

The Role of The Police In Cybersecurity For The Creative Economy and Tourism Sectors During The Digitalization Transition Period In Pamekasan Regency

Moh. Akbar Adhiyanto

Universitas Trunojoyo Madura, Indonesia
email: akbaradhityaa110203@gmail.com

Dewi Muti'ah

Universitas Trunojoyo Madura, Indonesia
email: dewi.mutiah@trunojoyo.ac.id

Abd. Wachid Habibullah

Universitas Trunojoyo Madura, Indonesia
email: achwahid.habibullah@trunojoyo.ac.id

Abstract

Based on Kaspersky data, there have been 483,980 malicious files targeting business actors in 2023. Seeing this, the role of the Government and the Police has a strategic position in cybersecurity policy efforts for the creative economy and tourism. Pamekasan Regency has potential in the development of the creative economy and tourism, so cybersecurity policies are urgent in the current era of digitalization. This article aims to examine how the role of the Police and the Government in cybersecurity policies is for the creative economy and tourism in the digitalization era. This research was conducted using an empirical juridical method with an exploratory approach. The results of the study show that cybersecurity protection efforts are still not a special concern for the local government and the Pamekasan Regency Police. In addition, policies regarding cybersecurity are still general, which means that they still do not include cybersecurity protection for the creative economy and tourism. Then the results show that the role of the Police is currently only limited to protection on social media (cyberpatrol) and there has been no effort to make cybersecurity policies for the creative economy and tourism sectors. This is influenced by several factors such as the absence of legal regulations, budget limitations, and lack of awareness about cooperation in improving cybersecurity.

Keywords: The Role of the Police; Cybersecurity; Creative Economy and Tourism

INTRODUCTION

Technology and information always provide a very significant benefit to the needs of society. The development of technology and information through new media, namely the internet, has an impact on unlimited social media relationships. In addition, these developments can have implications for social, economic or cultural changes that significantly occur in society so that they will have two consequences, namely positive impacts and negative impacts. The positive impact of technological and information developments can provide E-mail, E-commerce, cyber bank, online business, internet banking, and E-Learning facilities. However, on the other hand, technological and information developments also have a negative impact with the emergence of crimes in the cyber scope (Sari, 2021).

Based on Interpol data in 2020, there have been 907,000 spam, 737 malware incidents, and 48,000 malicious URLs. This proves that there are still many cybercrimes occurring in Indonesia (Ramadhan & Nurnawati, 2023). The State Cyber and Cryptography Agency (BSSN) also recorded that in 2020 the number of cyber attacks reached 495.3 million, an increase of 41 percent from the previous year 2019 which was 290.3 million. Bareskrim also conveyed that there was an increase in cybercrime reports. Where in 2019 there were 4,586 police reports submitted through cyberpatrol, an increase from the previous year of 4,360 reports in 2018. In line with this, cybersecurity is a priority issue in Indonesia (Fitri, 2022). The world of security and defense in cyberspace has created a new perspective, if previously the state was placed as an important element to be protected, then the new perspective that has emerged places humans as the most important element to be protected. This perspective is known as "human security" (Sintiya & Yulianto, 2024). Basically, the cybersecurity efforts implemented by the Indonesian government are the realization of BSSN as a government institution responsible for cybersecurity, which is expected to become the main institution in relation to the implementation of cybersecurity in Indonesia. In its implementation, BSSN has made various efforts to improve cybersecurity in Indonesia (Haryanto & Sutra, 2023).

In addition, the Indonesian government also established a legal regulation, namely Law Number 19 of 2016 concerning amendments to Law No. 11 of 2008 concerning the ITE Law. This law plays a very crucial role that guarantees legal certainty in the field of electronic transactions and cyberspace. However, there is still a need for a more supportive effort to ensure cybersecurity, namely by increasing the potential for the role of the police. As in Article 13 of Law Number 2 of 2002 which gives the National Police the authority to regulate and form authority in tackling certain crimes. Certain in this case, in particular, is the authority to handle criminal cases in the cyberscope (Umra et al., 2024). Then based on the Circular Letter of the National Police Chief Number SE/2/11/2021 concerning ethical cultural awareness to realize a clean, healthy and productive Indonesian digital space, this is a policy of

the Police to implement the ITE Law. This policy is owned by the Police in supervising and preventing crime in cyberspace. The existence of cybersecurity policies should be the full responsibility of both the Police and the local government that needs to be maximized. Cybercrime does not look at the boundaries of a jurisdiction, meaning that cybercrime is very broad and there can be cybercrime that has the potential for the development of the digital economy, namely the creative economy and tourism.

