How to cite this article:
Nourinezhad, M., Salarifar, A., & Zarghami, C. (2027). Comparative Analysis of the Legislative Criminal Policy of Iran and England in Confronting Emerging Challenges of Cybercrime (with Emphasis on Developments from 2020 to 2025). *Journal of Historical Research, Law and Policy, 5*(2), 1-25. https://doi.org/10.61838/jhrlp.342

Article history:
Original Research

Dates:
Submission Date: 04 March 2026
Revision Date: 01 June 2026
Acceptance Date: 06 June 2026
First Publication Date: 12 July 2026
Final Publication Date: 01 March 2027

Comparative Analysis of the Legislative Criminal Policy of Iran and England in Confronting Emerging Challenges of Cybercrime (with Emphasis on Developments from 2020 to 2025)

1. Mohammadamin. Nourinezhad[1] : Ph.D. student, Department of Criminal Law and Criminology, BA.C., Islamic Azad University, Bandar Abbas, Iran
2. Abuzar. Salarifar[2*]: Department of Criminal Law and Criminology, BA.C., Islamic Azad University, Bandar Abbas, Iran
3. Cyrus. Zarghami[3]: Department of Criminal Law and Criminology, BA.C., Islamic Azad University, Bandar Abbas, Iran

*corresponding author's email: 3161254627@iau.ac.ir

ABSTRACT

Technological developments and the expansion of cyberspace during the years 2020 to 2025 have confronted legal systems with emerging and complex challenges in the fields of criminalization and the control of cybercrime. This article adopts a comparative approach to examine and analyze the legislative criminal policy of Iran and England regarding new forms of cybercrime. The research method is descriptive–analytical and is based on newly enacted legal documents and regulations in both countries, including the amendments introduced under the Computer Misuse Act (CMA 1990) in England, the Iranian Computer Crimes Act, and the resolutions of the Supreme Council of Cyberspace. The findings indicate that the legal system of England, through a combined approach of traditional criminalization and technology-oriented reforms—such as the new Online Safety Act 2023—has demonstrated a more dynamic response to the rapid transformations of cyberspace and, in addition to criminal sanctions, has expanded preventive policies and victim protection mechanisms. In contrast, Iran's legislative policy continues to rely primarily on punitive responses and an extensive criminalization approach centered on state responsibility, while facing structural gaps in defining the scope of liability of private actors and in providing innovative mechanisms. By identifying the weaknesses of the Iranian legislative system, including the inadequacy of preventive measures, the lack of inter-institutional cooperation, and the slow adaptation to emerging technologies such as artificial intelligence and blockchain, the present study proposes solutions for improving Iran's criminal policy based on successful models adopted in England. The results of this analysis may assist policymakers in both countries in formulating forward-looking, flexible, and empirically grounded legislation aimed at addressing the growing threats of cybercrime.

Keywords: *Legislative criminal policy, cybercrime, legislative developments, emerging challenges.*

Introduction

One of the important issues in legislative criminal policy is criminalization. Criminalization, or the legal characterization of an act or omission as a crime, is a process through which new forms of conduct become subject to criminal law under penal legislation. In other words, criminalization, or the process of crime creation, refers to

resorting to criminal sanctions by defining a series of specific behaviors as criminal. Accordingly, the legislator, in light of social values and with the aim of preserving public order, brings certain acts that fall within the sphere of permissibility or deviance into the domain of criminal law by prescribing criminal sanctions. Therefore, the basic and essential element in legislative criminal policy is the examination of the foundations of criminalizing an offense as a crime (1).

In fact, criminalization is fundamentally contrary to the principle of freedom and the presumption of innocence and is justified only in exceptional cases, namely where a behavior is sufficiently harmful and blameworthy. This requirement prevents legislators from broadly criminalizing conduct and obliges them to limit criminalization to cases in which a behavior causes serious harm and warrants censure. Thus, criminalization is conditioned upon observance of the principles of harm and culpability. If a behavior criminalized by the legislator does not involve sufficient harm and blameworthiness, the rights and freedoms of members of society will be violated, and people may in practice disobey the legislator's command prohibiting such conduct. For example, the criminalization of intentional homicide, fraud, theft, and breach of trust is justifiable and has a legitimate basis. These crimes are compatible with both the harm principle and the principle of blameworthiness, because, on the one hand, they harm individuals' security, life, or property, and, on the other hand, they give rise to moral and social condemnation (2).

In England, in general, a person cannot be found guilty of committing a criminal offense unless the existence of two general constituent elements of crime is established: the actus reus, meaning the criminal conduct or act, and the mens rea, meaning the criminal state of mind. For an accused person to be found guilty of an offense, it is not sufficient that the accused merely acted in a particular way; rather, the accused must have possessed a specific mental attitude in relation to the conduct in question. Of course, proof of some offenses does not require the establishment of mens rea. These offenses are mostly known as strict liability offenses, and legal scholars generally use the term strict liability to impose liability for crimes that do not require a mental element alongside the material element of the offense (3).

The increasing expansion of information and communication technologies and the transformation of cyberspace in recent years have not only fundamentally changed the scope and form of cybercrimes but have also confronted countries' legal orders and criminal policies with new challenges. Traditional methods of combating cybercrime are no longer sufficient to respond to the complexity of emerging threats and require the revision and redesign of legislative policies in accordance with developments from 2020 to 2025. In this context, Iran and England, as two legal systems with different approaches and capacities, each face particular strengths and weaknesses in accountability, prevention, criminalization, and the protection of cybercrime victims. Despite certain legal reforms in both countries, serious deficiencies remain in relation to methods of responding to crimes based on emerging technologies, including challenges associated with artificial intelligence, blockchain, and organized cyberattacks. The main gap addressed by the present study is that most previous studies have either merely described laws or have lacked an up-to-date comparative analysis of the legislative criminal policies of the two countries. Therefore, in view of the developments of the past five years, it is necessary to examine strengths, weaknesses, opportunities, and threats comparatively, scientifically, and analytically in order to provide an appropriate model for improving Iran's criminal policy. The importance of the present research lies in the fact that, by focusing on emerging developments and threats, it can explain existing structural gaps, offer practical solutions for drafting efficient and forward-looking laws, and contribute to enhancing cybersecurity and the more effective administration of criminal justice in both countries.

Research Background

Mohammadifard et al. (2023), in an article entitled “Criminal Policy Regarding Crimes Against the Moral Dignity of Persons in Cyberspace in Light of Judicial Practice,” using a descriptive-analytical and library-based method, stated that the findings indicate that the country’s judiciary, particularly in relation to crimes against moral dignity in cyberspace, has pursued a criminal policy oriented toward absolute justice without sufficient attention to utilitarian considerations in the imposition of punishments. The widespread commission of crimes, lack of transparency in legislation, and lack of coordination among legislative, judicial, and executive criminal policies have resulted in confusion in adopting an appropriate criminal policy. At the same time, the failure to adopt a differentiated criminal policy and proportionate penal selection based on the existing realities of the cybercrime environment has led to the absence of unified judicial practice and to divergent judgments, which in turn cause prolonged proceedings and failure to vindicate the rights of victims of crimes against moral dignity (4).

Malekshaar (2023), in an article entitled “Iran’s Legislative Criminal Policy in Countering Crimes Against Chastity in Cyberspace,” using a descriptive-correlational method, showed that Iran’s legislative criminal policy in countering crimes against chastity in cyberspace has not been efficient and that confrontation with these crimes has been limited to judicial and coercive responses. Therefore, no significant success has so far been achieved in controlling internet-related harms (5).

Deylami-Moezzi et al. (2022), in an article entitled “Evaluation of the Legislative Criminal Policy of Iran and the European Union Toward Computer Crimes,” using a descriptive-analytical method, showed that the spectrum of criminal policies adopted in the European Union is more coherent than that of Iran’s criminal justice system, given the longer history of legislation and confrontation with cybercrimes. The main causes of the inefficiency of Iran’s criminal policy include reliance on penal policy, departure from non-penal preventive measures, failure to adopt situational and social crime-prevention measures, the law’s inadequate understanding of such crimes or inability to anticipate future emerging crimes, and the existence of a culture of improper use of cyberspace (6).

Nazari-Khanqah et al. (2021), in an article entitled “The Role of Participatory Criminal Policy in Preventing Cybercrimes in Iran,” stated that participatory criminal policy measures for cleansing cyberspace include a variety of measures, both technical measures such as licensing technologies and technologies related to the authentication of persons, especially their age and gender, and non-technical measures such as education and the enhancement of digital literacy (7).

Zhang and Dong (2023), in an article entitled “Criminal Law Regulation of Cyber Fraud Crimes: From the Perspective of Citizens’ Personal Information Protection in the Era of Edge Computing,” stated that, in the process of combating internet fraud, the state must continue to intensify its efforts (8).

Raharjo et al. (2022), in an article entitled “The Legal Policy of Criminal Justice Bureaucracy Cybercrime,” stated that a reactive policy model must be made more effective in preventing cybercrime and that the litigation process model is unsuitable for combating cybercrime with high speed and mobility. The reactive model must be improved in order to prevent cybercrime. The litigation model is not suitable for preventing highly mobile and fast-moving cybercrime. A preventive law-enforcement strategy is effective, but it requires a high level of law-enforcement capacity to detect and disable cybercrimes, a capacity possessed by few Indonesian law-enforcement authorities (9).

