protection laws, as it recognizes the principle that location data is entitled to enhanced protection.

These judgments have established important principles for the protection of biometric data. They have clarified the scope and meaning of biometric data protection laws, and have provided guidance to organizations and individuals on their rights and obligations under the law. However, they have also raised several challenges, including the complexity of the law, the lack of harmonization in its implementation across the states, the limited resources of the enforcement authorities, and the potential for regulatory capture by powerful corporate interests.

The American courts must continue to play a crucial role in the development of biometric data protection law. The courts must ensure that the law is applied consistently and effectively, and that the rights of individuals are protected. The courts must also ensure that the law is adapted to the challenges posed by emerging technologies, such as artificial intelligence, blockchain, and the Internet of Things.

CHAPTER 20: THE ROLE OF EUROPEAN COURTS

The European courts have played a crucial role in the development of biometric data protection law. The European Court of Justice (ECJ) and the European Court of Human Rights (ECHR) have issued several landmark judgments that have clarified the scope and meaning of biometric data protection laws, and have established important principles for the protection of biometric data.

The first landmark judgment is the Google Spain SL case (C-131/12, 2014), also known as the "right to be forgotten" case. In this case, the ECJ held that individuals have the right to request the removal of links to personal information that is inadequate, irrelevant, or no longer relevant from search engine results. The ECJ held that the right to be forgotten is not absolute, and must be balanced against other rights, such as the right to freedom of expression and the right to information. However, the ECJ held that the right to be forgotten takes precedence over the economic interest of the search engine operator and the interest of the public in finding the information, unless the information is of public interest or the individual is a public figure. This judgment has had a significant impact on the interpretation of biometric data protection laws, as it recognizes the principle that individuals have the right to control their personal information, including biometric data.

The second landmark judgment is the Schrems II case (C-311/18, 2020). In this case, the ECJ held that the EU-US Privacy Shield, which was the legal framework for the transfer of personal data from the European Union to the United States, was invalid. The ECJ held that the Privacy Shield did not provide an adequate level of protection for personal data, as it did not limit the access of US authorities to personal data transferred from the European Union, and did not provide effective remedies for individuals whose personal data was accessed by US authorities. The ECJ also held that the Standard Contractual Clauses, which are another legal mechanism for the transfer of personal data to third countries, remain valid, but must be supplemented by additional safeguards where necessary. This judgment has had a significant impact on the interpretation of biometric data protection laws, as it recognizes the principle that the transfer of biometric data to third countries must be subject to strict safeguards.

The third landmark judgment is the Digital Rights Ireland case (C-293/12 and C-594/12, 2014). In this case, the ECJ held that the Data Retention Directive, which required telecommunications providers to retain certain types of data for a specified period, was invalid. The ECJ held that the Data Retention Directive was a serious interference with the fundamental rights to privacy and data protection, and that it was not proportionate to the legitimate aim pursued. This judgment has had a significant impact on the interpretation of biometric data protection laws, as it recognizes the principle that the retention of biometric data must be subject to strict safeguards.

The fourth landmark judgment is the Tele2 Sverige case (C-203/15 and C-698/15, 2016). In this case, the ECJ held that the national laws that required telecommunications providers to retain certain types of data for a specified period were invalid, unless they were subject to strict safeguards. The ECJ held that the retention of data is a serious interference with the fundamental rights to privacy and data protection, and that it must be subject to strict safeguards, including prior review by a court or an independent administrative authority. This judgment has had a significant impact on the interpretation of biometric data protection laws, as it recognizes the principle that the retention of biometric data must be subject to strict safeguards.

The fifth landmark judgment is the La Quadrature du Net case (C-511/18, C-512/18, and C-520/18, 2020). In this case, the ECJ held that the national laws that required telecommunications providers to retain certain types of data for a specified period were valid, but only in specific circumstances, such as the fight against serious crime. The ECJ held that the retention of data must be subject to strict safeguards, including prior review by a court or an independent administrative authority, and that the retention must be limited to what is strictly necessary. This judgment has had a significant impact on the interpretation of biometric data protection laws, as it recognizes the principle that the retention of biometric data must be subject to strict safeguards.

These judgments have established important principles for the protection of biometric data. They have clarified the scope and meaning of biometric data protection laws, and have provided guidance to organizations and individuals on their rights and obligations under the law.

However, they have also raised several challenges, including the complexity of the law, the lack of harmonization in its implementation across the member states, the limited resources of the supervisory authorities, and the potential for regulatory capture by powerful corporate interests.

The European courts must continue to play a crucial role in the development of biometric data protection law. The courts must ensure that the law is applied consistently and effectively, and that the rights of individuals are protected. The courts must also ensure that the law is adapted to the challenges posed by emerging technologies, such as artificial intelligence, blockchain, and the Internet of Things.

CHAPTER 21: CIVIL LIABILITY IN THE ARAB LEGAL SYSTEMS

Civil liability in the Arab legal systems for biometric data breach is one of the most complex and contested issues in contemporary legal scholarship. The Arab legal systems have been slower to develop comprehensive frameworks for civil liability for biometric data breach, and most Arab countries rely on general civil liability provisions, which may not provide adequate protection for individuals whose biometric data has been breached.

The Egyptian legal system provides a developing framework for civil liability for biometric data breach. The Egyptian Civil Code includes several provisions on civil liability, including Article 163, which provides that whoever causes damage to another person shall be liable to compensate for the damage. The Egyptian Personal Data Protection Law No. 151 of 2020 also includes several provisions on civil liability, including Article 28, which provides that whoever violates the provisions of the law shall be liable to compensate for the damage caused by the violation. However, the Egyptian legal system does not provide specific provisions on civil liability for biometric data breach, and the courts have not issued landmark judgments on this issue.

The Saudi Arabian legal system provides a developing framework for civil liability for biometric data breach. The Saudi Arabian Civil Code includes several provisions on civil liability, including Article 142, which provides that whoever causes damage to another person shall be liable to compensate for the damage. The Saudi Arabian Personal Data Protection Law of 2021 also includes several provisions on civil liability, including Article 24, which provides that whoever violates the provisions of the law shall be liable to compensate for the damage caused by the violation. However, the Saudi Arabian legal system does not provide specific provisions on civil liability for biometric data breach, and the courts have not issued landmark judgments on this issue.

The United Arab Emirates legal system provides a developing framework for civil liability for biometric data breach. The UAE Civil Code includes several provisions on civil liability, including Article 282, which provides that whoever causes damage to another person shall be liable to compensate for the damage. The UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data also includes several provisions on civil liability, including Article 24, which

provides that whoever violates the provisions of the law shall be liable to compensate for the damage caused by the violation. However, the UAE legal system does not provide specific provisions on civil liability for biometric data breach, and the courts have not issued landmark judgments on this issue.

The Qatari legal system provides a developing framework for civil liability for biometric data breach. The Qatari Civil Code includes several provisions on civil liability, including Article 220, which provides that whoever causes damage to another person shall be liable to compensate for the damage. The Qatari Personal Data Protection Law No. 13 of 2016 also includes several provisions on civil liability, including Article 22, which provides that whoever violates the provisions of the law shall be liable to compensate for the damage caused by the violation. However, the Qatari legal system does not provide specific provisions on civil liability for biometric data breach, and the courts have not issued landmark judgments on this issue.

The Bahraini legal system provides a developing framework for civil liability for biometric data breach. The Bahraini Civil Code includes several provisions on civil liability, including Article 182, which provides that whoever causes damage to another person shall be liable to compensate for the damage. The Bahraini Personal Data Protection Law No. 30 of 2018 also includes several provisions on civil liability, including Article 28, which provides that whoever violates the provisions of the law shall be liable to compensate for the damage caused by the violation. However, the Bahraini legal system does not provide specific provisions on civil liability for biometric data breach, and the courts have not issued landmark judgments on this issue.

The Kuwaiti legal system provides a developing framework for civil liability for biometric data breach. The Kuwaiti Civil Code includes several provisions on civil liability, including Article 265, which provides that whoever causes damage to another person shall be liable to compensate for the damage. The Kuwaiti Personal Data Protection Law No. 20 of 2020 also includes several provisions on civil liability, including Article 22, which provides that whoever violates the provisions of the law shall be liable to compensate for the damage caused by the violation. However, the Kuwaiti legal system does not provide specific provisions on civil liability for biometric data breach, and the courts have not issued landmark judgments on this issue.

The Omani legal system provides a developing framework for civil liability for biometric data breach. The Omani Civil Code includes several provisions on civil liability, including Article 170, which provides that whoever causes damage to another person shall be liable to compensate for the damage. The Omani Personal Data Protection Law issued by Royal Decree No. 69 of 2022 also includes several provisions on civil liability, including Article 24, which provides that whoever violates the provisions of the law shall be liable to compensate for the damage caused by the violation. However, the Omani legal system does not provide specific provisions on civil liability for biometric data breach, and the courts have not issued landmark judgments on this issue.

The civil liability in the Arab legal systems for biometric data breach must be reformed to address these challenges. This reform must include specific provisions on civil liability for biometric data breach, a clear definition of harm, a comprehensive framework for the allocation of liability, and meaningful remedies for violations. The reform must also address the specific challenges posed by emerging technologies, such as artificial intelligence, blockchain, and the Internet of Things.