In CNN Indonesia data, it is said that cybercrime continues to target UMKM business actors or the creative economy industry, this was obtained from Kaspersky data which showed 63% or as many as 483,980 malicious file detectors targeting MSMEs during the first five months of 2023 (CNN Indonesia, 2023). The existence of the digital economy plays a role in supporting creative economy business actors in the digital transition change. The next problem is that the threat of cyberattacks has an impact on business actors, as well as the strength of passwords in managing E-commerce applications, internet access, insecure file sharing, phishing attacks on emails and hackers on business actors' accounts. Pamekasan Regency, which is a strategic area located on Madura Island, East Java Province, has the potential for the development of UMKM in it. This was conveyed directly by the Minister of Tourism and Creative Economy of the Republic of Indonesia Sandiaga Uno in the Kato Workshop event, he said that Pamekasan could develop the creative economy sector. So that these developments are also included in utilizing the digital era to market various business products in the creative economy and tourism places (Samsul Arifin, 2022). Therefore, cybersecurity in the current digitalization period is important by involving the role of the Police and the local government in determining the direction of strategic policies in protecting creative economy and tourism business actors.

Thus, based on the background description above, there are several formulations of problems, including: 1. What are the obstacles to local governments in realizing cybersecurity for the creative economy and tourism during the digitalization transition period in Pamekasan Regency, 2. What is the role of the Police in cybersecurity efforts during the digitalization transition period to the creative economy and tourism in Pamekasan Regency. The purpose of this study is to examine the role of the Police and the Government in cybersecurity policy as an effort to protect the creative economy and tourism in the digitalization era. The urgency of this research is based on Kaspersky data stating that cybercrime is growing and in this context that the development of cybercrime can also affect the development of the digital economy and business actors. So, regarding cybersecurity policies for the creative economy and tourism sectors, it is very crucial to see the rapid growth of the world of information technology transforming into the era of digitalization.

In the originality of this research, here we will compare the previous studies with the research to be studied. The first research is titled "Legal Protection of Copyright Content in the Digital Technology-Based Creative Economy-Indonesian Industrial and Business Revolution Era 5.0." This research focuses on examining the

legal protection of the creative economy for copyright content based on digital technology, the industrial and business revolution (Sugihono et al., 2024). The difference with the research studied is that the research entitled "The Role of the Police in Cybersecurity for the Creative Economy and Tourism Sectors in the Digitalization Transition Period in Pamekasan Regency" that this study focuses on discussing the role of the Police and the local government in cybersecurity policy efforts for the creative economy and tourism during the digitalization period in Pamekasan Regency.

The second study is titled "Police Efforts in Overcoming Cyber Hacking in M-Banking Break-In Mode." This research focuses on examining the role of the Police in overcoming the occurrence of Cyber Hacking in the M-banking break-in mode, and discusses the inhibiting factors of the Police in efforts to counter cyber hacking in m-banking break-ins. The difference with the research to be studied is that the research entitled "The Role of the Police in Cybersecurity for the Creative Economy and Tourism Sector in the Digitalization Transition Period in Pamekasan Regency" that this study focuses on discussing the role of the Police in cybersecurity aspects of the creative economy and tourism in Pamekasan, and also examines the inhibiting factors of the Police and the Government in the cyber security of the creative economy and tourism.

METHODS

This research uses a type of empirical juridical research, which is a legal research method that uses empirical facts taken based on human behavior, both verbal behavior obtained in interviews and real behavior carried out through direct observation (Fajar N.D & Achmad, 2010). The empirical juridical method is legal research conducted by examining the actual situation that occurs in society, namely by looking for facts related to the problem (Benuf & Azhar, 2020). In this study, it examines cybersecurity efforts in Pamekasan Regency so that later it will be associated with the facts that occur, namely the role of the Police in cybersecurity for the creative economy and tourism. This research uses an exploratory approach, which is a research conducted to obtain information, explanations and data about things that are not known in general (Mezak, 2006). In this study, data collection techniques are used which are divided into two, namely primary data and secondary data. Primary data were obtained through observation and interviews. The interview technique was carried out in collaboration with the Resort Police, Diskominfo and Disporapar Pamekasan which included 3 resource persons, namely the Head of unit II of the Satreskrim, the Head of the Encryption and Information Security Division of the Diskominfo and the Head of Tourism of the Pamekasan Regency Disporapar. Meanwhile, secondary data collection was obtained through literature studies. Then the next stage is the data analysis method, based on the primary data that has been

collected and then analyzed using secondary data through literature studies. The data analysis method used is qualitative descriptive, descriptive itself is a research intended to provide as accurate data as possible about the circumstances and symptoms that occur (Soekanto Soerjono, 2020). Qualitative descriptive is also intended to understand social phenomena presented in the form of in-depth analysis (Fadli, 2021). This research focuses on research locations in Pamekasan Regency including the Resort Police, Diskominfo and Pamekasan Disporapar.

DISCUSSION AND RESULT

Government Obstacles in Cyber Security to the Creative Economy and Tourism in the Digitalization Transition Period.