Sharma (2020), in a study entitled “Legislation Related to Cyber Crimes in the United Kingdom,” stated that cybercrimes are rapidly increasing due to greater access to cyberspace for various purposes such as commerce and other activities. Cyber laws in England focus on reducing issues related to cybercrime and on closely monitoring cybercrime activities. This research report highlights the application of laws related to cyber remedies in England for protecting the country’s cybersecurity. The Computer Misuse Act 1990 and the Data Protection Act 2018 are two laws commonly used to prohibit threats related to cybersecurity. The government of this country needs a responsible authority to enhance cybersecurity in order to prohibit crimes on social media platforms (10).

Research Method

The present research method is descriptive-analytical. The data collection method is library-based. Library methods are used to collect information related to the literature and research background. The data collection tools include databases, computer networks, the internet, books, articles, theses, journals, and similar sources. In this manner, by consulting books and informational sources, materials most closely related to the subject of the dissertation were collected, logically organized and classified, placed in the relevant chapters, and then the analysis of the dissertation was developed. The method of data analysis is documentary and analytical.

Theoretical Foundations

The term crime, derived from the Arabic root j-r-m, has been used to mean cutting, picking fruit from a tree, carrying, acquiring, committing sin, and compelling someone to do something blameworthy (11). Lexically, crime means sin, offense, and fault, and it is also expressed through terms such as wrongdoing, sin, evil deed, disobedience, and transgression (12). Crime is a behavioral deviation from ordinary conduct accompanied by loss and harm. Social, psychological, economic, and environmental factors are considered in matters related to crime. All of these concepts affect criminal events in different ways (13). Technically, it refers to any act prohibited by religious law and subject to worldly punishment, such as fixed punishment, discretionary punishment, retaliation, blood money, or expiation, or to otherworldly punishment, whether related to the offender himself, such as abandoning prayer and fasting or drinking wine, or related to another person, such as assault, battery, or killing. Therefore, in Islamic jurisprudential terminology, crime is synonymous with sin (14). In legal terminology, crime is defined as an act or omission that is punishable under the law or entails security and educational measures (15).

Criminal policy, which adopts the solution to the problem of crime as its main objective and framework, is defined as the set of principles according to which the social body organizes its response to the criminal phenomenon. In this regard, the way criminal policy is understood and its objectives are determined can affect the performance of criminal policy and direct its executive and operational programs toward different orientations. Therefore, if criminal policy is formed with the objective of ensuring security and maximizing its guarantee, all principles, conditions, strategies, mechanisms, and tools for implementing this objective must be defined and applied within the framework of criminal policy (16).

Criminal policy refers to a set of principles, measures, and strategies adopted by states and legal institutions to prevent, control, and combat crimes, as well as to reform and rehabilitate offenders. These policies are developed with the aim of ensuring public order, protecting social security, and supporting individual rights and freedoms (17).

Cyberspace is originally derived from the two words cybernetics and space. The word cybernetics has Greek roots. Its original meaning in Greek is governance and rule, and it was also used in this sense in Plato’s works.

Perhaps the science of guidance and control, or self-regulation, may be regarded as its Persian equivalent. In any case, cybernetics still preserves the older meaning to some extent and denotes a science that enables humans or automatic machines to govern and command (18).

Cyberspace refers to an environment formed through computer networks, the internet, and digital communication systems. It is a virtual space in which humans can exchange information, communicate, and engage in digital interactions. Cyberspace includes not only the internet and websites but also all digital communication infrastructures, including social networks, databases, computer systems, and even Internet of Things systems (19).

Legislative criminal policy is based on the personality of the offender, and the law is based on criminal policy when it enables the principle of individualization of criminal sanctions in order to facilitate the offender's return to society. In this situation, punishment and sanctions may not be fixed and inevitable and may not be proportionate to the committed offense (20).

Legislative criminal policy refers to a set of criminal laws and regulations enacted and implemented by legal authorities and state institutions to confront crimes in society. These policies specifically focus on drafting, amending, and implementing criminal and criminological laws and serve as a legal instrument for ensuring security and public order, as well as responding to criminal conduct. Legislative criminal policy is, in fact, a reflection of a country's general orientation in combating crime. These policies have a direct effect on the manner of dealing with offenders, the type and severity of punishments, crime prevention, and the method of reforming and rehabilitating offenders (21).

Research Findings

Challenges and Strategies for Strengthening Legislative Criminal Policy in Confronting Cybercrimes

With the continuous development of information and communication technologies, significant changes have occurred in social, economic, and cultural domains. The emergence of cybercrime as a new phenomenon has confronted the legal and legislative systems of countries, including Iran, with serious challenges. Although the enactment of specific laws such as the Computer Crimes Act represents an important effort in combating these crimes, the complexities of cyberspace, the speed of technological developments, and the transnational nature of this type of crime have repeatedly called into question the effectiveness of legislative criminal policy. In this context, obstacles to the proper enforcement of existing laws, problems related to the clarity and comprehensiveness of regulations, difficulties in proving crimes, and coordination among responsible agencies are only part of the challenges facing legislative criminal policy. Moreover, the changing and emerging needs of this field have doubled the necessity of reviewing, reforming, and updating laws. Accordingly, this section attempts to examine the most important challenges of legislative criminal policy in the field of cybercrimes and to offer solutions for strengthening and improving the effectiveness of the relevant laws and regulations, so that cybersecurity and the protection of citizens' rights may be more optimally guaranteed while responding to the growing needs of society.

Main Obstacles to the Enforcement of Current Laws

Despite the drafting and enactment of specific laws on cybercrimes in Iran, the optimal enforcement of these regulations still faces serious obstacles and challenges. Although legislation in this field has, to some extent, filled previous gaps, the reality is that the mere existence of a law cannot guarantee its efficiency and effectiveness.

Various factors at legislative, executive, and even technical-specialized levels have caused legislative criminal policy to encounter numerous problems from the stage of enactment to effective implementation. Some of these obstacles are rooted in the inherent characteristics of cyberspace, which is rapidly evolving and constantly generating new forms of criminal conduct. Others arise from structural weaknesses in existing laws and regulations themselves, which sometimes lack the necessary clarity, comprehensiveness, or coordination and therefore create obstacles both in the detection and proof of crime. In addition, conflicts or gaps between laws, technical and equipment limitations, lack of specialized training for law-enforcement officers and judges, and insufficient coordination among relevant institutions have aggravated this problem (22). This section will seek to examine the most important obstacles to the enforcement of existing laws in the field of cybercrime and to analyze in detail and in a documented manner the reasons for inefficiency and the problems that prevent the full realization of the legislator's objectives in this field. This examination will prepare the ground for presenting corrective solutions and proposals for strengthening legislative criminal policy in the fight against cybercrime.

a. Inadequate Clarity of Legal Concepts

One of the most important obstacles to the enforcement of cybercrime laws in Iran is the ambiguity and lack of clarity of legal concepts and terminology, which lead to confusion and differing interpretations at various judicial and executive levels. Given the specific nature of these crimes, cybercrime laws must be highly clear and transparent in order to precisely cover persons, technologies, and activities. However, in the Computer Crimes Act and related regulations, many principles and definitions are stated in general terms, making effective enforcement of the law difficult. For example, terms such as "unauthorized access," "confidential data," "computer system," and "personal information" are used without clear and comprehensible definitions, resulting in disagreement among law-enforcement officers, judges, and even litigants during judicial proceedings when comparing real cases with legal definitions. These ambiguities may appear more clearly in computer crimes, where the technical and specialized nature of the offense doubles the importance of conceptual clarity. The absence of a clear definition of fundamental concepts can lead to conflicting practices and different interpretations in judicial authorities. For instance, "unauthorized access" may, for one judge, simply mean entering a user account without the owner's permission, whereas for another judge it may mean an attempt to enter by breaking a system's security locks. These different interpretations lead to contradictory judgments, confusion among litigants, and even harm to the rights of the accused or the complainant (2).

Moreover, certain concepts such as "confidential data" or "personal information" do not have precise and clear definitions in Iran's domestic laws. This is while, in many advanced legal systems, codified standards and definitions exist for such important terms, and the boundaries of each type of data play a key role in determining the type of crime and the severity of punishment. In the absence of such clarity, the judge decides based on personal understanding or local practice, which is contrary to the principle of equality of citizens before the law. Specifically, the lack of an official definition of "cybercrimes" has made the boundary between some traditional crimes and cybercrimes ambiguous. It is sometimes observed that similar conduct is considered a cybercrime merely because it occurs on the internet or involves the use of a computer, while the material and mental elements of the offense overlap with classical examples. This issue requires revision and the formulation of up-to-date definitions coordinated with technological developments. Lack of clarity in the interpretation of some technical and legal terms such as "data destruction," "unauthorized manipulation," or "unauthorized use of a computer system" has several

practical consequences. First, the accused is often unable to predict the consequences of his conduct because it is unclear whether a specific behavior will fall within the scope of criminal enforcement. Second, police and judicial officers also hesitate in identifying and determining offenses and sometimes become passive, which can lead to delays in prosecution or even closure of cases (23).