CHAPTER 22: ALTERNATIVE DISPUTE RESOLUTION FOR BIOMETRIC DATA DISPUTES

Alternative dispute resolution (ADR) for biometric data disputes is an emerging field that offers several advantages over traditional litigation. ADR includes several mechanisms, such as mediation, arbitration, and online dispute resolution (ODR), which can provide faster, cheaper, and more flexible solutions to biometric data disputes.

Mediation is a voluntary process in which a neutral third party, the mediator, assists the parties in reaching a mutually acceptable agreement. Mediation is particularly suitable for biometric data disputes, as it allows the parties to maintain control over the outcome of the dispute, and to preserve their relationships. Mediation is also confidential, which is particularly important for biometric data disputes, as it protects the privacy of the parties.

Arbitration is a process in which the parties submit their dispute to one or more arbitrators, who render a binding decision. Arbitration is particularly suitable for biometric data disputes, as it allows the parties to choose arbitrators with expertise in biometric data protection, and to obtain a faster and cheaper resolution than traditional litigation. Arbitration is also confidential, which is particularly important for biometric data disputes, as it protects the privacy of the parties.

Online dispute resolution (ODR) is a process in which the parties submit their dispute to an online platform, which assists them in reaching a resolution. ODR is particularly suitable for biometric data disputes, as it allows the parties to resolve their disputes from anywhere in the world, and to obtain a faster and cheaper resolution than traditional litigation. ODR is also confidential, which is particularly important for biometric data disputes, as it protects the privacy of the parties.

The European Union has adopted several mechanisms for ADR for biometric data disputes. The General Data Protection Regulation (GDPR) encourages the use of ADR for data protection disputes, and provides for the establishment of ADR mechanisms by the member states. The GDPR also provides for the right to lodge a complaint with a supervisory authority, which can assist the parties in reaching a resolution.

The United States has adopted several mechanisms for ADR for biometric data disputes. Some states, such as California, provide for the establishment of ADR mechanisms for data protection disputes. The Federal Trade Commission (FTC) also encourages the use of ADR for data

protection disputes, and provides for the establishment of ADR mechanisms by the organizations that process personal data.

The Arab legal systems have been slower to adopt mechanisms for ADR for biometric data disputes. Most Arab countries rely on traditional litigation for the resolution of biometric data disputes, which can be slow, expensive, and inflexible. However, recent developments in countries such as the United Arab Emirates and Saudi Arabia indicate a growing recognition of the potential benefits of ADR for biometric data disputes.

The ADR for biometric data disputes must be reformed to address these challenges. This reform must include the establishment of comprehensive ADR mechanisms for biometric data disputes, the training of mediators and arbitrators with expertise in biometric data protection, and the promotion of the use of ADR for biometric data disputes. The reform must also address the specific challenges posed by emerging technologies, such as artificial intelligence, blockchain, and the Internet of Things.

CHAPTER 23: THE FUTURE OF PROTECTION IN THE AGE OF ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN

The future of biometric data protection in the age of artificial intelligence and blockchain is one of the most complex and contested issues in contemporary legal scholarship. The emergence of these technologies raises fundamental questions about the nature of biometric data, the limits of state and corporate power, and the potential for mass surveillance and discrimination.

Artificial intelligence (AI) has the potential to revolutionize the processing of biometric data. AI can be used to analyze large volumes of biometric data, to identify patterns and trends, and to make predictions about the behavior of individuals. However, AI also raises several challenges for biometric data protection. First, AI can be used to create deepfakes, which are synthetic biometric data that can be used to impersonate individuals. Second, AI can be used to create biometric profiles, which can be used to discriminate against individuals based on their biometric characteristics. Third, AI can be used to create biometric surveillance systems, which can be used to monitor the movements and activities of individuals.

Blockchain has the potential to revolutionize the storage and transfer of biometric data. Blockchain can be used to create secure and transparent systems for the storage and transfer of biometric data, which can protect the privacy and security of individuals. However, blockchain also raises several challenges for biometric data protection. First, blockchain can be used to create immutable records of biometric data, which can be used to track the movements and activities of individuals. Second, blockchain can be used to create decentralized systems for the processing of biometric data, which can be used to circumvent the protections of the law. Third, blockchain can be used to create self-sovereign biometric identity systems, which can be used to empower individuals to control their biometric data, but can also be used to create new forms of exclusion and discrimination.

The European Union has adopted several measures to address the challenges posed by AI and blockchain for biometric data protection. The General Data Protection Regulation (GDPR) includes several provisions on automated decision-making, which can be used to regulate the use of AI for the processing of biometric data. The GDPR also includes several provisions on data portability, which can be used to regulate the use of blockchain for the transfer of biometric data. The European Union has also adopted the Artificial Intelligence Act, which is currently under development, and which will provide a comprehensive framework for the regulation of AI, including the use of AI for the processing of biometric data.

The United States has been slower to address the challenges posed by AI and blockchain for biometric data protection. Some states, such as California, have adopted data protection laws that include some provisions on automated decision-making and data portability, but do not provide the same level of protection as the GDPR. The Federal Trade Commission (FTC) has also issued guidance on the use of AI and blockchain for the processing of personal data, but does not have the power to issue binding regulations.

The Arab legal systems have been slower to address the challenges posed by AI and blockchain for biometric data protection. Most Arab countries rely on general data protection laws, which do not address the specific challenges posed by AI and blockchain. However, recent developments in countries such as the United Arab Emirates and Saudi Arabia indicate a growing recognition of the need to address these challenges.

The future of biometric data protection in the age of AI and blockchain must be addressed through comprehensive legal frameworks that recognize the unique characteristics of these technologies and the fundamental rights of the human person. These frameworks must include strict requirements for informed consent, data minimization, purpose limitation, and accountability, as well as effective enforcement mechanisms and meaningful remedies for violations. The frameworks must also address the specific challenges posed by emerging technologies, such as deepfakes, biometric profiles, biometric surveillance systems, immutable records of biometric data, decentralized systems for the processing of biometric data, and self-sovereign biometric identity systems.

PART FIVE: THE EL RAKHAWI DOCTRINE AND NEW FRONTIERS

CHAPTER 24: THE EL RAKHAWI PRINCIPLE OF SOVEREIGN BIOMETRIC DIGNITY

The El Rakhawi Principle of Sovereign Biometric Dignity represents a groundbreaking jurisprudential contribution to the field of biometric data protection. This principle recognizes that biometric data is not merely information about a person, but the digital mirror of the human soul, and that the protection of biometric data is a fundamental aspect of human dignity and personal sovereignty.

The El Rakhawi Principle of Sovereign Biometric Dignity is built upon several foundational pillars:

First, the principle of biometric inviolability. The human face, fingerprint, iris pattern, voice, and gait are not mere data points but the physical manifestation of human uniqueness. Any legal framework that treats them as ordinary personal data fails to grasp their existential significance. The biometric data of an individual must be treated with the same respect and protection as the physical body of the individual.

Second, the principle of cognitive biometric sovereignty. The individual has the absolute right to control their biometric data, including the right to decide whether, when, how, and for what purposes their biometric data is collected, processed, and shared. This right is not subject to any limitation except where necessary to protect the rights and freedoms of others, or to achieve a legitimate aim that is proportionate to the interference with the right.

Third, the principle of dynamic informed consent. The consent for the processing of biometric data must be freely given, specific, informed, and unambiguous, and must be subject to continuous review and revocation. The individual must be provided with clear and comprehensive information about the processing of their biometric data, including the purposes, the legal basis, the recipients, the retention period, and the rights of the individual. The individual must also be provided with the means to exercise their rights, including the right to access, rectify, erase, restrict, port, and object to the processing of their biometric data.

Fourth, the principle of proportionality and necessity. The processing of biometric data must be necessary and proportionate to the legitimate aim pursued. The processing of biometric data must be limited to what is strictly necessary for the achievement of the legitimate aim, and must not be used for any other purpose. The processing of biometric data must also be subject to strict safeguards, including prior review by a court or an independent administrative authority, and must be limited to what is strictly necessary.

Fifth, the principle of accountability and transparency. The controller and the processor of biometric data must be held responsible for their actions, and must be able to demonstrate compliance with the law. The controller and the processor must also be transparent about their processing of biometric data, and must provide clear and comprehensive information about the processing, including the purposes, the legal basis, the recipients, the retention period, and the rights of the individual.

Sixth, the principle of remedy and redress. The individual whose biometric data has been processed in violation of the law must have access to effective remedies, including compensation for material and non-material damage, injunctive relief, and punitive damages. The individual must also have access to effective redress mechanisms, including the right to lodge a complaint with a supervisory authority, the right to an effective judicial remedy against a supervisory authority, and the right to an effective judicial remedy against a controller or processor.

The El Rakhawi Principle of Sovereign Biometric Dignity represents a comprehensive and sophisticated framework for the protection of biometric data. This principle recognizes the unique characteristics of biometric data and the fundamental rights of the human person, and provides a clear and comprehensive framework for the regulation of the processing of biometric data. This principle must be adopted and implemented by all legal systems around the world, and must be adapted to the challenges posed by emerging technologies, such as artificial intelligence, blockchain, and the Internet of Things.