Creative economy and tourism are one of the efforts to increase the economic influence, especially the local community, into the development of the digital economy that is developing today. This development is influenced by the sustainable global economic life system, both in the fields of production, distribution and consumption, to give rise to a pattern of use to meet the needs of goods in a creative and innovative way. The increasingly unlimited business creativity indirectly affects the optimal use of resources from those that have no selling value to have high economic value (Pancawati & Widaswara, 2023).

Seeing this, of course, the Pamekasan Regency government gives its best efforts considering that one of the important aspects in the development of the creative economy and tourism in the current digitalization transition era is not only focusing on improving skills and increasing people's creativity in doing business. However, there is one important aspect, namely efforts to protect cyberspace. Based on Article 40 paragraph (2) of Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 explains "The government protects the public interest from all types of disturbances as a result of the misuse of Electronic Information and Electronic Transactions that disturb public order, in accordance with the provisions of laws and regulations." Cybersecurity has become an important problem in the development of information technology, this affects the protection of cybersecurity for creative economy and tourism actors. Based on this, there are three approaches that can be used as a strategy in maintaining and protecting the cyberscope, the first is the technological approach, the second is the socio-cultural-ethical approach, and the third is the legal approach (Komunikasi & Indonesia, 2008).

Based on the facts and data obtained in the three concepts of the approach above, the Pamekasan Regency government cannot always realize it properly, so the realization of cyber security needs to be a strong cooperation, both from various agencies or existing sectors, in this case with agencies that have authority in the protection of communication and information (Communication and Information Service), agencies that oversee aspects of the creative economy and tourism (Disporapar), along with the Police in Pamekasan Regency. In the data obtained that

the cyber security currently implemented has several problems, in the problem there are limitations in realizing cyber security policies in Pamekasan Regency which are still classified as underprivileged in reaching all aspects, this is influenced by several government obstacles as follows:

1. Legal regulations on cyber security instruments within the scope of the region.

Cybersecurity is an ecosystem that involves legal, organizational, skills, cooperation, and engineering implementation aspects in synergy to achieve effective results. The legal aspect in this case is the law, the existing laws are sometimes not specific enough to deal with certain cybercrimes. Cybercrime, which is a very dynamic and rapidly evolving crime, is often faster than the development of legal regulations. As a result, current laws may not have clear enough provisions or definitions to deal with emerging or complex types of cybercrime (Najwa, 2024). Therefore, the law always places its crucial position in the interests of every development in the existing problems. In general, the cyber security legal framework in Indonesia is built based on the Information and Electronic Transactions Law No. 11 of 2008 which was revised into Law No. 19 of 2016, Government Regulation No. 82 of 2012, and ministerial regulations. However, there are fundamental problems related to cybersecurity, such as the weak understanding of stakeholders related to cybersecurity, the need for adequate legality in handling cyberattacks, partial institutional governance, and the weakness of the industry in developing hardware related to information technology (Mahendra & Pinatih, 2023).

One of the facts explains that in Pamekasan Regency, cybersecurity is manifested in the legal basis of the Decree of the Regent of Pamekasan Number: 188/211/432.013/2022 concerning the Establishment of the Computer Security Incident Response Team of Pamekasan Regency (Pamekasan-CSIRT) which was formed through the Communication and Information Service. However, even so, the CSIRT team that was formed still does not have excellence in its implementation, because there are still limitations to its main tasks and functions which are only limited to cybersecurity protection against the Government domain, in this case the protection of government websites. Of course, this is due to the absence of further regulations such as the establishment of a Regional Regulation on Cybersecurity that regulates cybersecurity policies on aspects of the creative economy and tourism. Based on Abdul Hamid Riadi explanation in the formation of the Regional Regulation on cyber security in overshadowing all aspects hampered by the process of forming legal regulations, it takes a very long time. So according to the Head of Encryption and Information Security of Pamekasan Regency, this affects the scope of cybersecurity authority and efforts to protect all existing aspects. In addition, according to Moh. Zahri as the Head of Tourism explained that regarding the authority to protect aspects of the creative

economy and tourism, there are two agencies that oversee it, namely the UKM Cooperative Office and the Disporapar. This is an obstacle in the formation of cybersecurity protection because there is a dualism of authority in it. Thus, the limitations regarding legal regulations result in limitations in the scope of cybersecurity that have not yet reached the creative economy and tourism sectors in Pamekasan Regency to date.