Another negative consequence of ambiguity in legal concepts is the creation of conflict with similar or superior regulations in domestic and international law. Lack of transparency threatens human rights principles, protection of personal data, users' rights, and even intellectual property rights. In some cases, failure to comply with international treaties or globally accepted standards can create distrust among international institutions and even hinder cross-border judicial and law-enforcement cooperation. Under such conditions, victims of cybercrime also suffer, because they may not receive the necessary criminal protection due to the judge's narrow or broad interpretation of the legal term or may face delays in proceedings. This problem also reduces public trust in the judicial system and state accountability. At the macro level, legal opacity increases the number of undetected crimes and leaves the core of organized cybercrime intact, because professional criminals, aware of legal gaps and ambiguities, commit acts that are difficult to prove or are not fundamentally covered by criminal regulations. This harms public security and creates opportunities for organized groups to exploit cyberspace (24).

Moreover, ambiguity in legal concepts is not limited to the Computer Crimes Act and is also reflected in executive regulations and instructions. Some secondary laws and complementary regulations drafted to supervise cyberspace activities suffer from this problem, calling into question the coordination of executive and law-enforcement bodies. In sum, effective confrontation with cybercrimes requires that ambiguity and excessive brevity in legal concepts be eliminated. A scientific, specialized approach based on stakeholder participation, legal revision, and the precise and up-to-date definition of concepts not only gives judges and enforcement authorities greater capacity to apply criminal concepts to concrete cases but also guarantees the rights of the accused and the complainant in the best possible way under the principles of transparency and the rule of law.

b. Problems of Proving Crime

One of the most fundamental challenges in enforcing legislative criminal policy in relation to cybercrimes is the issue of proving the crime and the difficulties associated with collecting, preserving, and presenting evidence in cyberspace. Unlike traditional crimes, cybercrimes mostly occur in an intangible environment, without the physical presence of the offender, and often through the use of unknown tools and identities. These conditions have completely changed the nature of the process of detection, prosecution, and proof of crime and have confronted the judicial system with numerous problems. In the first step, one of the fundamental problems in proving crime is the shortage or absence of reliable electronic evidence. Digital data and evidence can easily be manipulated, deleted, or transferred, and the recovery of deleted or encrypted data requires technical knowledge, advanced equipment, and rapid cooperation among relevant institutions. Many cybercrimes remain without any trace identifiable by law-enforcement officers, and features such as encryption, fake IP addresses, and the use of private networks make the identification process more complex (25).

In addition, the storage of and reliance on electronic evidence itself entails numerous legal obstacles. Under the law, for digital evidence to be considered valid, the chain of custody must be maintained in such a way as to eliminate suspicion of data manipulation or distortion. In practice, however, the lack of technical infrastructure, poor training of officers, and even lack of coordination among responsible organizations call into question the validity of

electronic evidence and cause judicial authorities to doubt and distrust this type of evidence. In this regard, the absence of national standards or specific judicial practice is another reason. Precise and codified criteria for collecting, documenting, and validating electronic evidence have not yet been established in the country, and this has led to conflicting and sometimes contradictory opinions in similar cases. Each judge acts according to his own interpretation of electronic evidence and the criteria for its admissibility, while the technical nature of such evidence requires unified, scientific, and reliable methods to be defined at the national level. Another area of difficulty is the heavy reliance on international cooperation in cases with transnational elements. A substantial part of criminal data and communications is stored on servers outside the country, and this makes investigations directly dependent on the cooperation of foreign governments and companies. Given tensions and legal and political limitations, especially the absence of mutual legal assistance agreements in the cyber domain with some countries, access to data or inquiries into offenders' identities becomes practically impossible or highly time-consuming and delays proof of the crime (26).

Another factor that makes proof of crime difficult is the rapid change in cyber technologies and tools. Offenders increasingly use more complex methods such as securing traces, simulating identities, using chain attacks, and deploying new technologies to prevent identification. Updating the technical knowledge and capabilities of law-enforcement officers in proportion to rapid changes in this field is one of the fundamental but less fulfilled needs in the country.

In addition to these factors, the rights of the accused, as a fundamental criminal-law principle, also complicate the process of proof. Guaranteeing the right to defense, the presumption of innocence, and the prohibition of unlawful intrusion into privacy require that the process of collecting and presenting electronic evidence be fully based on law and principles. Any violation of these principles, even for the purpose of detecting crime, makes the evidence inadmissible and weakens the proof process. Moreover, the low public awareness of victims regarding the importance of preserving digital evidence or reporting crimes properly is another important obstacle. In many cases, victims, due to insufficient awareness of the nature of digital evidence or proper methods of dealing with computer systems after a crime occurs, unintentionally destroy many traces of the crime or restore them to their original state. This creates a gap in the process of detection and inference and makes proof of crime more difficult. The issue of time and urgency is also of double importance in cybercrime. Many cases require immediate action by officers and prosecutors, but traditional procedures and administrative bureaucracy limit, and in some cases eliminate, the golden opportunity to collect evidence. Achieving proof of crime in this environment requires a rapid, flexible, and technology-based approach throughout the entire chain of data collection, transfer, and analysis (27).

Finally, it should be noted that solutions such as forming specialized groups, establishing technical teams within the cyber police, increasing interaction with domestic technology companies, drafting standard guidelines, and updating the training of judicial officers and official experts can reduce some obstacles to proving crime. The gradual acceptance of electronic evidence in the judicial system and the creation of technical and legal support structures are necessary to improve the effectiveness of criminal policy in combating cybercrimes.

c. Conflict Between Laws

One of the major obstacles to the effective enforcement of legislative criminal policy regarding cybercrimes is the problem of contradiction and conflict among different laws in this field. This conflict not only causes confusion among law-enforcement officers and citizens but also leads to contradictory judgments, weakens legal certainty, and

reduces the effectiveness of the country's overall countermeasures against new criminal phenomena in cyberspace. Cybercrimes have technical and complex dimensions that often overlap with aspects of criminal conduct in other areas, such as intellectual property, privacy, access to data, and similar fields. On the one hand, there is the Computer Crimes Act of 2009, which has attempted to determine the general framework for dealing with cybercrimes; on the other hand, there are regulations such as the Electronic Commerce Act, the Law on the Protection of the Rights of Creators of Computer Software, the Islamic Penal Code, and even instructions in the field of information technology, each of which offers its own understandings and interpretations. Many concepts, punishments, or even procedural rules are defined differently in these bills and laws. For example, the issue of "unauthorized access to personal data" has a relative and scattered definition in the Computer Crimes Act, whereas in some provisions of data-protection law, at the level of proposed bills or executive enactments, as well as in laws concerning trade secrets or the Islamic Penal Code, completely different definitions or sanctions are observed. These differences sometimes concern the definition of the offense, sometimes punishment, and even the determination of the competent authority for adjudication, creating practical conflicts. Moreover, the issue of "privacy" and the possibility of monitoring individuals in cyberspace is one of the most important areas of conflict between regulations. While the Constitution and higher-level regulations consider privacy and its observance necessary, certain legal powers granted to officers under the Computer Crimes Act and regulations related to the cyber police give them broad authority in cyber surveillance. This duality has led to divergent practices in courts and prosecutors' offices (28).

Conflict between laws is evident not only in the field of concepts and instances but also in the issue of determining jurisdiction. The lack of clarity regarding the boundary between the inherent jurisdiction of general, criminal, or specialized courts and sometimes even administrative authorities, such as the Supreme Council of Cyberspace or the Information Technology Organization, causes prolonged proceedings or even violations of the rights of the parties. This creates additional difficulties in cases involving international or transnational elements. On the other hand, some existing regulations have been adopted in line with the country's legislative policies on cyberspace, but their legal basis differs from parent laws. For example, there are rules in the field of combating online gambling or cyber betting that sometimes do not fully conform to the criminological definitions of the Islamic Penal Code or to constitutional principles. This difference has caused judges to make different decisions in similar cases, reduced legal certainty, and eliminated the expectation of predictability from the judicial system (29).

The technology-oriented and evolving nature of cybercrimes has also created additional conflict between laws, because some regulations, regardless of rapid technological changes and the emergence of new instances, still insist on a traditional approach. On the other hand, in the absence of a codified and comprehensive law, enactments of the Supreme Council of Cyberspace or urgent orders of executive bodies become the basis of action, which causes confusion among executive authorities and even violations of citizens' rights. Another manifestation of conflict concerns the type and degree of prescribed punishments; for a single behavior, depending on which regulation or legal provision applies, different or even apparently contradictory punishments may be imposed. This situation not only calls criminal justice into question but, in some cases, exposes the accused to selective treatment, which is contrary to the principles of fair trial (30).

It is noteworthy that conflicts between laws sometimes arise from lack of coordination among legislators, insufficient consultation with experts in information-technology and computer crimes, and the multiplicity of decision-making bodies in cyberspace. The continuation of this situation also causes the process of legal reform and updating

to face interruption and conflict and constitutes a major obstacle to the development of a unified, transparent, and efficient legislative criminal policy. In conclusion, fundamental conflicts and contradictions among criminal laws, technology regulations, and executive bylaws cause the greatest harm to the rule of law, effective protection of victims, and guarantees of the rights of the accused. Resolving this challenge requires a comprehensive and scientific review of the body of laws related to cyberspace, the unification of judicial practice, and the creation of a unified legislative system in this field.