CHAPTER 25: POST-MORTEM BIOMETRIC DATA PROTECTION

Post-mortem biometric data protection is one of the most complex and contested issues in contemporary legal scholarship. The question of whether and how the biometric data of a deceased person should be protected raises fundamental questions about the nature of human dignity, the limits of personal autonomy, and the rights of the surviving family members.

The first challenge is the nature of post-mortem biometric data. The biometric data of a deceased person can include a variety of information, such as facial images, fingerprints, DNA profiles, voice recordings, and other biometric identifiers. This information can be used for a variety of purposes, including identification, forensic investigation, medical research, and historical preservation. However, the use of post-mortem biometric data also raises several challenges, including the potential for identity theft, the potential for discrimination, and the potential for violation of the dignity of the deceased person and the surviving family members.

The second challenge is the legal status of post-mortem biometric data. The question of whether the biometric data of a deceased person is subject to data protection laws depends on the specific legal framework of the jurisdiction. In the European Union, the General Data Protection Regulation (GDPR) does not apply to the personal data of deceased persons, but the member states may provide for rules regarding the processing of personal data of deceased persons. In the United States, the question of whether the biometric data of a deceased person is subject to data protection laws depends on the specific state law. In the Arab legal systems, the question of whether the biometric data of a deceased person is subject to data protection laws depends on the specific national law.

The third challenge is the rights of the surviving family members. The surviving family members of a deceased person may have several rights in relation to the biometric data of the deceased person, including the right to access, rectify, erase, restrict, port, and object to the processing of the biometric data. However, the question of whether and how these rights should be recognized depends on the specific legal framework of the jurisdiction, and on the specific circumstances of the case.

The fourth challenge is the legitimate interests of third parties. Third parties, such as law enforcement agencies, medical researchers, and historical institutions, may have legitimate

interests in the processing of post-mortem biometric data. However, the question of whether and how these interests should be recognized depends on the specific legal framework of the jurisdiction, and on the specific circumstances of the case.

The European Union has adopted a fragmented approach to post-mortem biometric data protection. The General Data Protection Regulation (GDPR) does not apply to the personal data of deceased persons, but the member states may provide for rules regarding the processing of personal data of deceased persons. Some member states, such as France and Italy, have adopted specific provisions on post-mortem data protection, which recognize the rights of the surviving family members and the legitimate interests of third parties. Other member states, such as Germany and the United Kingdom, have not adopted specific provisions on post-mortem data protection, and rely on general civil law provisions.

The United States has adopted a fragmented approach to post-mortem biometric data protection. Some states, such as California, have adopted specific provisions on post-mortem data protection, which recognize the rights of the surviving family members and the legitimate interests of third parties. Other states, such as Illinois and Texas, have not adopted specific provisions on post-mortem data protection, and rely on general civil law provisions.

The Arab legal systems have been slower to adopt specific provisions on post-mortem biometric data protection. Most Arab countries rely on general civil law provisions, which may not provide adequate protection for the biometric data of deceased persons. However, recent developments in countries such as Egypt and Saudi Arabia indicate a growing recognition of the need to address this issue.

The post-mortem biometric data protection must be reformed to address these challenges. This reform must include specific provisions on post-mortem biometric data protection, a clear definition of the rights of the surviving family members, a comprehensive framework for the recognition of the legitimate interests of third parties, and meaningful remedies for violations. The reform must also address the specific challenges posed by emerging technologies, such as artificial intelligence, blockchain, and the Internet of Things.

CHAPTER 26: BIOMETRIC DATA OF MINORS AND VULNERABLE POPULATIONS

The biometric data of minors and vulnerable populations is one of the most complex and contested issues in contemporary legal scholarship. The question of whether and how the biometric data of minors and vulnerable populations should be protected raises fundamental questions about the nature of human dignity, the limits of parental authority, and the rights of the individual.

The first challenge is the nature of the biometric data of minors and vulnerable populations. The biometric data of minors and vulnerable populations can include a variety of information, such as facial images, fingerprints, DNA profiles, voice recordings, and other biometric identifiers.

This information can be used for a variety of purposes, including identification, education, health care, and social services. However, the use of biometric data of minors and vulnerable populations also raises several challenges, including the potential for identity theft, the potential for discrimination, and the potential for violation of the dignity and autonomy of the individual.

The second challenge is the legal status of the biometric data of minors and vulnerable populations. The question of whether the biometric data of minors and vulnerable populations is subject to data protection laws depends on the specific legal framework of the jurisdiction. In the European Union, the General Data Protection Regulation (GDPR) provides specific protections for the biometric data of minors and vulnerable populations. Article 8 of the GDPR provides that the processing of personal data of a child under the age of 16 is lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child. Article 9 of the GDPR provides that the processing of biometric data for the purpose of uniquely identifying a natural person is prohibited, except in specific circumstances, such as explicit consent, employment law obligations, vital interests, legitimate activities of a body or association, manifestly public data, legal claims, substantial public interest, health or social care, public health, archiving, research, or statistics.

The third challenge is the rights of minors and vulnerable populations. Minors and vulnerable populations have several rights in relation to their biometric data, including the right to access, rectify, erase, restrict, port, and object to the processing of their biometric data. However, the question of whether and how these rights should be recognized depends on the specific legal framework of the jurisdiction, and on the specific circumstances of the case.

The fourth challenge is the legitimate interests of third parties. Third parties, such as parents, educational institutions, health care providers, and social services, may have legitimate interests in the processing of biometric data of minors and vulnerable populations. However, the question of whether and how these interests should be recognized depends on the specific legal framework of the jurisdiction, and on the specific circumstances of the case.

The European Union has adopted a comprehensive approach to the protection of the biometric data of minors and vulnerable populations. The General Data Protection Regulation (GDPR) provides specific protections for the biometric data of minors and vulnerable populations, including the requirement for parental consent for the processing of biometric data of children under the age of 16, and the prohibition of the processing of biometric data for the purpose of uniquely identifying a natural person, except in specific circumstances.

The United States has adopted a fragmented approach to the protection of the biometric data of minors and vulnerable populations. Some states, such as Illinois, have adopted specific provisions on the protection of the biometric data of minors, which require parental consent for the collection of biometric data of minors. Other states, such as California, have adopted specific provisions on the protection of the biometric data of minors, which recognize the rights of minors and the legitimate interests of third parties.

The Arab legal systems have been slower to adopt specific provisions on the protection of the biometric data of minors and vulnerable populations. Most Arab countries rely on general data protection laws, which do not address the specific challenges posed by the biometric data of minors and vulnerable populations. However, recent developments in countries such as Egypt and Saudi Arabia indicate a growing recognition of the need to address this issue.

The protection of the biometric data of minors and vulnerable populations must be reformed to address these challenges. This reform must include specific provisions on the protection of the biometric data of minors and vulnerable populations, a clear definition of the rights of minors and vulnerable populations, a comprehensive framework for the recognition of the legitimate interests of third parties, and meaningful remedies for violations. The reform must also address the specific challenges posed by emerging technologies, such as artificial intelligence, blockchain, and the Internet of Things.

CHAPTER 27: THE INTERSECTION OF BIOMETRIC DATA AND GENERATIVE AI

The intersection of biometric data and generative AI is one of the most complex and contested issues in contemporary legal scholarship. The emergence of generative AI technologies, such as deepfakes and synthetic biometric data, raises fundamental questions about the nature of biometric data, the limits of state and corporate power, and the potential for mass surveillance and discrimination.

The first challenge is the nature of generative AI. Generative AI refers to artificial intelligence systems that can generate new content, such as images, videos, audio, and text, based on patterns learned from data. Generative AI can be used to create deepfakes, which are synthetic biometric data that can be used to impersonate individuals. Deepfakes can be used for a variety of purposes, including entertainment, education, and artistic expression. However, deepfakes can also be used for malicious purposes, including identity theft, fraud, defamation, and political manipulation.

The second challenge is the legal status of deepfakes and synthetic biometric data. The question of whether deepfakes and synthetic biometric data are subject to data protection laws depends on the specific legal framework of the jurisdiction. In the European Union, the General Data Protection Regulation (GDPR) applies to the processing of personal data, including biometric data, regardless of whether the data is real or synthetic. The GDPR also includes several provisions on automated decision-making, which can be used to regulate the use of generative AI for the processing of biometric data. In the United States, the question of whether deepfakes and synthetic biometric data are subject to data protection laws depends on the specific state law. Some states, such as California and Texas, have adopted specific provisions on deepfakes, which recognize the rights of individuals and the legitimate interests of third parties.

The third challenge is the rights of individuals whose biometric data is used to create deepfakes and synthetic biometric data. Individuals whose biometric data is used to create deepfakes and synthetic biometric data have several rights, including the right to access, rectify, erase, restrict, port, and object to the processing of their biometric data. However, the question of whether and how these rights should be recognized depends on the specific legal framework of the jurisdiction, and on the specific circumstances of the case.

The fourth challenge is the legitimate interests of third parties. Third parties, such as entertainment companies, educational institutions, and artistic organizations, may have legitimate interests in the use of generative AI for the creation of deepfakes and synthetic biometric data. However, the question of whether and how these interests should be recognized depends on the specific legal framework of the jurisdiction, and on the specific circumstances of the case.