2. Budget factors in cybersecurity in Pamekasan.

There are three approaches that can protect and defend the cyber world against existing cybercrime, namely the legal approach, the ethical-cultural approach and the technological approach. In the technology approach, this approach basically requires a developing technology that can make a non-penal effort or an effort to prevent the occurrence of cybercrime through cyber security policies. This effort is carried out by utilizing special cybersecurity technology which can be in the form of applications or tolls, hardware to infrastructure to monitor and detect cybercrime which can be an effort to prevent cybercrime (Siagian et al., 2018). In its development, the need for technology to improve cybersecurity requires a very large cost budget, this is felt by the government in Pamekasan Regency. Budget limitations influence existing cybersecurity protection policies, the absence of a budget or a small budget can make the availability of advanced tools unrealized. Therefore, the current cybersecurity only relies on makeshift technological tools. So that what is felt by the Diskominfo and Disporapar as well as the Pamekasan Police is the main obstacle in providing more protection for cybersecurity, especially in the creative economy and tourism and not only that, the absence of a cyber crime antidote in Pamekasan is also influenced by the small budget owned by

3. Lack of cooperation between the government, law enforcement officials and the private sector.

A cybersecurity strategy is a set of actions, policies, and practices designed to protect computer systems, networks, software, and data from cyberattacks and other security threats. The strategy also includes training on stakeholder awareness related to cybersecurity, development of sustainability policies related to cybersecurity, and collaboration and partnerships with other cybersecurity agencies to share intelligence and develop technologies related to cybersecurity (Irawan et al., 2024). In the development of cybersecurity policies in the future, a joint coordination force is needed, both the Regional or Central Government, law enforcement officials and the private sector. In Pamekasan Regency, creative economy and tourism have potential in the economic development of the local community. These developments also include the development of the digital-based economic sector, therefore related to cyber security protection for digital-

based creative economy and tourism actors, coordination with stakeholders is needed in developing cybersecurity policy protection in it.

Cybersecurity, the creative economy and tourism, we will see government agencies that have duties, principals and functions in them, including Diskominfo, Disporapar and the Pamekasan Regency Police. However, in the facts obtained, there is no coordination between the three agencies, and even the private sector is still not involved in efforts to develop cyber security policies. This is because cybersecurity has not been a full concern of the government and law enforcement agencies in it, it has an impact on the inability to realize the development of cyber security policies through joint coordination efforts for the creative economy and tourism sectors in Pamekasan.

Regarding cybersecurity policy, in principle, it has been outlined in the Presidential Instruction or Presidential Instruction Number 3 of 2003 concerning national policies and strategies for the development of E-Government. In this provision, it instructs related to policies in dealing with the challenges of using cyber facilities in public services which include the following: First, it is widely guaranteed for accessing, managing and utilizing information in a large capacity quickly and accurately, Second, policies through E-Government will increase the efficiency, effectiveness, transparency and accountability of government administration, Third, ensuring the implementation of good policies by improving effective and efficient public services requires policies and strategies through E-Government, and Fourth, the need for common understanding, harmony of actions and integration between government agencies (Ika & Anita, 2020). Based on the provisions in Presidential Instruction No. 3 of 2003, in principle there are several strategic steps that can be realized to realize cyber security in Pamekasan Regency, including: (Budi et al., 2021)

- a. Increasing the capacity of authorized agencies in cybersecurity, increasing capacity between agencies is by improving the capabilities of human resources by providing cybersecurity skills training carried out by the coordination of the Cyber Operations Center work team. This is being done to increase understanding of preventive measures by improving the cyber defense system for the creative economy and tourism.
- b. With the establishment of a law (Regional Regulation on cyber protection of the creative economy and tourism), the law has a strategic position in determining the direction of policy, the absence of regulation is the main factor in cybersecurity policies cannot be realized. In principle, the cybersecurity established by the Pamekasan government is manifested in the Regent's Decree Number: 188/211/432.013/2022 concerning the Pamekasan Regency Computer Security Incident Response Team. However, the regulation has not explicitly regulated the protection of the creative economy and tourism. Thus, special

regulations in regulating cybersecurity policies for the creative economy and tourism sectors are the main thing in its formation, seeing that cyber attacks can have a bad impact on business actors.

- c. Cooperation between agencies in improving cyber security and cybersecurity is a very complex problem. This cannot eliminate the role of the government, the police and the private sector in determining E-Government as stated in Presidential Instruction No. 3 of 2003. As in the fourth point above, it is explained that there needs to be a common understanding, harmony of actions and integration between government agencies (government agencies in this case include Diskominfo, Disporapar and the Police). Cooperation between agencies can improve cybersecurity governance, the implementation of the multi-stakeholder principle is very important. Without cooperation and collaboration among stakeholders starting from the authorities, the private sector, to academia and the public), problems related to cybersecurity will continue to be one-dimensional and incomplete (Budi et al., 2021).

The Role of the Police in Cyber Security for the Creative Economy and Tourism Sector in Pamekasan Regency.