Emerging Needs and Challenges of Cyberspace in Regulating Legislative Policy

With the emergence and expansion of information and communication technologies, especially after the spread of the internet and smart devices, new needs have arisen in the field of criminal policy-making and legislation that traditional legal systems had never experienced. These developments have challenged the existing order of the legislative system and have turned efficient, up-to-date, and effective legislation in the field of cybercrimes into an undeniable necessity.

The first emerging need is the identification and precise definition of legal concepts compatible with the realities of cyberspace. Many fundamental concepts, such as data, information, digital identity, virtual intellectual property, and privacy, have complexities that do not fit within traditional legal definitions. The absence of these precise definitions not only causes disagreement in judicial decisions but also creates grounds for broad or narrow interpretation of the law and undermines legal certainty. The next challenge is the rapid change in the nature and instances of cybercrimes. Technology has developed in such a way that every day new communication and network platforms, along with new tools for encryption, identity theft, and data transfer, create grounds for new types of cybercrimes. This situation means that the law, even at the stages of drafting and enactment, is always several steps behind new events; whether intentional or not, legal gaps are constantly emerging. The third issue is the global and borderless nature of cyberspace. Many computer crimes are transnational in nature; the offender may be on one continent and the victim on another, or some vital data and evidence may be stored on servers in a third country. This situation has seriously challenged the traditional system of territorial jurisdiction and has turned obtaining evidence and punishing the accused into a requirement for complex international cooperation (31).

At the same time, cyberspace creates various risks for citizens' fundamental rights and freedoms. Especially in the areas of privacy, protection of personal data, freedom of expression, and free access to information, these issues require policymakers to place the creation of transparent and balanced laws between the guarantee of security and freedom on the agenda. The absence of transparent regulations can either give a green light to violations of freedoms or, conversely, facilitate criminal conduct. The transformation of social relations in cyberspace has also led to the emergence of new instances of intellectual property, digital works, cryptocurrencies, and even interactive and virtual identities, each of which requires its own legal requirements and protections. Traditional law, which often views property only in the form of physical assets, is inadequate in the face of digital assets and their transfer, and this gap creates grounds for crimes such as virtual fraud, forgery of digital assets, and theft of cryptocurrencies. The emergence of phenomena such as malware, ransomware, DDoS attacks, and phishing has created a new level of threats requiring legal action to develop flexible and technology-based laws compatible with global standards. However, legislation in Iran and many other countries has often lagged behind these threats and, in many cases, has remained limited to criminalization and punishment without defined requirements or preventive mechanisms for victim protection (32).

Another emerging need is the existence of regulations protecting whistleblowers and victims of cybercrimes. Individuals usually do not report or document crimes due to fear of identity disclosure and insufficient protection. Therefore, legislative policy must always be examined from the perspective of improving reporters' security and strengthening structural protection for victims. Furthermore, the growing expansion of the Internet of Things, artificial intelligence, big data, and cloud computing has created new challenges in the areas of ownership, criminal liability, and the nature of criminal conduct. For example, criminal acts arising from intelligent algorithms or robotics have raised fundamental questions about criminal liability and the determination of the offender, questions to which current law largely lacks clear answers. Another challenge is the issue of proportionality between crime and punishment in cyberspace. The intangible nature of many cybercrimes and the breadth of their effects can multiply the scope of damage. Therefore, legislative policy must not neglect alternative punishments, preventive technical tools, appropriate compensation, and even social and educational measures (33).

From another perspective, the need to strengthen the expert and technical capacity of law-enforcement officers and judicial authorities is prominent. Developing technology-based laws without practical support will, in effect, be fruitless. This requires relative growth in the specialized capacity of executive institutions. It also requires continuous training, organized communication with universities and knowledge-based companies, and the updating of executive guidelines in parallel with technological advances. Limiting the powers of executive and judicial authorities in dealing with cyberspace is another important issue. Given the scope of surveillance and the volume of data generated, there is always a concern that state or judicial interventions may exceed legal boundaries and become a threat to privacy and civil liberties. Policymakers must always strike a balance between public security and individual rights when regulating the powers of law-enforcement officers and ensuring judicial oversight.

In addition to the above challenges, the problem of conflict or overlap between traditional laws and new regulations related to information technology is evident. Lack of legislative coordination among general criminal laws, communications regulations, regulations of the Supreme Council of Cyberspace, and even technical standards can be regarded as a significant vulnerability in cybercrime policy-making. Uniform practice and organizational consensus for developing a unified legislative system are fundamental needs that must be addressed. The legislative process must be participatory, expert-based, and grounded in reality.

Confronting Legal and Procedural Challenges in England's Cyber Criminal Policy

Given the rapid growth of information technology and the expansion of cyberspace, England's cybercrime policy has faced numerous legal and procedural challenges. The transnational, dynamic, and complex nature of cybercrimes has compelled the English legal system to update its laws and judicial structures in step with technological advances. However, the increasing growth of cyber threats has revealed gaps and contradictions in the legislative and criminal justice systems that require serious attention from policymakers. One fundamental challenge is updating and adapting existing laws to new methods of committing and proving cybercrimes. Many traditional regulations are unable to respond to the complexities of computer and internet crimes, which increases the need for reform and the drafting of specific regulations. In addition, determining criminal liability, defining the boundaries of privacy, and managing jurisdictional conflicts between countries are among the most important concerns of the English judicial system in dealing with this type of crime. On the other hand, judicial and technical procedures also face challenges such as presenting reliable digital evidence, protecting the rights of accused persons and victims, and ensuring the principles of fair trial. Providing suitable infrastructure for the training of

judges and judicial officers, using technological tools in detecting and documenting cybercrimes, and attempting to establish a balance between state authority and the preservation of individual freedoms are among the main axes of cybercrime policy-making in England (34). These challenges require a comprehensive and interdisciplinary approach to improving and making the criminal justice system efficient in the digital age.

Legal and Procedural Challenges in Dealing with Cybercrimes

The expansion of information and communication technologies in recent decades has created unprecedented opportunities for economic and social development, but it has also provided grounds for the emergence of new forms of crime. Because of their complex technical nature and global scope, cybercrimes have confronted legal systems with fundamental challenges. England, as one of the leading European countries in combating cybercrime, also faces numerous legal and procedural issues that require innovative approaches and specialized solutions. One of the most important challenges is the inadequacy or ambiguity of legal definitions of cybercrimes and the evidentiary standards for proving these crimes. Many traditional legal provisions and regulations were not drafted to respond to the specific issues of internet crimes, and this creates gaps or conflicts in identifying crimes, determining criminal liability, and even establishing the jurisdiction of courts. Moreover, the collection, preservation, and presentation of digital evidence before judicial authorities require specific legal and technical rules and guidelines so that both the accuracy and validity of evidence are guaranteed and the rights of the parties are preserved. Alongside legal issues, procedural challenges are also fundamentally important. Judicial practice in dealing with cyber cases must be adapted to the requirements of new technologies. Training and specialization of judges and officers in the field of technology, ensuring fair trial in cases based on digital evidence, and executive mechanisms for international cooperation are among the most important procedural axes in responding to these crimes (35). Together, these challenges have driven England's criminal policy toward structural reforms and the strengthening of specialized tools.

a. Examining Existing Legal Failures and Gaps in Confronting Emerging Forms of Crime

The emergence of new technologies and the expansion of the internet have created a basis for the emergence of various new types of cybercrimes, posing significant challenges to the traditional structure of legal systems. Many of these cases, including complex ransomware attacks, intrusions into critical infrastructure, digital-asset crimes, and misuse of artificial intelligence, are not properly identified and punished in the absence of clear and up-to-date regulations. These gaps usually arise from the distance between the speed of technological developments and the slowness of the legislative process, which causes new crimes to remain outside the protective and preventive umbrella of criminal laws. A clear example of this gap is the lack of a precise and comprehensive definition of certain cases such as "cyber sabotage" or "algorithmic manipulation." In many cases, existing criminal laws only cover theft, fraud, or physical destruction and do not address concepts such as data corruption or misuse of intelligent algorithms. Such shortcomings force courts to attempt to cover new cases through broad interpretations or resort to analogical laws, which increases the risk of weakening the legality of crimes and punishments (36).

On the other hand, changes in crime patterns and in the tools used by criminals have also exposed the inefficiency of traditional tools and procedures. For example, crimes such as the illegal provision of malware-as-a-service or criminal operations based on blockchain technology go beyond classical legislative frameworks. The absence of specific regulations for such crimes allows offenders to exploit legal gaps and benefit from the

concealment and rapid-movement features of cyberspace. Another major challenge is the conflict of laws and jurisdiction in cyberspace. Many cybercrimes are transnational in nature, and, in the traditional system, determining jurisdiction and using international assistance tools involve numerous complexities. The absence of common and coordinated frameworks among national systems, as well as the absence of comprehensive international treaties, has caused significant disruptions in the process of rights enforcement and countering major international offenders (37).