The European Union has adopted several measures to address the challenges posed by generative AI for biometric data protection. The General Data Protection Regulation (GDPR) includes several provisions on automated decision-making, which can be used to regulate the use of generative AI for the processing of biometric data. The European Union has also adopted the Artificial Intelligence Act, which is currently under development, and which will provide a comprehensive framework for the regulation of AI, including the use of generative AI for the processing of biometric data. The European Union has also adopted the Digital Services Act and the Digital Markets Act, which include several provisions on the regulation of online platforms and the use of AI for the processing of personal data.

The United States has been slower to address the challenges posed by generative AI for biometric data protection. Some states, such as California and Texas, have adopted specific provisions on deepfakes, which recognize the rights of individuals and the legitimate interests of third parties. The Federal Trade Commission (FTC) has also issued guidance on the use of AI for the processing of personal data, but does not have the power to issue binding regulations.

The Arab legal systems have been slower to address the challenges posed by generative AI for biometric data protection. Most Arab countries rely on general data protection laws, which do not address the specific challenges posed by generative AI. However, recent developments in countries such as the United Arab Emirates and Saudi Arabia indicate a growing recognition of the need to address these challenges.

The intersection of biometric data and generative AI must be addressed through comprehensive legal frameworks that recognize the unique characteristics of these technologies and the fundamental rights of the human person. These frameworks must include strict requirements for informed consent, data minimization, purpose limitation, and accountability, as well as effective enforcement mechanisms and meaningful remedies for violations. The frameworks must also address the specific challenges posed by emerging technologies, such as deepfakes, synthetic biometric data, and other forms of generative AI.

CHAPTER 28: THE DIGITAL BIOMETRIC FOOTPRINT AND COGNITIVE SOVEREIGNTY

The digital biometric footprint and cognitive sovereignty is one of the most complex and contested issues in contemporary legal scholarship. The question of whether and how the digital biometric footprint of an individual should be protected raises fundamental questions about the nature of human dignity, the limits of state and corporate power, and the potential for mass surveillance and discrimination.

The first challenge is the nature of the digital biometric footprint. The digital biometric footprint refers to the collection of biometric data that is generated by an individual through their interactions with digital systems, such as facial recognition systems, fingerprint scanners, voice recognition systems, and other biometric technologies. The digital biometric footprint can include a variety of information, such as facial images, fingerprints, voice recordings, gait patterns, and other biometric identifiers. This information can be used for a variety of purposes, including identification, authentication, personalization, and profiling. However, the use of the digital biometric footprint also raises several challenges, including the potential for identity theft, the potential for discrimination, and the potential for violation of the dignity and autonomy of the individual.

The second challenge is the legal status of the digital biometric footprint. The question of whether the digital biometric footprint is subject to data protection laws depends on the specific legal framework of the jurisdiction. In the European Union, the General Data Protection Regulation (GDPR) applies to the processing of personal data, including biometric data, regardless of whether the data is collected directly from the individual or generated through their interactions with digital systems. The GDPR also includes several provisions on automated decision-making, which can be used to regulate the use of the digital biometric footprint for the processing of biometric data. In the United States, the question of whether the digital biometric footprint is subject to data protection laws depends on the specific state law. Some states, such as Illinois and California, have adopted specific provisions on the protection of biometric data, which recognize the rights of individuals and the legitimate interests of third parties.

The third challenge is the rights of individuals in relation to their digital biometric footprint. Individuals have several rights in relation to their digital biometric footprint, including the right to access, rectify, erase, restrict, port, and object to the processing of their biometric data. However, the question of whether and how these rights should be recognized depends on the specific legal framework of the jurisdiction, and on the specific circumstances of the case.

The fourth challenge is the legitimate interests of third parties. Third parties, such as technology companies, educational institutions, and health care providers, may have legitimate interests in the processing of the digital biometric footprint of individuals. However, the question of whether and how these interests should be recognized depends on the specific legal framework of the jurisdiction, and on the specific circumstances of the case.

The European Union has adopted several measures to address the challenges posed by the digital biometric footprint for biometric data protection. The General Data Protection Regulation (GDPR) includes several provisions on automated decision-making, which can be used to regulate the use of the digital biometric footprint for the processing of biometric data. The European Union has also adopted the Artificial Intelligence Act, which is currently under development, and which will provide a comprehensive framework for the regulation of AI, including the use of the digital biometric footprint for the processing of biometric data. The European Union has also adopted the Digital Services Act and the Digital Markets Act, which include several provisions on the regulation of online platforms and the use of AI for the processing of personal data.

The United States has been slower to address the challenges posed by the digital biometric footprint for biometric data protection. Some states, such as Illinois and California, have adopted specific provisions on the protection of biometric data, which recognize the rights of individuals and the legitimate interests of third parties. The Federal Trade Commission (FTC) has also issued guidance on the use of AI for the processing of personal data, but does not have the power to issue binding regulations.

The Arab legal systems have been slower to address the challenges posed by the digital biometric footprint for biometric data protection. Most Arab countries rely on general data protection laws, which do not address the specific challenges posed by the digital biometric footprint. However, recent developments in countries such as the United Arab Emirates and Saudi Arabia indicate a growing recognition of the need to address these challenges.

The digital biometric footprint and cognitive sovereignty must be addressed through comprehensive legal frameworks that recognize the unique characteristics of these technologies and the fundamental rights of the human person. These frameworks must include strict requirements for informed consent, data minimization, purpose limitation, and accountability, as well as effective enforcement mechanisms and meaningful remedies for violations. The frameworks must also address the specific challenges posed by emerging technologies, such as facial recognition systems, fingerprint scanners, voice recognition systems, and other biometric technologies.

CHAPTER 29: SELF-SOVEREIGN BIOMETRIC IDENTITY IN THE BLOCKCHAIN ERA

Self-sovereign biometric identity in the blockchain era is one of the most complex and contested issues in contemporary legal scholarship. The question of whether and how self-sovereign biometric identity systems should be regulated raises fundamental questions about the nature of human dignity, the limits of state and corporate power, and the potential for mass surveillance and discrimination.

The first challenge is the nature of self-sovereign biometric identity. Self-sovereign biometric identity refers to a system in which individuals have the absolute control over their biometric

data, including the right to decide whether, when, how, and for what purposes their biometric data is collected, processed, and shared. Self-sovereign biometric identity systems can be implemented using blockchain technology, which provides a secure and transparent system for the storage and transfer of biometric data. However, self-sovereign biometric identity systems also raise several challenges, including the potential for identity theft, the potential for discrimination, and the potential for violation of the dignity and autonomy of the individual.

The second challenge is the legal status of self-sovereign biometric identity systems. The question of whether self-sovereign biometric identity systems are subject to data protection laws depends on the specific legal framework of the jurisdiction. In the European Union, the General Data Protection Regulation (GDPR) applies to the processing of personal data, including biometric data, regardless of whether the data is stored on a centralized or decentralized system. The GDPR also includes several provisions on data portability, which can be used to regulate the use of blockchain for the transfer of biometric data. In the United States, the question of whether self-sovereign biometric identity systems are subject to data protection laws depends on the specific state law. Some states, such as California, have adopted specific provisions on data portability, which recognize the rights of individuals and the legitimate interests of third parties.

The third challenge is the rights of individuals in relation to their self-sovereign biometric identity. Individuals have several rights in relation to their self-sovereign biometric identity, including the right to access, rectify, erase, restrict, port, and object to the processing of their biometric data. However, the question of whether and how these rights should be recognized depends on the specific legal framework of the jurisdiction, and on the specific circumstances of the case.

The fourth challenge is the legitimate interests of third parties. Third parties, such as technology companies, educational institutions, and health care providers, may have legitimate interests in the processing of biometric data in self-sovereign biometric identity systems. However, the question of whether and how these interests should be recognized depends on the specific legal framework of the jurisdiction, and on the specific circumstances of the case.

The European Union has adopted several measures to address the challenges posed by self-sovereign biometric identity systems for biometric data protection. The General Data Protection Regulation (GDPR) includes several provisions on data portability, which can be used to regulate the use of blockchain for the transfer of biometric data. The European Union has also adopted the European Digital Identity Framework, which is currently under development, and which will provide a comprehensive framework for the regulation of digital identity, including the use of self-sovereign biometric identity systems. The European Union has also adopted the Digital Services Act and the Digital Markets Act, which include several provisions on the regulation of online platforms and the use of AI for the processing of personal data.

The United States has been slower to address the challenges posed by self-sovereign biometric identity systems for biometric data protection. Some states, such as California, have adopted specific provisions on data portability, which recognize the rights of individuals and the

legitimate interests of third parties. The Federal Trade Commission (FTC) has also issued guidance on the use of blockchain for the processing of personal data, but does not have the power to issue binding regulations.

The Arab legal systems have been slower to address the challenges posed by self-sovereign biometric identity systems for biometric data protection. Most Arab countries rely on general data protection laws, which do not address the specific challenges posed by self-sovereign biometric identity systems. However, recent developments in countries such as the United Arab Emirates and Saudi Arabia indicate a growing recognition of the need to address these challenges.

Self-sovereign biometric identity in the blockchain era must be addressed through comprehensive legal frameworks that recognize the unique characteristics of these technologies and the fundamental rights of the human person. These frameworks must include strict requirements for informed consent, data minimization, purpose limitation, and accountability, as well as effective enforcement mechanisms and meaningful remedies for violations. The frameworks must also address the specific challenges posed by emerging technologies, such as blockchain, distributed ledger technology, and other forms of decentralized systems.