The application of criminal law in Indonesia to overcome a form of crime is not a fundamental problem, this can be seen from the practice of legislation that has shown that the use of criminal law is an inseparable form of legal policy or politics used in Indonesia. In the Criminal Code (KUHP), which is the main system for criminal law regulations in Indonesia, the formulation of criminal acts listed in the Criminal Code is mostly still conventional, in the sense that it is still not directly related to the development of cybercrime itself. Therefore, the position of the Police currently plays a crucial role in eradicating and protecting all aspects of crime, one of which is cybercrime (Sari, 2021, p. 61).

Referring to the Circular Letter of the National Police Chief Number SE/2/11/2021 concerning ethical cultural awareness to realize a clean, healthy and productive Indonesian digital space. As well as Telegram Letter/339/II/RES.1.1.1./2021 concerning guidelines for handling cybercrime cases using the ITE Law. Where the two policy rules are policy efforts in the implementation of Law No. 19 of 2016 concerning ITE. The two policy rules make the authority of the Police in eradicating crime in cyberspace by prioritizing efforts through preemptive and preventive. For example, in countering cybercrime, law enforcement agencies in various countries have established specialized units composed of information technology experts, cybercrime analysts, and investigators specially trained to deal with cyberattacks (Farhan et al., 2023). In Indonesia itself, a special cyber unit was formed based on Perpol Number 14 of 2018. The Directorate of Cyber Investigation (Ditressiber) has the function of conducting investigations and investigations of cybercrimes as well as detecting and analyzing suspected cybercrimes (Nadia Putri R, 2024). However, the *Justitia Jurnal Hukum*, Vol 9, No 1, 2025, 33-50

existence of the Ditressiber currently has limitations that currently only exist in 8 Regional Provincial Police (Polda) in Indonesia and does not include the formation of a special cyber unit in the Regency/City.

Overall, cybercrime law enforcement is a complex and ever-moving job. To be able to create a safe cyberspace environment, an integrated approach is needed that involves cooperation between the government, law enforcement agencies, the private sector (stakeholders), and the community. To meet these challenges and protect communities from the threat of cybercrime, there is a need for continued cooperation and investment in capacity and technology to improve cybersecurity. As Barda Nawawi Arief argued that in efforts to combat crime, especially cybercrime, it must be passed with several policy approaches, such as: a). There is an integration between criminal politics and social politics; b). There is an integration between efforts to eradicate crime with penal and non-penal (Arief, 2017). As in integral policy theory, criminal law in countering cybercrime requires an integrated combination of penal and non-penal policies in a planned, focused, and professional manner.

As the policy is intended, efforts to combat cybercrime are essentially an integral part of efforts to protect the community (social defence) and efforts to achieve community welfare (social welfare). So that the integration between the penal facilities policy and the non-penal facilities policy is essentially a sub-part of the criminal policy itself. Thus, as an effort to improve cybersecurity, it encourages and makes non-penal policies have a strategic role in it. The strategic position of non-penal policies can be seen in the Resolution of the UN Congress VII/1990 on "Computer related crimes" which proposes several policies in the context of efforts to tackle cybercrime, among others: 1). Modernizing material criminal law and criminal procedure law, 2). Develop computer prevention and security measures, and 3). Conducting training efforts for judges, officials, and law enforcement officials on economic crimes and cybercrime (Mufid, 2017). As referred to as computer prevention and security measures as in point 2 above, it can be interpreted as preventive efforts used in preventing the occurrence of cybercrime, in the sense that it includes policies on prevention and countermeasures with technological advances (techno prevention). Policies through cyber security are basically inseparable from the use of technological advancements, cyber security requires that to be able to prevent cybercrime, it is necessary to utilize technological advances and integration using a structured approach.

Based on the explanation described above, in the facts obtained, the Pamekasan Police have currently developed innovations through integrated criminal law policies by using a technological approach (techno prevention) as an effort to overcome cybercrime. The integral policy of criminal law itself is to integrate policies between crime prevention efforts with penal and non-penal means (Arief, 2017), In this case, it is implemented using one of the technological approaches. The technological approach is a non-penal effort of criminal law to prevent the occurrence of cybercrime

that uses technological advances to be able to prevent technological methods. Forms of techno prevention can be in the form of restrictions on negative content or illegal content, blocking of unregistered sites or applications, personal data protection applications and Cyber Patrol. This is based on the IIIC (International Information Industry Congress), in the IIIC it is explained that as the key to tackling cybercrime, it is possible to use technological means so that in its prevention and countermeasures, technology is also needed in solving it (Rendie, 2024).