Furthermore, the issue of digital evidence and its validity before judicial authorities has created a gap in the process of proving crimes. Existing laws often lack the necessary guidelines for collecting, preserving, and presenting digital evidence in a standardized and reliable manner, a problem that leads to the acquittal of many accused persons due to insufficient evidence or the absence of uniform court practice. In addition to technical and structural aspects, gaps in the protection of emerging victims are also concerning. Many current regulations focus mainly on criminal prosecution and lack the necessary support for victims, including data protection, compensation, and access to legal advice (38).

Finally, to remedy these shortcomings and gaps, policymakers must continuously amend and revise criminal laws, develop new procedures for collecting and evaluating digital evidence, and expand international cooperation treaties. Cooperation among technology specialists, lawyers, and regulatory bodies can lead to the creation of a more up-to-date and effective system for addressing emerging cybercrimes.

b. Problems Related to Conceptual Ambiguity, Jurisdiction, and Conflict Between Domestic and Transnational Laws

One of the most important challenges in dealing with cybercrimes is ambiguity in defining the concepts and instances of this category of crimes. Many common terms in the field of cybercrimes, such as “unauthorized access,” “cyber sabotage,” or even “data,” are not clearly defined in legal texts or are interpreted differently in practice. This conceptual ambiguity creates grounds for judicial interpretation and the emergence of different practices, thereby endangering the unity of judicial practice. The absence of precise definitions can also lead to the acquittal of accused persons or the violation of their rights (39).

Moreover, the speed of technological change has created problems for the legislative process. Laws are often formed with a delay in relation to developments in the cyber domain, causing current regulations to be unable to respond to emerging instances. For example, new tools and methods currently used for cyberattacks, such as artificial-intelligence-based malware or sophisticated phishing, are not recognized in traditional laws, and this intensifies conceptual gaps. Another fundamental problem is the complexity of determining the jurisdiction of judicial authorities in cybercrime cases. The transnational nature of most of these crimes means that the place of commission, the nationality of the offender or victim, and the context in which the offense occurred, whether server or data-transfer network, all play a role in determining jurisdiction. Disagreement over which country or judicial authority has jurisdiction creates confusion and even practical conflict in the prosecution and trial of accused persons (40). In many cases, countries attempt to extend their jurisdiction beyond geographic borders by resorting to the principles of territorial or protective jurisdiction. However, such expansion of jurisdiction without international coordination can create disputes and even conflicts with the principles of national sovereignty. Resolving these conflicts becomes a serious challenge, especially when several countries simultaneously claim jurisdiction or different legal systems enact conflicting regulations (37).

The issue of conflict of laws is another important matter in the field of cybercrimes. Because of differences in substantive and procedural laws among different countries, dealing with a single crime may produce completely different outcomes; for example, conduct criminalized in one country may be lawful in another. In addition, differences in procedures for evidence collection, privacy protection, and data transfer complicate judicial cooperation. Some countries attempt to help resolve these disputes by concluding bilateral or multilateral treaties, but the absence of a comprehensive and binding international legal framework remains a serious gap in combating cybercrimes. The Budapest Convention was one of the first attempts in this regard, but despite all its advantages, because of the non-membership of some countries and conflicting interpretations of its provisions, it has not been able to become a global standard (41).

Finally, to overcome problems of conceptual ambiguity, jurisdiction, and conflict of laws, continuous review of regulations, strengthening of international legal and judicial cooperation, and movement toward conceptual and procedural transparency are unavoidable. In addition, convergence of legal systems, specialized training of judges and law-enforcement officers, and the use of new technologies in cybercrime investigation and prosecution processes can provide a suitable basis for addressing existing challenges.

c. Differences in Enforcement and Practice in Courts and Critique of Recent Judicial Practices

In recent years, the enforcement and interpretation of cybercrime laws in English courts have differed significantly. Depending on the judge's background, the volume of cyber cases, and the judge's technical understanding of the issues, courts have sometimes adopted different approaches to the admissibility of digital evidence, the definition of concepts such as "unauthorized access," or the limits of criminal liability. This lack of uniformity in dealing with similar cases can reduce the predictability of the criminal justice system and weaken public trust in the judiciary. In some jurisdictions, because of lack of expertise, courts have hesitated to admit or validate evidence when faced with digital data or the technical complexities of cyberattacks. This is especially evident when parties present different technical arguments. Sometimes digital evidence is rejected because of defects in the collection process or the chain of custody, which can contribute to the acquittal of cybercriminals (42).

There are also significant differences in approaches from the perspective of interpreting legal texts. Some courts attempt to cover emerging instances through broad interpretation of existing laws, while others insist on narrow interpretation and consider legislative shortcomings an obstacle to judicial review. This difference in approach affects the uniformity of judicial practice and the development of cyber law and can lead to contradictory judgments regarding similar crimes. In several important recent cases, lawyers have raised numerous criticisms regarding the manner of reliance on digital evidence and its reliability. Some courts have accepted data as conclusive evidence without carefully examining its technical validity or source, while in other cases excessive strictness in admitting such evidence has resulted in violation of the victim's rights. The emergence of this enforcement gap highlights the need for standard guidelines and specialized training for judges (38).

Review of recent judgments shows that issues related to users' privacy and the manner of data collection have also affected the interpretation and enforcement of the law. In some cases, courts have limited the scope of search and access to the personal data of accused persons by relying on the principles of proportionality and necessity. In others, however, they have applied fewer restrictions by invoking the priority of public security. This duality has led to inconsistent enforcement of cybercrime policy. Legal critics have also pointed to the slowness of mechanisms for enforcing cybercrime judgments. The enforcement of judicial orders to block access, remove content, or

compensate damages faces difficulties because of the international nature of cyberspace and the role of foreign intermediaries, such as technology companies or servers located abroad. The lack of strong tools for effectively enforcing these orders reduces deterrence and the effectiveness of judicial measures against offenders (43).

Overall, to address these differences and achieve a coherent and efficient practice, it is proposed that standardization of procedures, centralized training of judges, updating of regulations, and use of technical expertise in the process of adjudicating cybercrimes be considered. Moreover, using the experiences of other countries and international forums can play an effective role in improving England's cyber justice system.

Reforms and New Approaches in Strengthening Cyber Criminal Policy

In recent decades, with the continuous development of information and communication technologies, cybercrimes have expanded in various dimensions and forms. This trend has confronted policymakers and legislators with complex challenges in effectively combating cyber threats. Many legal systems, especially in developed countries, have attempted to strengthen the efficiency and flexibility of their criminal policy against cybercrimes by revising existing laws and adopting new approaches. One axis of reform is the clarification and updating of definitions of cybercrimes in order to minimize legal ambiguities and enable the development of more coordinated judicial practice. New regulations also emphasize the importance of prevention and combating emerging technologies, including artificial intelligence and advanced encryption. This trend has also led to the expansion of the scope of criminal liability of natural and legal persons, including internet service providers and digital platforms. New approaches now focus more than ever on international cooperation, information exchange, and strengthening joint law-enforcement mechanisms. Given the transnational nature of cybercrimes, drafting regional and global treaties and creating platforms for identifying and extraditing offenders are effective approaches to reducing operational and legal gaps. Specialized institutions and commissions have also been established with the aim of greater coordination and standardization of procedures for combating cybercrimes (44). Overall, reforms and new approaches in cybercrime policy-making are highly conditional and dynamic, and efforts are being made to provide more efficient and effective responses to this complex phenomenon by combining legal instruments, technology, and intersectoral cooperation. Success in this path requires the convergence of political will, improvement of technical-legal literacy, and continuous communication between the legal system and technology specialists in order to protect society while preserving individuals' fundamental freedoms and rights.

a. New Plans of the English Government for Reviewing and Reforming Laws Related to Cyberspace

In recent years, the English government has recognized the need to update and reform its cyber laws in order to combat cybercrimes more effectively. One of the key areas of this effort has been the review of the Computer Misuse Act, enacted in 1990, which, despite its historical role, has faced widespread criticism for failing to keep pace with emerging threats and technologies. Technological advances and the increasing complexity of cyberattacks have highlighted the need for structural reforms. One criticism of the 1990 Act is that many behaviors now necessary for cybersecurity and vulnerability testing, such as exploit hunting or authorized penetration testing, are criminalized under the current text. This issue is concerning for cybersecurity specialists because it also exposes white-hat hackers to prosecution. In response to this challenge, the English government has announced the launch of a consultation process with stakeholders for fundamental reform of the Computer Misuse Act (45).

The most important proposed reforms include a more precise definition of “unauthorized access,” regulation of legitimate cybersecurity research, and requiring security specialists to undergo licensing procedures. The government also seeks to create a clearer distinction between malicious activities and research or protective activities in the cyber domain. This is intended to support the development of the cybersecurity industry and enhance national defense. In addition to reviewing the Computer Misuse Act, the English government has implemented programs to develop more comprehensive frameworks requiring companies to report cyberattacks and security breaches. These programs have gained particular importance from the perspective of greater transparency and greater accountability of the private sector, especially in critical infrastructure sectors such as energy, transportation, and health. Drafting new regulations for stronger protection of citizens’ personal data is another axis of reform (34).