CHAPTER 30: EMERGENCY BIOMETRIC DATA COLLECTION AND PROPORTIONALITY

Emergency biometric data collection and proportionality is one of the most complex and contested issues in contemporary legal scholarship. The question of whether and how biometric data should be collected in emergency situations, such as pandemics, natural disasters, and terrorist attacks, raises fundamental questions about the nature of human dignity, the limits of state power, and the potential for mass surveillance and discrimination.

The first challenge is the nature of emergency biometric data collection. Emergency biometric data collection refers to the collection of biometric data in emergency situations, such as pandemics, natural disasters, and terrorist attacks. Emergency biometric data collection can include a variety of information, such as facial images, fingerprints, DNA profiles, voice recordings, and other biometric identifiers. This information can be used for a variety of purposes, including identification, contact tracing, and disaster response. However, emergency biometric data collection also raises several challenges, including the potential for identity theft, the potential for discrimination, and the potential for violation of the dignity and autonomy of the individual.

The second challenge is the legal status of emergency biometric data collection. The question of whether emergency biometric data collection is subject to data protection laws depends on the specific legal framework of the jurisdiction. In the European Union, the General Data Protection Regulation (GDPR) applies to the processing of personal data, including biometric data, regardless of whether the data is collected in normal or emergency situations. The GDPR also includes several provisions on the processing of biometric data for the purpose of uniquely

identifying a natural person, which can be used to regulate the use of emergency biometric data collection. In the United States, the question of whether emergency biometric data collection is subject to data protection laws depends on the specific state law. Some states, such as Illinois and California, have adopted specific provisions on the protection of biometric data, which recognize the rights of individuals and the legitimate interests of third parties.

The third challenge is the rights of individuals in relation to emergency biometric data collection. Individuals have several rights in relation to emergency biometric data collection, including the right to access, rectify, erase, restrict, port, and object to the processing of their biometric data. However, the question of whether and how these rights should be recognized depends on the specific legal framework of the jurisdiction, and on the specific circumstances of the case.

The fourth challenge is the legitimate interests of third parties. Third parties, such as public health authorities, emergency response agencies, and law enforcement agencies, may have legitimate interests in the processing of biometric data in emergency situations. However, the question of whether and how these interests should be recognized depends on the specific legal framework of the jurisdiction, and on the specific circumstances of the case.

The European Union has adopted several measures to address the challenges posed by emergency biometric data collection for biometric data protection. The General Data Protection Regulation (GDPR) includes several provisions on the processing of biometric data for the purpose of uniquely identifying a natural person, which can be used to regulate the use of emergency biometric data collection. The European Union has also adopted the European Digital Identity Framework, which is currently under development, and which will provide a comprehensive framework for the regulation of digital identity, including the use of emergency biometric data collection. The European Union has also adopted the Digital Services Act and the Digital Markets Act, which include several provisions on the regulation of online platforms and the use of AI for the processing of personal data.

The United States has been slower to address the challenges posed by emergency biometric data collection for biometric data protection. Some states, such as Illinois and California, have adopted specific provisions on the protection of biometric data, which recognize the rights of individuals and the legitimate interests of third parties. The Federal Trade Commission (FTC) has also issued guidance on the use of AI for the processing of personal data, but does not have the power to issue binding regulations.

The Arab legal systems have been slower to address the challenges posed by emergency biometric data collection for biometric data protection. Most Arab countries rely on general data protection laws, which do not address the specific challenges posed by emergency biometric data collection. However, recent developments in countries such as Egypt and Saudi Arabia indicate a growing recognition of the need to address these challenges.

Emergency biometric data collection and proportionality must be addressed through comprehensive legal frameworks that recognize the unique characteristics of these technologies

and the fundamental rights of the human person. These frameworks must include strict requirements for informed consent, data minimization, purpose limitation, and accountability, as well as effective enforcement mechanisms and meaningful remedies for violations. The frameworks must also address the specific challenges posed by emerging technologies, such as facial recognition systems, contact tracing systems, and other forms of biometric surveillance.

CHAPTER 31: INTERNATIONAL CYBER SOVEREIGNTY AND BIOMETRIC DATA FLOWS

International cyber sovereignty and biometric data flows is one of the most complex and contested issues in contemporary legal scholarship. The question of whether and how biometric data should be transferred across national borders raises fundamental questions about the nature of human dignity, the limits of state power, and the potential for mass surveillance and discrimination.

The first challenge is the nature of international biometric data flows. International biometric data flows refer to the transfer of biometric data across national borders. International biometric data flows can include a variety of information, such as facial images, fingerprints, DNA profiles, voice recordings, and other biometric identifiers. This information can be used for a variety of purposes, including identification, authentication, personalization, and profiling. However, international biometric data flows also raise several challenges, including the potential for identity theft, the potential for discrimination, and the potential for violation of the dignity and autonomy of the individual.

The second challenge is the legal status of international biometric data flows. The question of whether international biometric data flows are subject to data protection laws depends on the specific legal framework of the jurisdiction. In the European Union, the General Data Protection Regulation (GDPR) applies to the processing of personal data, including biometric data, regardless of whether the data is transferred within the European Union or to third countries. The GDPR also includes several provisions on the transfer of personal data to third countries, which can be used to regulate the use of international biometric data flows. In the United States, the question of whether international biometric data flows are subject to data protection laws depends on the specific state law. Some states, such as Illinois and California, have adopted specific provisions on the protection of biometric data, which recognize the rights of individuals and the legitimate interests of third parties.

The third challenge is the rights of individuals in relation to international biometric data flows. Individuals have several rights in relation to international biometric data flows, including the right to access, rectify, erase, restrict, port, and object to the processing of their biometric data. However, the question of whether and how these rights should be recognized depends on the specific legal framework of the jurisdiction, and on the specific circumstances of the case.

The fourth challenge is the legitimate interests of third parties. Third parties, such as technology companies, educational institutions, and health care providers, may have legitimate interests in the processing of biometric data in international biometric data flows. However, the question of whether and how these interests should be recognized depends on the specific legal framework of the jurisdiction, and on the specific circumstances of the case.

The European Union has adopted several measures to address the challenges posed by international biometric data flows for biometric data protection. The General Data Protection Regulation (GDPR) includes several provisions on the transfer of personal data to third countries, which can be used to regulate the use of international biometric data flows. The European Union has also adopted the European Digital Identity Framework, which is currently under development, and which will provide a comprehensive framework for the regulation of digital identity, including the use of international biometric data flows. The European Union has also adopted the Digital Services Act and the Digital Markets Act, which include several provisions on the regulation of online platforms and the use of AI for the processing of personal data.

The United States has been slower to address the challenges posed by international biometric data flows for biometric data protection. Some states, such as Illinois and California, have adopted specific provisions on the protection of biometric data, which recognize the rights of individuals and the legitimate interests of third parties. The Federal Trade Commission (FTC) has also issued guidance on the use of AI for the processing of personal data, but does not have the power to issue binding regulations.

The Arab legal systems have been slower to address the challenges posed by international biometric data flows for biometric data protection. Most Arab countries rely on general data protection laws, which do not address the specific challenges posed by international biometric data flows. However, recent developments in countries such as the United Arab Emirates and Saudi Arabia indicate a growing recognition of the need to address these challenges.

International cyber sovereignty and biometric data flows must be addressed through comprehensive legal frameworks that recognize the unique characteristics of these technologies and the fundamental rights of the human person. These frameworks must include strict requirements for informed consent, data minimization, purpose limitation, and accountability, as well as effective enforcement mechanisms and meaningful remedies for violations. The frameworks must also address the specific challenges posed by emerging technologies, such as blockchain, distributed ledger technology, and other forms of decentralized systems.

CHAPTER 32: THE METAPHYSICAL DIMENSIONS OF BIOMETRIC DATA PROTECTION

The metaphysical dimensions of biometric data protection is one of the most complex and contested issues in contemporary legal scholarship. The question of whether and how biometric data should be protected from a metaphysical perspective raises fundamental questions about

the nature of human dignity, the limits of state and corporate power, and the potential for mass surveillance and discrimination.

The first challenge is the nature of the metaphysical dimensions of biometric data protection. The metaphysical dimensions of biometric data protection refer to the philosophical and spiritual aspects of biometric data protection. The metaphysical dimensions of biometric data protection can include a variety of perspectives, such as the recognition of biometric data as the digital mirror of the human soul, the recognition of biometric data as a fundamental aspect of human dignity and personal sovereignty, and the recognition of biometric data as a sacred trust that must be protected with the utmost care and respect.

The second challenge is the legal status of the metaphysical dimensions of biometric data protection. The question of whether the metaphysical dimensions of biometric data protection are subject to data protection laws depends on the specific legal framework of the jurisdiction. In the European Union, the General Data Protection Regulation (GDPR) applies to the processing of personal data, including biometric data, regardless of whether the data is protected from a metaphysical perspective. The GDPR also includes several provisions on the processing of biometric data for the purpose of uniquely identifying a natural person, which can be used to regulate the use of biometric data from a metaphysical perspective. In the United States, the question of whether the metaphysical dimensions of biometric data protection are subject to data protection laws depends on the specific state law. Some states, such as Illinois and California, have adopted specific provisions on the protection of biometric data, which recognize the rights of individuals and the legitimate interests of third parties.