Based on this explanation in the cybercrime prevention policy, the role of the Police is to realize cybersecurity policies in the form of "Cyber Patrol". This is actively carried out by the Pamekasan Resort Police in monitoring the activities of the internet space in Pamekasan. The Cyber Patrol is carried out by conducting 24-hour surveillance and monitoring of cyberspace or social media activities in Pamekasan carried out by the Intelligence and Technology (Intelligence and Technology) Satintelkam and Satreskrim Unit. Based on the monitoring data carried out, there are cases of cybercrime that have occurred in Pamekasan Regency that have had various forms of crime, this was conveyed by the Head II of the IPDA Satreskrim Muhammad Eko Feriyanto. The following is a table related to cybercrime cases, both handled and not handled by the Pamekasan Resort Police:

Table 1. Number of Cybercrime Cases in 2024.

Number.	Types of Cybercrime			Years	Number of cases that occurred	Number of cases that have been handled
1	Defamation			2024	3 (three)	1 case
2	Online	Scams	Via	2024	3 (three)	3 cases
	Facebook		and			
	Telegram					
3	Sexual Harassment (Immoral)			2024	1 (one)	1 case
4	Hacker			2024	2 (two)	0 case
5	Online Gambling			2024	2 (two)	2 cases

Based on the table above, it can be explained that in handling cybercrime, the role of the Police has basically been actively working to overcome cybercrime that occurs in Pamekasan. In this case, there are 3 cases of online fraud that have been resolved, as well as cases of defamation, sexual harassment and online gambling that have been handled in the settlement of the case in 2024. However, there are still weaknesses in handling crime cases that have not been handled in an integrated

manner, in this case the existence of hacker crimes. The obstacle in solving hacker crimes is that the Police consider hacker crimes not to be the domain of the Police's authority currently, considering that this is the authority of the Communication and Information Service (Diskominfo). In addition, technology-related obstacles are currently still not able to track anonymous account users or hackers. However, according to Muhammad Eko Feriyanto, during the 2024 period, cyberattacks against creative economy and tourism business actors have not yet occurred and until now the Satreskrim has not received reports related to the crime.

Basically, regarding the existence of cybersecurity efforts policies which are manifested in the form of Cyber Patrol that actively supervise cyberspace activities, it is an innovation in keeping up with technological and information developments and to compete with the development of cybercrime. In principle, the duties and scope of the Cyber Patrol itself include cyber campaigns and education in the community, proactive detection and prevention and collaborative law enforcement in cyberspace. In the mechanism of Cyber Patrol implemented in Pamekasan Regency currently supervises all community activities in social media activities, this is actively carried out for 24 hours by continuing to provide supervision and monitoring in cyberspace and in the event of a cybercrime case. The Cyber Patrol is tasked with helping to take down all cybercrime posts with negative content such as hoax news, defamation, immorality or hate speech. The Cyber Patrol policy carried out by the Satintelkam team and the Pamekasan Satreskrim unit is part of the investigation process about cybercrime activities to provide supervision of cyberspace in Pamekasan. Currently, the obstacle is that the current technology still does not have a high level of sophistication. The reason is that there are still many shortcomings that occur in the tools we have today, this was conveyed by Muhammad Eko Feriyanto who explained that the technological tools used are still not able to reach cybersecurity widely because the technological tools are still only limited to tracking "IMEI trash" and "cek post cp (tracking through phone numbers)".

So that if you look at the role of the Police in cybersecurity in Pamekasan, in fact it has been realized in the form of Cyber Patrol, but the policy has an obstacle that the technology used still does not reach the protection of the creative economy and tourism. Based on Law Number 02 of 2002 concerning the National Police of the Republic of Indonesia in Article 13 states "The main duties of the National Police include: a. Maintaining public security and order, b. Enforce the law, c. Providing protection, protection, and service to the community. This provision is none other than the authority of the Police in protecting all aspects of society, including the creative economy and tourism. The creative economy and tourism have now entered a digitalization transition, therefore the development of the digital economy, it is very important for policymakers to focus on increasing digital literacy to be able to build a cybersecurity system. Cybersecurity strategy policy development steps for the

creative economy and tourism have the potential to mitigate cyber threats, protect their digital assets, and can improve their defense and competitiveness in the development of the digital economy (Napu et al., 2024). Therefore, the growing number of cybercrimes without a strong cybersecurity system provides great opportunities for cybercrime perpetrators who target creative economy and tourism business actors in the current digital transition period.

Hackers/cracking, phishing, and skimming will be crimes that will often occur if cybersecurity is still not implemented against business actors. Hackers themselves are those who like to play the internet, browsing other people's internet sites if they damage it is called cracking (Hartono, 2014). Hackers still have not found a solution to handle it because the Cyber Patrol in Pamekasan is still focusing on monitoring cyber activities. Hackers have the potential to interfere with, damage and steal personal data through business actors' accounts in developing their businesses in the digital space. If cybercrime is growing, crimes in the form of phishing will become an opportunity for crimes that will occur in the future. Phishing is the act of obtaining personal information such as User ID, PIN, bank account number, credit card number illegally. This information will then be used by the fraudster to access an account, commit a credit card fraud or guide them to make a transfer to a certain account under the lure of a reward (Caniago & Sutabri, 2023). The creative economy and tourism that have switched to a digital economy during the digital transition period urge business actors to follow the flow of technological developments, if local communities do not have the ability to protect their personal data and awareness of technology, it will have an impact on the vulnerability of personal data of business people, one of which is the creative economy and tourism.