The English government also emphasizes greater convergence between state institutions and the private sector while creating advisory bodies and specialized working groups. This new cooperative approach, especially within the framework of the Cyber Security Council and horizon-scanning programs, leads to continuous monitoring of threats and effective coordination among key actors in this field. Using international experiences and modeling the practices of leading countries in cybersecurity are also on the agenda. Another important aspect of reforms is attention to emerging crimes, such as artificial-intelligence-based attacks, cryptocurrency crimes, and misuse of cloud infrastructure. To prevent and effectively combat these threats, the government seeks to integrate flexible and up-to-date regulations into existing legal frameworks in order to enable responsiveness to future developments. This approach will increase the flexibility and dynamism of the English legal system in confronting cybercrimes (38).

In general, the new path of cyber reforms in England is a combination of reviewing old laws, drafting new regulations, and strengthening participation among the state, the private sector, and the professional cybersecurity community. The success of these initiatives depends on continuous dialogue with stakeholders, training of judges and prosecutors, and the use of new technologies. The outlook of recent reforms is the creation of a transparent, dynamic, and efficient platform for combating and preventing cybercrimes at national and international levels.

b. New Policies for Increasing Transparency, Protecting Victims, and Related Measures

In recent years, the English government, recognizing new threats arising from technologies such as artificial intelligence and the Internet of Things, has adopted new policies to improve transparency and effectiveness in combating cybercrimes. These policies specifically emphasize the need for companies to be transparent about their performance in dealing with cyberattacks, disclosing security incidents, and providing timely information to users and relevant authorities. The aim is for organizations and businesses to assume greater responsibility for their conduct and to help society become aware of the level of risks and potential threats (46). In the field of cyber victim protection, the English government has designed and implemented new strategies such as creating special guidelines for psychological and technical support for victims of digital attacks. This measure is intended to reduce secondary harm and ensure the rapid rehabilitation of victims. Facilitating reporting processes and increasing access to legal advice through online platforms are also examples of these supportive policies (34).

In addition, drafting new guidelines for collecting and using data in a way that protects victims’ rights and privacy has been another axis of government reform. Approaches have moved toward establishing “minimum data-protection standards” and requiring companies to adopt stronger security measures. In this regard, ethical principles and transparency in processing user and victim data have received greater attention than before. In the field of

emerging technologies, especially artificial intelligence and the Internet of Things, the English government is developing laws and policies aimed at identifying legal liability in the face of new threats. For example, frameworks have been proposed to provide a clearer path for legal action and compensation for victims in the event of attacks related to Internet of Things devices or misuse of artificial-intelligence algorithms. Requiring manufacturers and providers of services based on these technologies to comply with security standards is also part of the new protective policies (34).

Transparent and timely reporting of cyberattacks by public and private sectors is another key element of England's new policies. Recent laws require companies to notify regulatory bodies and persons affected by attacks of any significant security incident within a specified period. In addition to increasing public trust, this approach creates a basis for better education and preparedness of society in the face of threats. The government is also seeking to launch educational and awareness-raising campaigns to teach the general public and businesses how to protect themselves against cyberattacks and, if victimized, how to pursue legal and supportive procedures. This approach plays an important role in reducing damage caused by cybercrimes, especially for vulnerable groups and small businesses (47).

Finally, England's new policies for increasing transparency, supporting victims, and preparing for new technologies reflect a progressive and forward-looking vision that remains at the forefront of the rapid evolution of digital technologies. These measures, in addition to more effectively protecting individuals and data, have also enhanced England's position as a leading country in cyber governance and protection of victims' rights in the cyber world.

c. Analysis of the Role of Deterrent and Incentive Policies in Confronting Emerging Cyber Threats

Deterrent policies have always played a key role in controlling and containing cybercrimes. By increasing punishments, developing monitoring mechanisms, and updating anti-intrusion laws, the English government sends a clear message to cybercriminals that such crimes will not go unpunished. Examples such as increasing financial penalties for companies that fail to comply with security requirements or imposing stricter punishments for organized attacks constitute an important part of these deterrent policies. In addition to deterrent policies, the English legislature has paid particular attention to incentive-based tools. Providing financial and credit incentives to companies and organizations that implement advanced security protocols and take training seriously are among effective incentive strategies. The launch of schemes such as Cyber Essentials and national information-security certificates has also been welcomed with the aim of raising security standards and increasing the resilience of the private sector (41).

New regulations drafted in recent years emphasize not only the prevention of cyberattacks but also require companies to continuously upgrade their security infrastructures and report security incidents quickly. These regulations, in line with international requirements and similar European Union laws, have made cybersecurity standards transparent and measurable and have increased the legal responsibilities of companies and managers. The English legislator's forward-looking approach to cyberspace has led to the design of regulations that remain dynamic and flexible in relation to emerging threats. For example, new regulations for technologies such as artificial intelligence, machine learning, and the Internet of Things include policies that enable rapid response to unforeseen vulnerabilities and intelligent attacks. This approach combines risk-based standardization with detailed regulation (37).

In confronting emerging cyber threats, the role of active partnership with the private sector and the technology community has become more prominent than ever. By creating platforms for dialogue, sharing experiences, and exchanging threat information, the government has created appropriate synergy among the state, industry, and researchers to increase national preparedness against complex attacks. Public participation and building trust in government policies are also pillars of the success of these policies. The deterrent and incentive policies of the English government, while creating a balance between legal obligations and support, have provided a basis for preserving technological innovations and users' legitimate freedoms; at the same time, firm and effective response to complex and transnational threats remains a practical priority. This combined model places security and economic development alongside each other and strengthens England's global competitiveness in the cyber domain (41).

Finally, England's experience shows that an intelligent combination of deterrence, through strict regulations and severe punishments, and incentives, through benefits and credits, together with forward-looking laws, is an effective strategy for legitimate and dynamic resilience against new cyber threats. For this reason, the English government's approach has been regarded in many international forums as a successful model.

Revision and Innovation in Criminal Policy-Making for Cybercrimes

With the rapid expansion of information technologies and the emergence of new forms of cybercrime, legal systems around the world, including Iran and the United Kingdom, have faced serious challenges concerning the efficiency and updating of criminal policies. The relentless growth of cyber threats and the complexity of criminal tools have rendered traditional laws and mechanisms unable to effectively confront these crimes and have made deep revision of criminal-policy approaches a necessity. Under such conditions, moving toward structural reform and drafting innovative strategies has gained increased importance. Using comparative experiences, benefiting from new technologies, and broad participation of scientific and specialized institutions can prepare the ground for transformation in criminal policy. Rethinking criminal policy and accepting innovation are not only options for improving cybersecurity but also vital necessities for preserving citizens' rights and ensuring the efficiency of criminal justice in the digital age.

Pathology of Current Policies and the Need for Structural Reforms

The current policy-making systems of Iran and England toward cybercrimes, given the rapid growth of emerging technologies, face fundamental challenges in adapting to and responding to new threats. Many existing laws are unable to effectively cover the broad range of contemporary digital crimes and tools (48). One fundamental weakness is the existence of gaps and ambiguities in defining the concepts of cybercrime and its instances, which has led to differing interpretations among judicial and executive authorities and has reduced the effectiveness of criminal policy-making (34).

Confronting complex threats such as artificial-intelligence-based attacks, supply-chain attacks, and deepfakes requires continuous reform and updating of legal and executive structures; however, the process of these reforms in both countries has been slow and often reactive (49).

In Iran, insufficient coordination among parliament as the legislative branch, the government as the executive branch, and the judiciary has caused interruptions and internal conflicts in the criminal policy-making process and has made the creation of unified practice difficult. The role of the legislative branch in reviewing and reforming

computer-crime laws is highly vital; however, in practice, many proposed reforms either remain inactive due to the absence of political consensus or are implemented in an unstable manner. The executive branch and law-enforcement agencies often lack the specialized infrastructure and tools necessary for effectively pursuing cybercrimes, and this severely limits the effectiveness of current laws (50). In England, the failure to properly update the Computer Misuse Act 1990 after more than three decades has faced serious criticism from experts and executive institutions, because a substantial part of today's threats has not been incorporated into that law. The recent review of Iran's computer-crime law faces challenges such as human-rights concerns, lack of transparency, and political and cultural considerations that prevent achievement of a comprehensive and timely law. In both countries, serious gaps exist in supportive procedures for victims of cybercrimes and in the system for collecting digital evidence; slow progress in developing specialized tools and training human resources has merely added to the complexity of the situation (48).

Limited and uncoordinated cooperation between the private and public sectors is another weakness of current policy-making. Companies and organizations often show little willingness to share their data and experiences with the state. In England, the launch of programs such as the National Cyber Security Centre and the upgrading of supervisory standards indicate the beginning of structural reforms, but implementation problems and slow adaptation remain observable (51). Examples such as the WannaCry attack on the National Health Service in 2017 tangibly revealed England's infrastructural gaps and the inefficiency of interorganizational coordination and raised the need for serious legal reform.

Analytical reports show that most countries, including Iran and England, suffer from weaknesses in regulation and interinstitutional coordination in relation to the detection and prosecution of advanced attacks such as ransomware or unknown malware. The comparative trend in recent legal reviews shows that England, despite its long legislative history, has recently paid more active attention than Iran to the need to repair and strengthen institutions for combating cybercrimes, although this path is still far from full maturity. The future of effective criminal policy-making in the cyber domain depends on structural reforms, dynamic legislation, increased institutional coordination, and continuous updating of cyber training and tools. Without these requirements, no system will be able to respond to emerging threats.