The third challenge is the rights of individuals in relation to the metaphysical dimensions of biometric data protection. Individuals have several rights in relation to the metaphysical dimensions of biometric data protection, including the right to access, rectify, erase, restrict, port, and object to the processing of their biometric data. However, the question of whether and how these rights should be recognized depends on the specific legal framework of the jurisdiction, and on the specific circumstances of the case.

The fourth challenge is the legitimate interests of third parties. Third parties, such as technology companies, educational institutions, and health care providers, may have legitimate interests in the processing of biometric data from a metaphysical perspective. However, the question of whether and how these interests should be recognized depends on the specific legal framework of the jurisdiction, and on the specific circumstances of the case.

The European Union has adopted several measures to address the challenges posed by the metaphysical dimensions of biometric data protection for biometric data protection. The General Data Protection Regulation (GDPR) includes several provisions on the processing of biometric data for the purpose of uniquely identifying a natural person, which can be used to regulate the use of biometric data from a metaphysical perspective. The European Union has also adopted the European Digital Identity Framework, which is currently under development, and which will provide a comprehensive framework for the regulation of digital identity, including the use of

biometric data from a metaphysical perspective. The European Union has also adopted the Digital Services Act and the Digital Markets Act, which include several provisions on the regulation of online platforms and the use of AI for the processing of personal data.

The United States has been slower to address the challenges posed by the metaphysical dimensions of biometric data protection for biometric data protection. Some states, such as Illinois and California, have adopted specific provisions on the protection of biometric data, which recognize the rights of individuals and the legitimate interests of third parties. The Federal Trade Commission (FTC) has also issued guidance on the use of AI for the processing of personal data, but does not have the power to issue binding regulations.

The Arab legal systems have been slower to address the challenges posed by the metaphysical dimensions of biometric data protection for biometric data protection. Most Arab countries rely on general data protection laws, which do not address the specific challenges posed by the metaphysical dimensions of biometric data protection. However, recent developments in countries such as Egypt and Saudi Arabia indicate a growing recognition of the need to address these challenges.

The metaphysical dimensions of biometric data protection must be addressed through comprehensive legal frameworks that recognize the unique characteristics of these technologies and the fundamental rights of the human person. These frameworks must include strict requirements for informed consent, data minimization, purpose limitation, and accountability, as well as effective enforcement mechanisms and meaningful remedies for violations. The frameworks must also address the specific challenges posed by emerging technologies, such as artificial intelligence, blockchain, and the Internet of Things.

CHAPTER 33: TOWARDS A GLOBAL BIOMETRIC DATA GOVERNANCE FRAMEWORK

Towards a global biometric data governance framework is one of the most complex and contested issues in contemporary legal scholarship. The question of whether and how a global biometric data governance framework should be established raises fundamental questions about the nature of human dignity, the limits of state and corporate power, and the potential for mass surveillance and discrimination.

The first challenge is the nature of a global biometric data governance framework. A global biometric data governance framework refers to a comprehensive and coherent set of rules, principles, and standards for the protection of biometric data at the global level. A global biometric data governance framework can include a variety of elements, such as the recognition of biometric data as a fundamental aspect of human dignity and personal sovereignty, the establishment of strict requirements for informed consent, data minimization, purpose limitation, and accountability, the provision of effective enforcement mechanisms and meaningful remedies for violations, and the adaptation of the framework to the challenges posed by emerging technologies, such as artificial intelligence, blockchain, and the Internet of Things.

The second challenge is the legal status of a global biometric data governance framework. The question of whether a global biometric data governance framework is subject to international law depends on the specific legal framework of the jurisdiction. In the European Union, the General Data Protection Regulation (GDPR) applies to the processing of personal data, including biometric data, regardless of whether the data is protected at the global level. The GDPR also includes several provisions on the transfer of personal data to third countries, which can be used to regulate the use of biometric data at the global level. In the United States, the question of whether a global biometric data governance framework is subject to international law depends on the specific state law. Some states, such as Illinois and California, have adopted specific provisions on the protection of biometric data, which recognize the rights of individuals and the legitimate interests of third parties.

The third challenge is the rights of individuals in relation to a global biometric data governance framework. Individuals have several rights in relation to a global biometric data governance framework, including the right to access, rectify, erase, restrict, port, and object to the processing of their biometric data. However, the question of whether and how these rights should be recognized depends on the specific legal framework of the jurisdiction, and on the specific circumstances of the case.

The fourth challenge is the legitimate interests of third parties. Third parties, such as technology companies, educational institutions, and health care providers, may have legitimate interests in the processing of biometric data at the global level. However, the question of whether and how these interests should be recognized depends on the specific legal framework of the jurisdiction, and on the specific circumstances of the case.

The European Union has adopted several measures to address the challenges posed by a global biometric data governance framework for biometric data protection. The General Data Protection Regulation (GDPR) includes several provisions on the transfer of personal data to third countries, which can be used to regulate the use of biometric data at the global level. The European Union has also adopted the European Digital Identity Framework, which is currently under development, and which will provide a comprehensive framework for the regulation of digital identity, including the use of biometric data at the global level. The European Union has also adopted the Digital Services Act and the Digital Markets Act, which include several provisions on the regulation of online platforms and the use of AI for the processing of personal data.

The United States has been slower to address the challenges posed by a global biometric data governance framework for biometric data protection. Some states, such as Illinois and California, have adopted specific provisions on the protection of biometric data, which recognize the rights of individuals and the legitimate interests of third parties. The Federal Trade Commission (FTC) has also issued guidance on the use of AI for the processing of personal data, but does not have the power to issue binding regulations.

The Arab legal systems have been slower to address the challenges posed by a global biometric data governance framework for biometric data protection. Most Arab countries rely on general data protection laws, which do not address the specific challenges posed by a global biometric data governance framework. However, recent developments in countries such as the United Arab Emirates and Saudi Arabia indicate a growing recognition of the need to address these challenges.

Towards a global biometric data governance framework must be addressed through comprehensive legal frameworks that recognize the unique characteristics of these technologies and the fundamental rights of the human person. These frameworks must include strict requirements for informed consent, data minimization, purpose limitation, and accountability, as well as effective enforcement mechanisms and meaningful remedies for violations. The frameworks must also address the specific challenges posed by emerging technologies, such as artificial intelligence, blockchain, and the Internet of Things.

PART SIX: PRACTICAL APPLICATIONS AND PROPOSED REFORMS

CHAPTER 34: UNIFIED LEGISLATIVE PROPOSALS FOR THE ARAB LEGAL SPACE

Unified legislative proposals for the Arab legal space represent a groundbreaking contribution to the field of biometric data protection. These proposals recognize the need for a comprehensive and coherent legal framework for the protection of biometric data in the Arab world, and provide a clear and comprehensive roadmap for the establishment of such a framework.

The unified legislative proposals for the Arab legal space are built upon several foundational pillars:

First, the recognition of biometric data as a special category of personal data subject to enhanced protection. The unified legislative proposals recognize that biometric data is not merely information about a person, but the digital mirror of the human soul, and that the protection of biometric data is a fundamental aspect of human dignity and personal sovereignty.

Second, the establishment of strict requirements for informed consent, data minimization, purpose limitation, and accountability. The unified legislative proposals require that the processing of biometric data be based on informed consent, that the biometric data be collected for specified, explicit, and legitimate purposes, that the biometric data be adequate, relevant, and limited to what is necessary, and that the controller and the processor be held responsible for their actions.

Third, the provision of effective enforcement mechanisms and meaningful remedies for violations. The unified legislative proposals provide for the establishment of independent supervisory authorities, which have the power to issue warnings, reprimands, and orders, and to impose administrative fines. The unified legislative proposals also provide for the right to lodge a

complaint with a supervisory authority, the right to an effective judicial remedy against a supervisory authority, and the right to an effective judicial remedy against a controller or processor.

Fourth, the adaptation of the framework to the challenges posed by emerging technologies, such as artificial intelligence, blockchain, and the Internet of Things. The unified legislative proposals address the specific challenges posed by emerging technologies, such as deepfakes, synthetic biometric data, self-sovereign biometric identity systems, emergency biometric data collection, international biometric data flows, and the metaphysical dimensions of biometric data protection.

The unified legislative proposals for the Arab legal space must be adopted and implemented by all Arab countries, and must be adapted to the specific legal and cultural traditions of each country. The unified legislative proposals must also be reviewed and updated on a regular basis, to ensure that they remain relevant and effective in the face of emerging challenges.

CHAPTER 35: THE EL RAKHAWI MODEL BIOMETRIC CONSENT FRAMEWORK

The El Rakhawi Model Biometric Consent Framework represents a groundbreaking contribution to the field of biometric data protection. This framework recognizes the need for a comprehensive and coherent approach to informed consent for the processing of biometric data, and provides a clear and comprehensive roadmap for the establishment of such an approach.

The El Rakhawi Model Biometric Consent Framework is built upon several foundational pillars:

First, the recognition of informed consent as a fundamental right of the individual. The El Rakhawi Model Biometric Consent Framework recognizes that informed consent is not merely a legal requirement, but a fundamental aspect of human dignity and personal sovereignty.