The limitations in protecting the creative economy and tourism sectors are caused by the absence of a legal basis that currently exists, the legal basis of the Pamekasan Police in cybersecurity policy still holds the ITE Law as the foundation. In addition, the legal basis of the Diskominfo has not regulated cyber protection for the creative economy and tourism sectors in Pamekasan. So, there is still no underlying policy in cybersecurity protection for the creative economy and tourism sectors. In fact, the fact that cybercrime currently targets business actors as easy targets, because the vulnerability and awareness of businesspeople is very low regarding the security of their personal data in cyberspace. Based on this, there are strategic steps that can be applied as an effort to maximize cyber security protection apart from the formation of legislation through Regional Regulations in protecting the creative economy and tourism sectors and increasing cooperation efforts between authorized agencies, both the Police, Regional or Central Governments, and the Private Sector. There are approaches that can be taken as an effort to protect aspects of the creative economy and tourism, which include: Cultural Approach, Moral (educational) approach, scientific approach and global approach (Haryadi, 2012).

- a. Cultural Approach, this approach is a preventive effort carried out by knowing and complying with ethics (Cyberethics) in utilizing technological advances. This approach can serve as a prevention against the impact and existence of cybercrime by providing an understanding and compliance with internet ethics;
- b. Moral (educational) approach, an educational approach is a strategic step that can be applied if the technological approach, legal approach and cultural approach are no longer effective. This approach is carried out by providing moral, religious and knowledge related to cybercrime. Through this, in addition to being able to build awareness of the impact of cybercrime, it can also increase people's digital literacy, so that people can improve their ability and understanding of personal data protection in the use of information technology in the digital world;
- c. Scientific Approach, a scientific approach, is an approach that is carried out by using scientific principles and methods. The scientific approach aims to develop science and applications that can have a better, effective and efficient impact (Frensh dkk., 2017);
- d. Global Approach, a global approach is carried out by conducting bilateral and multilateral agreements related to cybersecurity. Cybercrime is a crime that can be committed without being hindered by territorial boundaries, therefore cyber security protection for digital economy business actors is crucial in terms of building international cooperation between countries.

CONCLUSION

Cybercrime has always been a concern for developments in the era of digitalization, and special attention to the existence of cybersecurity policies for the creative economy and tourism sectors. Pamekasan Regency is a strategic area in the development of creative economy and tourism, due to the potential of local communities in developing their own tourism places and local products. The cybersecurity system that is developing today still has several weaknesses due to the lack of attention from the local government. Cybersecurity that is of concern to the Pamekasan government is the realization of the CSRIT Team by the Pamekasan Diskominfo. However, this is not the main weapon in the cyber security system policy in Pamekasan. The reason is that the role of the Police in cybersecurity in the Pamekasan Regency area also has an important role in all activities and developments of the community in the digital world. The cybersecurity system that has been formed today is an application of the ITE Law itself and the existence of new policies that use a technological approach (techno prevention). Cyber Patrol as a technological approach plays a role in supervising all cyberspace activities. However, the cybersecurity policy carried out by the Diskominfo and the Pamekasan Police still does not cover the creative economy and tourism sectors. So, there is still no policy

from the government and the Police in building a cybersecurity system for the creative economy and tourism sectors. The obstacles are related to legal regulations, budgets that affect the availability of advanced technological tools and lack of awareness of the coordination of the Government, the private sector and the Police.

Based on this as in Presidential Instruction Number 03 of 2003 concerning national policies and strategies for the development of E-Government. In principle, the policy instructs strategic steps that can be applied in the development of cybersecurity policies for the creative economy and tourism sectors which include: a. Increasing the capacity of authorized agencies in the development of cybersecurity policies, both law enforcement officials, Regional or Central Governments and the Private Sector, b. Forming laws and regulations through Regional Regulations related to rules in protecting and improving cybersecurity for the creative economy and tourism sectors, c. Increasing cooperation between agencies in the formation and development of protection for the creative economy and tourism sectors. In addition, there are also several approaches that can be used as an effort to improve cybersecurity policies which include: cultural approach, moral (educational) approach, scientific approach and global approach.