New Strategies for Improving Criminal Policy

New criminal policies for combating cybercrimes must go beyond traditional legislation and follow flexible and technology-oriented models. Risk-based regulation, especially in fields such as artificial intelligence and the Internet of Things, has already become the axis of many policies in leading countries. The development of specific regulations for artificial intelligence and machine-learning algorithms, such as the proposed European Union AI Act, provides a model for other countries so that they can prevent harmful consequences while simultaneously supporting innovation. Policy-making in the field of the Internet of Things requires interinstitutional cooperation and the definition of standards for safety, data protection, and accountability; the United Kingdom's approach in creating a legal framework for Internet of Things security is regarded as a successful example. New strategies must rely on big-data analysis, threat prediction, and proactive regulation rather than a purely reactive approach; such models are being institutionalized in the United States and the United Kingdom (52).

Specialized institutions such as the National Cyber Security Centre in England and Iran's Computer Emergency Response Team play a key role in identifying complex threats and drafting operational guidelines for the entire

country. Cooperation between the legislature, university researchers, and technology companies is increasingly important so that policies remain coordinated with the rapid developments of industry. Universities, as centers of innovation and skilled human-resource training, have a prominent role in shaping forward-looking criminal policies, and examples of cybersecurity research centers in Europe and the United States merit consideration. The private sector, by developing secure-by-design technologies, specialized crime-detection tools, and adaptive frameworks, complements public institutions and drives efficient partnerships in policy-making. International networking and information-sharing among states, companies, and universities pave the way for identifying transnational threats and responding rapidly (52).

Future policies must be based on the principles of privacy by design and security by design and must adopt international standards, including ISO/IEC 27001 and the European General Data Protection Regulation, as guiding models. The experience of Scandinavian countries in the tripartite convergence of judicial, technical, and academic institutions provides valuable insights for comparative policy-making. Innovation in criminal policies depends on the use of emerging technologies such as blockchain to increase transparency and data traceability. Forward-looking approaches, such as scenario writing and horizon analysis, have become strategic tools for criminal policy-making in advanced countries and are used to confront unpredictable threats. International cooperation through conventions such as the Budapest Convention and joint projects coordinates policies and strengthens the possibility of cross-border law enforcement. Ultimately, the combination of smart government, an empowered private sector, and active universities, together with reactive and forward-looking innovation, is the only possible solution for improving effective and sustainable criminal policy in the age of digital threats.

Future Challenges and Opportunities in Confronting Emerging Cyber Threats

Rapid technological developments and the emergence of new cyber phenomena have confronted criminal policymakers with unprecedented challenges. Cybercrimes become more complex every day and, by using new technologies such as artificial intelligence, blockchain, the Internet of Things, and advanced encryption tools, constitute a serious threat to the national, economic, and individual security of countries. Confronting this new reality requires continuous revision of strategies and legal and technical preparedness to deal with threats whose dimensions and scope expand day by day. Alongside these challenges, opportunities have also emerged that can prepare the ground for improving criminal policy-making and making the fight against cybercrimes more effective. Expansion of international cooperation, exchange of successful experiences, increased public awareness, and enhancement of scientific and technical capacities are among the capacities that, if properly managed, can create a safer and stronger future against cyber threats. Responding to these threats will require a combination of innovation, convergence, and forward-looking thinking in criminal policy-making.

The Most Important Emerging Challenges Facing Policy-Making

One of the most important policy-making challenges is the speed of growth of new technologies such as artificial intelligence, the Internet of Things, and cloud computing, which leads to the emergence of new types of cybercrime and confronts policymakers with constant regulatory lag. Ambiguity in jurisdiction and conflict between national and international laws cause many cybercriminals to evade conventional legal mechanisms; weak interstate cooperation further aggravates this problem. Protection of personal data against misuse, unauthorized disclosure, and complex attacks has become one of the most complex challenges of the present era due to the multiplicity of actors and

technological tools. The shortage of specialized human resources equipped with up-to-date skills in the judicial and law-enforcement domains causes delays in identifying and prosecuting cybercriminals and reduces the efficiency of the criminal justice system (48).

The complexity and anonymity of cyberattacks, such as ransomware or supply-chain attacks, have made the detection of evidence, evidentiary attribution, and collection of digital evidence extremely difficult and have threatened the efficiency of criminal investigations. The issue of insider threats and misuse by authorized individuals of access to sensitive systems is a growing danger that traditional laws have been unable to fully anticipate and manage. Another challenge is gaining public trust and guaranteeing citizens' rights against extensive interventions by the state and the private sector in cyberspace so that policies do not result in the violation of fundamental freedoms (53).

Requirements and Opportunities for Developing Cyber Criminal Policy

The development of cyber criminal policy requires continuous updating of laws so that they can respond to new technologies and changing threats. Comparative analyses show that countries must adopt a dynamic and forward-looking legislative system in order to prevent structural lag. One of the basic requirements is strengthening professional and specialized training for judges, officers, and cybercrime experts so that they become familiar with the latest developments and digital tools and acquire the ability to detect, collect, and rely on electronic evidence. Creating mechanisms for cross-sectoral and interinstitutional cooperation, including communication among the state, academic institutions, and technology companies, provides a valuable opportunity for synergy among global information and experiences. The availability of international standard frameworks, such as the General Data Protection Regulation guidelines or ISO/IEC 27001, enables policymakers to preserve a balance between security and civil liberties while observing human-rights principles (54).

One opportunity in criminal policy-making is the use of artificial intelligence and big data for monitoring, predicting, and intelligently countering new patterns of cybercrime, provided that risks are properly managed. Drafting special supportive policies for victims of cybercrimes and improving their access to legal and psychological services not only increases public trust in the justice system but also prevents the growth of social harms arising from cyberspace. The opportunity for international and regional cooperation, especially through agreements such as the Budapest Convention, is a unique opportunity for countries to share their experiences and resources and facilitate transnational confrontation with cybercrimes (55).

Conclusion

The accelerated developments of technology and the emergence of new digital tools between 2020 and 2025 have confronted the traditional order of criminal policy in many countries with fundamental challenges in the field of legislation and combating cybercrimes. Using a comparative approach, this study examined the legislative capacities of Iran and England in this field and showed that the level of success and efficiency of each system is closely related to the degree of updating of legal policy-making and flexibility in the face of technological developments. England, through continuous investment in reforming basic laws such as the Computer Misuse Act 1990 and enacting new regulations such as the Online Safety Act 2023, has been able to identify part of the emerging threats and provide legal solutions for them. This country has also adopted a dynamic and responsive

approach to cybercrimes by pursuing a multifaceted approach combining criminal responses, preventive measures, and victim protection.

By contrast, Iran's legislative model remains based on traditional criminalization policies and a focus on judicial responses. Although steps have been taken to develop the legal framework through the enactment of the Computer Crimes Act and the resolutions of the Supreme Council of Cyberspace, active responsiveness to newly emerging issues and vulnerable new technologies remains weaker. One of the key findings of the present study is the weakness of preventive policy-making and the inadequacy of supportive measures for victims in Iran's criminal policy. While England, through the development of supportive structures and active cooperation among the state, the private sector, and civil institutions, provides better coverage against cyber threats, Iran has largely remained focused on penal tools and the role of security institutions.

The comparative analysis shows that substantive and formal changes in cybercrimes, including the increase in artificial-intelligence-based attacks, advanced phishing, cryptocurrency-based crimes, and privacy-related threats, require a multidimensional and flexible perspective in the legal system. Legislative objectives will not be achieved merely through criminalization, and action must also be taken to develop technical infrastructures, improve digital literacy, and promote international cooperation. In terms of coordination among executive and supervisory bodies, England's experience shows that unity among the government, national police, specialized cyber centers, and the active participation of technology-industry actors has led to the formation of a more effective mechanism for preventing and combating threats. This experience can provide an appropriate model for reforming criminal-policy structures in Iran.

The examination of legal weaknesses in both countries showed that, despite the progress achieved, weaknesses remain in determining the scope of platform liability, regulating data and artificial intelligence, fully protecting victims, and aligning the law with international structures. Resolving these gaps requires interaction and use of international experiences. Accordingly, it is proposed that Iran improve the efficiency of its criminal policy in cyberspace through comprehensive legal revision, adoption of complementary non-penal measures such as education, psychological warnings, and judicial-social support, creation of specialized institutions, and movement toward convergence with global standards. It is also necessary to develop platforms for scientific cooperation and the exchange of empirical data among researchers and policymakers of the two countries, as well as more active participation in international cyber conventions and commissions, so that effective responsiveness to future challenges becomes possible.

Finally, this article emphasizes that legislative criminal policy in the field of cybercrimes must always be dynamic, flexible, and forward-looking in order to remain efficient against the wave of technological innovations and the complex threats of cyberspace. Using successful international experiences and continuously adapting national laws to global requirements is a fundamental strategy for ensuring security and justice in the digital age.

Acknowledgments

We would like to express our appreciation and gratitude to all those who helped us carrying out this study.