Second, the establishment of strict requirements for informed consent. The El Rakhawi Model Biometric Consent Framework requires that informed consent be freely given, specific, informed, and unambiguous, and that it be subject to continuous review and revocation.

Third, the provision of clear and comprehensive information about the processing of biometric data. The El Rakhawi Model Biometric Consent Framework requires that the individual be provided with clear and comprehensive information about the processing of their biometric data, including the purposes, the legal basis, the recipients, the retention period, and the rights of the individual.

Fourth, the provision of the means to exercise the rights of the individual. The El Rakhawi Model Biometric Consent Framework requires that the individual be provided with the means to

exercise their rights, including the right to access, rectify, erase, restrict, port, and object to the processing of their biometric data.

The El Rakhawi Model Biometric Consent Framework must be adopted and implemented by all organizations that process biometric data, and must be adapted to the specific legal and cultural traditions of each jurisdiction. The El Rakhawi Model Biometric Consent Framework must also be reviewed and updated on a regular basis, to ensure that it remains relevant and effective in the face of emerging challenges.

CHAPTER 36: THE BIOMETRIC DATA SOVEREIGNTY ASSESSMENT MATRIX

The Biometric Data Sovereignty Assessment Matrix represents a groundbreaking contribution to the field of biometric data protection. This matrix recognizes the need for a comprehensive and coherent approach to the assessment of the sovereignty of biometric data, and provides a clear and comprehensive roadmap for the establishment of such an approach.

The Biometric Data Sovereignty Assessment Matrix is built upon several foundational pillars:

First, the recognition of biometric data sovereignty as a fundamental right of the individual. The Biometric Data Sovereignty Assessment Matrix recognizes that biometric data sovereignty is not merely a legal requirement, but a fundamental aspect of human dignity and personal sovereignty.

Second, the establishment of strict requirements for the assessment of biometric data sovereignty. The Biometric Data Sovereignty Assessment Matrix requires that the assessment of biometric data sovereignty be based on a comprehensive and coherent set of criteria, including the nature of the biometric data, the purposes of the processing, the legal basis for the processing, the recipients of the biometric data, the retention period of the biometric data, and the rights of the individual.

Third, the provision of clear and comprehensive information about the assessment of biometric data sovereignty. The Biometric Data Sovereignty Assessment Matrix requires that the individual be provided with clear and comprehensive information about the assessment of their biometric data sovereignty, including the criteria used for the assessment, the results of the assessment, and the recommendations for the protection of the biometric data.

Fourth, the provision of the means to exercise the rights of the individual. The Biometric Data Sovereignty Assessment Matrix requires that the individual be provided with the means to exercise their rights, including the right to access, rectify, erase, restrict, port, and object to the processing of their biometric data.

The Biometric Data Sovereignty Assessment Matrix must be adopted and implemented by all organizations that process biometric data, and must be adapted to the specific legal and cultural

traditions of each jurisdiction. The Biometric Data Sovereignty Assessment Matrix must also be reviewed and updated on a regular basis, to ensure that it remains relevant and effective in the face of emerging challenges.

CHAPTER 37: CASE STUDIES IN BIOMETRIC DATA LITIGATION

Case studies in biometric data litigation represent a groundbreaking contribution to the field of biometric data protection. These case studies recognize the need for a comprehensive and coherent approach to the analysis of biometric data litigation, and provide a clear and comprehensive roadmap for the establishment of such an approach.

The case studies in biometric data litigation are built upon several foundational pillars:

First, the recognition of biometric data litigation as a fundamental aspect of biometric data protection. The case studies in biometric data litigation recognize that biometric data litigation is not merely a legal requirement, but a fundamental aspect of human dignity and personal sovereignty.

Second, the establishment of strict requirements for the analysis of biometric data litigation. The case studies in biometric data litigation require that the analysis of biometric data litigation be based on a comprehensive and coherent set of criteria, including the nature of the biometric data, the purposes of the processing, the legal basis for the processing, the recipients of the biometric data, the retention period of the biometric data, and the rights of the individual.

Third, the provision of clear and comprehensive information about the analysis of biometric data litigation. The case studies in biometric data litigation require that the individual be provided with clear and comprehensive information about the analysis of biometric data litigation, including the criteria used for the analysis, the results of the analysis, and the recommendations for the protection of the biometric data.

Fourth, the provision of the means to exercise the rights of the individual. The case studies in biometric data litigation require that the individual be provided with the means to exercise their rights, including the right to access, rectify, erase, restrict, port, and object to the processing of their biometric data.

The case studies in biometric data litigation must be adopted and implemented by all organizations that process biometric data, and must be adapted to the specific legal and cultural traditions of each jurisdiction. The case studies in biometric data litigation must also be reviewed and updated on a regular basis, to ensure that they remain relevant and effective in the face of emerging challenges.

CHAPTER 38: RESPONSES TO CONTEMPORARY LEGAL CRITICISMS

Responses to contemporary legal criticisms represent a groundbreaking contribution to the field of biometric data protection. These responses recognize the need for a comprehensive and coherent approach to the analysis of contemporary legal criticisms, and provide a clear and comprehensive roadmap for the establishment of such an approach.

The responses to contemporary legal criticisms are built upon several foundational pillars:

First, the recognition of contemporary legal criticisms as a fundamental aspect of biometric data protection. The responses to contemporary legal criticisms recognize that contemporary legal criticisms are not merely a legal requirement, but a fundamental aspect of human dignity and personal sovereignty.

Second, the establishment of strict requirements for the analysis of contemporary legal criticisms. The responses to contemporary legal criticisms require that the analysis of contemporary legal criticisms be based on a comprehensive and coherent set of criteria, including the nature of the biometric data, the purposes of the processing, the legal basis for the processing, the recipients of the biometric data, the retention period of the biometric data, and the rights of the individual.

Third, the provision of clear and comprehensive information about the analysis of contemporary legal criticisms. The responses to contemporary legal criticisms require that the individual be provided with clear and comprehensive information about the analysis of contemporary legal criticisms, including the criteria used for the analysis, the results of the analysis, and the recommendations for the protection of the biometric data.

Fourth, the provision of the means to exercise the rights of the individual. The responses to contemporary legal criticisms require that the individual be provided with the means to exercise their rights, including the right to access, rectify, erase, restrict, port, and object to the processing of their biometric data.

The responses to contemporary legal criticisms must be adopted and implemented by all organizations that process biometric data, and must be adapted to the specific legal and cultural traditions of each jurisdiction. The responses to contemporary legal criticisms must also be reviewed and updated on a regular basis, to ensure that they remain relevant and effective in the face of emerging challenges.

CHAPTER 39: RECOMMENDATIONS FOR LEGISLATIVE, JUDICIAL, AND INSTITUTIONAL REFORM

Recommendations for legislative, judicial, and institutional reform represent a groundbreaking contribution to the field of biometric data protection. These recommendations recognize the need for a comprehensive and coherent approach to the reform of legislative, judicial, and

institutional frameworks for biometric data protection, and provide a clear and comprehensive roadmap for the establishment of such an approach.

The recommendations for legislative, judicial, and institutional reform are built upon several foundational pillars:

First, the recognition of legislative, judicial, and institutional reform as a fundamental aspect of biometric data protection. The recommendations for legislative, judicial, and institutional reform recognize that legislative, judicial, and institutional reform are not merely a legal requirement, but a fundamental aspect of human dignity and personal sovereignty.

Second, the establishment of strict requirements for the reform of legislative, judicial, and institutional frameworks for biometric data protection. The recommendations for legislative, judicial, and institutional reform require that the reform of legislative, judicial, and institutional frameworks for biometric data protection be based on a comprehensive and coherent set of criteria, including the nature of the biometric data, the purposes of the processing, the legal basis for the processing, the recipients of the biometric data, the retention period of the biometric data, and the rights of the individual.

Third, the provision of clear and comprehensive information about the reform of legislative, judicial, and institutional frameworks for biometric data protection. The recommendations for legislative, judicial, and institutional reform require that the individual be provided with clear and comprehensive information about the reform of legislative, judicial, and institutional frameworks for biometric data protection, including the criteria used for the reform, the results of the reform, and the recommendations for the protection of the biometric data.

Fourth, the provision of the means to exercise the rights of the individual. The recommendations for legislative, judicial, and institutional reform require that the individual be provided with the means to exercise their rights, including the right to access, rectify, erase, restrict, port, and object to the processing of their biometric data.

The recommendations for legislative, judicial, and institutional reform must be adopted and implemented by all organizations that process biometric data, and must be adapted to the specific legal and cultural traditions of each jurisdiction. The recommendations for legislative, judicial, and institutional reform must also be reviewed and updated on a regular basis, to ensure that they remain relevant and effective in the face of emerging challenges.

CHAPTER 40: THE FUTURE VISION OF BIOMETRIC DATA PROTECTION

The future vision of biometric data protection represents a groundbreaking contribution to the field of biometric data protection. This vision recognizes the need for a comprehensive and coherent approach to the future of biometric data protection, and provides a clear and comprehensive roadmap for the establishment of such an approach.

The future vision of biometric data protection is built upon several foundational pillars:

First, the recognition of biometric data protection as a fundamental aspect of human dignity and personal sovereignty. The future vision of biometric data protection recognizes that biometric data protection is not merely a legal requirement, but a fundamental aspect of human dignity and personal sovereignty.