Authors' Contributions

All authors equally contributed to this study.

Declaration of Interest

The authors of this article declared no conflict of interest.

Ethical Considerations

All ethical principles were adhered in conducting and writing this article.

Transparency of Data

In accordance with the principles of transparency and open research, we declare that all data and materials used in this study are available upon request.

Funding

This research was carried out independently with personal funding and without the financial support of any governmental or private institution or organization.

References

1. Dehnamaki M, Babaei-Khanesar A, Goldouzian I. Legislative Criminal Policy of the Islamic Republic of Iran Toward Press Crimes: Traditional and Electronic. International Legal Research. 2017;10(35).
2. Hajidehabadi A, Salimi E. Principles of Criminalization in Cyberspace: A Critical Approach to the Computer Crimes Act. Parliament and Strategy Quarterly. 2014;21(80).
3. Quinn F, Elliott C. English Criminal Law. Tehran: Ney Publishing; 2019.
4. Mohammadifard H, Hashemi SH, Darabi S. Criminal Policy Regarding Crimes Against the Moral Dignity of Persons in Cyberspace in Light of Judicial Practice. Comparative Criminal Jurisprudence. 2023;3(4):155-66.
5. Malekshaar M, editor Iran's Legislative Criminal Policy in Countering Crimes Against Chastity in Cyberspace. Fifteenth International Conference on Law and Judicial Sciences; 2023.
6. Deylami-Moezzi N, Esmaili M, Hajitabar-Firouzjaei H. Evaluation of the Legislative Criminal Policy of Iran and the European Union Toward Computer Crimes. International Legal Research. 2022;15(56):105-27.
7. Nazari-Khanqah SG, Jafarzadeh S, Nikkhah-Sarnaqi R. The Role of Participatory Criminal Policy in Preventing Cybercrimes in Iran. Quarterly Journal of Political Research in the Islamic World. 2021;11(4):151-74.
8. Zhang Y, Dong H. Criminal Law Regulation of Cyber Fraud Crimes: From the Perspective of Citizens' Personal Information Protection in the Era of Edge Computing. Journal of Cloud Computing. 2023;12(1):55-64.
9. Raharjo A, Bintoro RW, Utami NAT. The Legal Policy of Criminal Justice Bureaucracy Cybercrime. BestuuR. 2022;10(2):1-19.
10. Sharma R. Legislation Related to Cyber Crimes in United Kingdom. 2020.
11. Ibn Abi Jumhur M. Awali al-La'ali al-Aziziyyah fi al-Ahadith al-Diniyyah. Qom: Mojtaba Iraqi Press; 1985.
12. Ibn al-Athir M. Al-Nihayah fi Gharib al-Hadith wa al-Athar. Cairo: Al-Qahirah Press; 1965.
13. Boba R. Crime Analysis and Crime Mapping. USA: Sage; 2005.
14. Ibn Hazm A. Al-Muhalla. Beirut: Dar al-Jil; 1995.
15. Ibn al-Farra M. Al-Ahkam al-Sultaniyyah. Cairo: Muhammad Hamid Faqi Press; 1938.
16. Qannad F, Akbari M. Security-Oriented Criminal Policy. Criminal Law Research Quarterly. 2017;5(18).
17. Janofsky A. How AI Can Help Stop Cyber Attacks. The Wall Street Journal. 2018.
18. Jahangir I. Shiism in Cyberspace: A Social Approach. 1 ed. Qom: Imam Khomeini Educational and Research Institute Press; 2012.
19. Payne BK. Defining Cybercrime. The Palgrave Handbook of International Cybercrime and Cyberdeviance. Cham: Palgrave Macmillan; 2020.
20. Lazerges C. An Introduction to Criminal Policy. 10 ed. Tehran: Mizan; 2021.
21. Sheikh S, Ghiyasi J, Salehi MK. A Reflection on the Pathology of Substantive Legislative Penal Policy Concerning Currency Crimes Against Security. Iranian Political Sociology Monthly. 2022;5(10).

22. Maleki-Azinabadi R, Jamali J. A Comparative Study of Cyber Laws in China, the United States, and Russia: Requirements and Necessities for Cybersecurity in the Islamic Republic of Iran. Defense Supply and Technology Quarterly. 2024;7(3).
23. Yaghoubi M, Jafari A, Salmanzadeh J. An Examination of the Strengths and Weaknesses of the Law on Publication and Free Access to Information from the Perspective of Jurists. Parliament and Strategy. 2024;31(117).
24. Hajmohammadi A. A Comparative Study of Cyberterrorism in the Criminal Laws of Iran and the United States. 1 ed. Tehran: Mobin Edalat; 2019.
25. Tahmasbi J, Shahmoradi K. Challenges and Gaps in the Process of Adjudicating Cybercrimes. Judiciary Legal Journal. 2018;82(104).
26. Shirmohammadi J, editor An Examination of Challenges and Methods of Proving Cybercrimes. Second National Conference on Cyber Defense; 2019; Maragheh.
27. Hajidehabadi MA, Salimi E. Offending and Victimization of Internet Natives: From Etiology to Responsiveness in the Restorative Paradigm. Criminal Law and Criminology Studies. 2019;49(1).
28. Naseri A. An Analytical Study of Conflicts and Interactions Between Laws Related to Computer Crimes and Audiovisual Offenses in the Iranian Legal System. Scientific Journal of Islamic Humanities Studies. 2024;10(40).
29. Dashti B, Afshari M. A Comparative Study of Cybercrimes in Iran and International Law. Comparative Law Research Quarterly. 2019;3(1).
30. Zandi MR. Preliminary Investigations in Cybercrimes. 1 ed. Tehran: Jangal Publications; 2015.
31. Sadeghi H. Protection of Copyright in Cyberspace in National Law and International Instruments. Judicial Legal Perspectives Quarterly. 2022;19(65).
32. Qannad F, Aligholi A. The Concept and Importance of Personal Data and Privacy and Types of Protection for Them in Cyberspace. Law of New Technologies: Contract Law and New Technologies. 2020;1(1).
33. Moshrefi A, Mohammadali A, Qayoumzadeh M. Protection of Intellectual Property in Cyberspace in Iranian Law and International Instruments. Comparative Research in Jurisprudence, Law, and Politics. 2025;7(1).
34. Wall DS. Cybercrime: The Transformation of Crime in the Information Age: Polity Press; 2023.
35. Brenner SW. Cybercrime: Criminal Threats from Cyberspace: Greenwood Publishing Group; 2010.
36. Zavrsnik A. The Routledge Handbook of Technology, Crime and Justice: Routledge; 2022.
37. Gercke M. Understanding Cybercrime: Phenomena, Challenges and Legal Response. ITU Publications, 2019.
38. Casey E. Handbook of Digital Forensics and Investigation: Academic Press; 2020.
39. Maras MH. Cybercriminology: Oxford University Press; 2017.
40. Clough J. Principles of Cybercrime: Cambridge University Press; 2021.
41. Koops BJ, Goodwin M. Cyberspace, Jurisdiction, and Control: Some Challenges and Solutions. Transnational Legal Theory. 2017;8(2).
42. Moisejevas R, Gineitis A. Jurisdictional Challenges in Fighting Cybercrime. International Comparative Jurisprudence. 2018;4(1).
43. Goode S. Cybercrime, Evidence and Criminal Procedure. Computer Law & Security Review. 2017;33(4).
44. Brown CS. Judicial Approaches to Digital Evidence and Cybercrime in the UK. Information & Communications Technology Law. 2022;31(3).
45. Witzleb N, Lindsay D, Paterson M, Rodrick S. Privacy and Data Protection in the UK: The Law and Practice: Hart Publishing; 2017.
46. Kearney J. The UK's Computer Misuse Act Needs an Overhaul. Computer Law & Security Review. 2022;44(1).
47. Svantesson DJB. Solving the Internet Jurisdiction Puzzle: Oxford University Press; 2016.
48. Sarre R, Lau LY, Chang LC. Responding to Cybercrime: Current Trends. Police Practice and Research. 2018;19(6).
49. Broadhurst R, Grabosky P, Alazab M, Bouhours B, Chon S. Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime. International Journal of Cyber Criminology. 2014;8(1).
50. Malek H, editor Ensuring Cybersecurity in Iran: Challenges and Solutions. Fourth National Conference on Cyber Defense; 2023; Maragheh.
51. Anderson R, Barton C, Bohme R, Clayton R, van Eeten MJG, Levi M, et al. Measuring the Cost of Cybercrime. In: Bohme R, editor. The Economics of Information Security and Privacy. 1 ed2013.
52. Ballot Jones L, Thornton J, De Silva D. Limitations of Risk-Based Artificial Intelligence Regulation: A Structuration Theory Approach. Discover Artificial Intelligence. 2025;5(14).
53. Abdelkarim YA. Jurisdiction Conflicts in Cyberspace: Leeds Beckett University; 2022.

54. Fahey E. The Evolution of EU-US Cybersecurity Law and Policy: On Drivers of Convergence. Journal of European Integration. 2024;46(7).
55. Chen C, Dong B. Digital Forensics Analysis Based on Cybercrime and the Study of the Rule of Law in Space Governance. Open Computer Science. 2023;13(1).