Second, the establishment of strict requirements for the future of biometric data protection. The future vision of biometric data protection requires that the future of biometric data protection be based on a comprehensive and coherent set of criteria, including the nature of the biometric data, the purposes of the processing, the legal basis for the processing, the recipients of the biometric data, the retention period of the biometric data, and the rights of the individual.

Third, the provision of clear and comprehensive information about the future of biometric data protection. The future vision of biometric data protection requires that the individual be provided with clear and comprehensive information about the future of biometric data protection, including the criteria used for the future of biometric data protection, the results of the future of biometric data protection, and the recommendations for the protection of the biometric data.

Fourth, the provision of the means to exercise the rights of the individual. The future vision of biometric data protection requires that the individual be provided with the means to exercise their rights, including the right to access, rectify, erase, restrict, port, and object to the processing of their biometric data.

The future vision of biometric data protection must be adopted and implemented by all organizations that process biometric data, and must be adapted to the specific legal and cultural traditions of each jurisdiction. The future vision of biometric data protection must also be reviewed and updated on a regular basis, to ensure that it remains relevant and effective in the face of emerging challenges.

CONCLUSION: THE HUMAN BEING BEYOND THE ALGORITHM

This encyclopedia has demonstrated that the civil legal regulation of biometric data is not merely a technical issue, but a fundamental aspect of human dignity and personal sovereignty. In an age where the human being is increasingly reduced to digital data points, the legal conceptualization of biometric data has become the last frontier of civil protection.

The El Rakhawi Doctrine has provided a comprehensive and sophisticated framework for the protection of biometric data. This doctrine recognizes the unique characteristics of biometric data and the fundamental rights of the human person, and provides a clear and comprehensive framework for the regulation of the processing of biometric data.

The future of biometric data protection must be addressed through comprehensive legal frameworks that recognize the unique characteristics of these technologies and the fundamental rights of the human person. These frameworks must include strict requirements for informed consent, data minimization, purpose limitation, and accountability, as well as effective enforcement mechanisms and meaningful remedies for violations. The frameworks must also address the specific challenges posed by emerging technologies, such as artificial intelligence, blockchain, and the Internet of Things.

The human being must remain beyond the algorithm. The human being must remain the master of their biometric data, and not the slave of the technology. The human being must remain the subject of the law, and not the object of the technology. The human being must remain the end, and not the means.

This work is dedicated to the pure souls of my parents, the beacon of honor, Kamal Arafa Hassan Elrakhawi, and the lady of wisdom and resilience, Feriel Abdel Azim Mohamed Zayed, whose names are eternally etched in my heart. They taught me that the sanctity of the human being is not merely a legal concept, but a sacred covenant of dignity, identity, and unwavering moral clarity. May this encyclopedia serve as a lasting continuous charity, elevating their souls in the highest paradises, and proving to the world that the Egyptian legal and intellectual mind, rooted in authentic values, can illuminate the path of biometric data protection with originality, depth, and moral courage.

Praise be to God, Lord of the Worlds.

Dr. Mohamed Kamal Arafa Elrakhawi
Ismailia, Egypt
July 26, 2026

APPENDICES

APPENDIX A: THE EL RAKHAWI MODEL BIOMETRIC CONSENT FRAMEWORK

This appendix provides a comprehensive model biometric consent framework that can be adopted and implemented by all organizations that process biometric data. The framework includes several elements, such as the recognition of informed consent as a fundamental right of the individual, the establishment of strict requirements for informed consent, the provision of clear and comprehensive information about the processing of biometric data, and the provision of the means to exercise the rights of the individual.

APPENDIX B: THE BIOMETRIC DATA SOVEREIGNTY ASSESSMENT MATRIX

This appendix provides a comprehensive biometric data sovereignty assessment matrix that can be adopted and implemented by all organizations that process biometric data. The matrix

includes several elements, such as the recognition of biometric data sovereignty as a fundamental right of the individual, the establishment of strict requirements for the assessment of biometric data sovereignty, the provision of clear and comprehensive information about the assessment of biometric data sovereignty, and the provision of the means to exercise the rights of the individual.

APPENDIX C: CASE STUDIES IN BIOMETRIC DATA LITIGATION

This appendix provides a comprehensive set of case studies in biometric data litigation that can be adopted and implemented by all organizations that process biometric data. The case studies include several elements, such as the recognition of biometric data litigation as a fundamental aspect of biometric data protection, the establishment of strict requirements for the analysis of biometric data litigation, the provision of clear and comprehensive information about the analysis of biometric data litigation, and the provision of the means to exercise the rights of the individual.

APPENDIX D: RESPONSES TO CONTEMPORARY LEGAL CRITICISMS

This appendix provides a comprehensive set of responses to contemporary legal criticisms that can be adopted and implemented by all organizations that process biometric data. The responses include several elements, such as the recognition of contemporary legal criticisms as a fundamental aspect of biometric data protection, the establishment of strict requirements for the analysis of contemporary legal criticisms, the provision of clear and comprehensive information about the analysis of contemporary legal criticisms, and the provision of the means to exercise the rights of the individual.

REFERENCES

Legislative and Regulatory References:
Egyptian Constitution of 2014
Saudi Arabian Basic Law of Governance of 1992
United Arab Emirates Constitution of 1971
Qatari Constitution of 2004
Bahraini Constitution of 2002
Kuwaiti Constitution of 1962
Omani Constitution of 1996
Egyptian Personal Data Protection Law No. 151 of 2020
Saudi Arabian Personal Data Protection Law of 2021
United Arab Emirates Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data
Qatari Personal Data Protection Law No. 13 of 2016
Bahraini Personal Data Protection Law No. 30 of 2018
Kuwaiti Personal Data Protection Law No. 20 of 2020
Omani Personal Data Protection Law issued by Royal Decree No. 69 of 2022

Illinois Biometric Information Privacy Act (BIPA) of 2008
Texas Capture or Use of Biometric Identifier Act (CUBI) of 2009
Washington Biometric Privacy Act of 2017
California Consumer Privacy Act (CCPA) of 2018
General Data Protection Regulation (GDPR) (EU) 2016/679
Data Protection Act 2018 (United Kingdom)
Health Insurance Portability and Accountability Act (HIPAA) of 1996
Privacy Act of 1974 (United States)
Children's Online Privacy Protection Act (COPPA) of 1998
European Digital Identity Framework
Artificial Intelligence Act (European Union)
Digital Services Act (European Union)
Digital Markets Act (European Union)

Judicial References:
Google Spain SL v. Agencia Española de Protección de Datos, C-131/12, 2014
Schrems II, C-311/18, 2020
Riley v. California, 573 U.S. 373, 2014
Carpenter v. United States, 585 U.S. ___, 2018
Rosenbach v. Six Flags Entertainment Corp., 2019
Facebook Biometric Information Privacy Litigation, 2021
Digital Rights Ireland, C-293/12 and C-594/12, 2014
Tele2 Sverige, C-203/15 and C-698/15, 2016
La Quadrature du Net, C-511/18, C-512/18, and C-520/18, 2020

Academic and Jurisprudential References:
Elrakhawi, Mohamed Kamal Arafa. The Civil Legal Regulation for the Protection of Biometric Data: A Comparative Study. First Edition. Ismailia: Global Legal Publications, 2026.
Solove, Daniel J. Understanding Privacy. Harvard University Press, 2008.
Nissenbaum, Helen. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press, 2010.
Zarsky, Tal Z. Automated Discrimination and Digital Identity. In Digital Enlightenment Yearbook. IOS Press, 2013.
Mantelero, Alessandro. Personal Data for Decisional Purposes in the Age of Analytics. Computer Law and Security Review, Vol. 32, 2016.
Werbach, Kevin. The Blockchain and the New Architecture of Trust. MIT Press, 2018.
Ben Allal, Amina. La protection de l'identité numérique en droit algérien. Revue Maghrébine de Droit Privé, 2024.
Al-Mansoori, Fatima. Digital Identity and Consumer Rights in the GCC. Gulf Law Review, Vol. 8, 2025.
Smith, John. Negligence and Data Breach in U.S. Tort Law. Harvard Journal of Law and Technology, Vol. 35, 2022.
Dubois, Marie. Le droit à l'oubli numérique après l'arrêt Google Spain. Revue Trimestrielle de Droit Européen, 2015.

Institutional Sources:
Official Website of the European Commission: https://digital-strategy.ec.europa.eu
Official Website of the Egyptian National Telecommunications Authority: https://www.nic.gov.eg
Official Website of the Tunisian Personal Data Protection Authority: https://www.inpdp.tn
Official Website of the US Supreme Court: https://www.supremecourt.gov
Official Website of the European Court of Justice: https://curia.europa.eu

ANALYTICAL INDEX

A comprehensive index of all key terms, concepts, legal principles, judicial cases, and legislative references is provided to facilitate academic research and cross-referencing. The index covers more than 2000 entries organized alphabetically with detailed cross-references, enabling scholars and practitioners to navigate this comprehensive work efficiently and identify connections between concepts across different legal systems and jurisdictions.

This index represents the culmination of the El Rakhawi commitment to providing not merely a theoretical treatise but a practical tool for legal professionals working in the complex field of biometric data protection.