REFERENCES

- Arief, B. N. (2017). *Bunga rampai kebijakan hukum pidana: Perkembangan penyusunan konsep KUHP baru* (cet. 6). Prenada Media Group.
- Benuf, K., & Azhar, M. (2020). Metodologi Penelitian Hukum sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer. *Gema Keadilan*, 7(1), 20–33.
- Budi, E., Wira, D., & Infantono, A. (2021). Strategi penguatan cyber security guna mewujudkan keamanan nasional di era society 5.0. *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia p-ISSN*, 2086, 5805. <https://www.academia.edu/download/85669790/141.pdf>
- Caniago, K., & Sutabri, T. (2023). Tindak Kejahatan Phising Di Sektor Pelayan Di Universitas Bina Insan Lubuklinggau. *Jurasik (Jurnal Riset Sistem Informasi dan Teknik Informatika)*, 8(1), 117–125.
- CNN Indonesia. (2023). *UMKM Jadi Incaran Penjahat Siber, Waspada Menyusup dari Karyawan*. <https://www.cnnindonesia.com/teknologi/20230702203036-192-968608/umkm-jadi-incaran-penjahat-siber-waspada-menyusup-dari-karyawan>
- Fadli, M. R. (2021). Memahami desain metode penelitian kualitatif. *Humanika, Kajian Ilmiah Mata Kuliah Umum*, 21(1), 33–54.
- Fajar N.D, M., & Achmad, Y. (2010). *Dualisme penelitian hukum: Normatif & empiris*. Pustaka pelajar.
- Farhan, M., Syaefunaldi, R., Hidayat, D. R. D., & Hosnah, A. U. (2023). Penerapan Hukum Dalam Menanggulangi Kejahatan Siber Penegakan Hukum Terhadap

- Tindak Pidana Siber. *Kultura: Jurnal Ilmu Hukum, Sosial, dan Humaniora*, 1(6), 8–20.
- Fitri, S. N. (2022). Politik Hukum Pembentukan Cyber Law Undang-Undang Informasi dan Transaksi Elektronik di Indonesia. *Jurnal Justisia: Jurnal Ilmu Hukum, Perundang-Undangan Dan Pranata Sosial*, 7(1), 104–124.
- Frensh, W. F., Kalo, S., Mulyadi, M., & Bariah, C. (2017). Kebijakan Kriminal Penanggulangan Cyber Bullying terhadap Anak sebagai Korban. *USU Law Journal*, 5(2), 164999.
- Hartono, B. (2014). Hacker Dalam Perspektif Hukum Indonesia. *Masalah-Masalah Hukum*, 43(1), 23–30.
- Haryadi, D. (2012). *Kebijakan Integral Penanggulangan Cyberporn di Indonesia*. Penerbit Lima.
- Haryanto, A., & Sutra, S. M. (2023). Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020. *Global Political Studies Journal*, 7(1), 56–69.
- Ika, R. P., & Anita, A. (2020). Smartcity: Model Ketahanan Siber Untuk Usaha Kecil Dan Menengah. *Jurnal Ketahanan Nasional*, 26(3). <http://doc-pak.undip.ac.id/id/eprint/8421/1/Jurnal%20Nasional%20Smartcity%20%20Model%20Ketahanan%20Siber%20Untuk%20Usaha%20Kecil%20Dan%20Menengah.pdf>
- Irawan, A., Fadholi, W. H. N., Erikamaretha, Z., & Sinlae, F. (2024). Tantangan dan Strategi Manajemen Keamanan Siber di Indonesia berbasis IoT. *JOURNAL ZETROEM*, 6(1), Article 1. <https://doi.org/10.36526/ztr.v6i1.3376>
- Komunikasi, D., & Indonesia, I. R. (2008). Naskah Akademik Rancangan Undang-Undang Tentang Informasi dan Transaksi Elektronik. *Jakarta, Kementerian Komunikasi dan Informatika RI, Jakarta*.
- Mahendra, Y. C., & Pinatih, N. K. D. S. A. P. (2023). STRATEGI PENANGANAN KEAMANAN SIBER (CYBER SECURITY) DI INDONESIA. *Jurnal Review Pendidikan Dan Pengajaran (JRPP)*, 6(4), 1941–1949. <https://doi.org/10.31004/jrpp.v6i4.20659>
- Mezak, M. H. (2006). *Jenis, metode dan pendekatan dalam penelitian hukum*. https://www.academia.edu/download/33676150/lw-05-03-2006-jenis_metode_dan_pendekatan.pdf
- Mufid, F. L. (2017). *KEBIJAKAN INTEGRAL HUKUM PIDANA DENGAN TECHNO PREVENTION DALAM UPAYA PENCEGAHAN KEJAHATAN CYBERBULLYING* [Thesis, Universitas Jember]. <https://repository.unej.ac.id/xmlui/handle/123456789/82803>
- Nadia Putri R. (2024). *Polri: Pembentukan Ditressiber jadi komitmen lawan kejahatan siber – ANTARA News*. <https://www.antaranews.com/berita/4352291/polri-pembentukan-ditressiber-jadi-komitmen-lawan-kejahatan-siber>

- Najwa, F. R. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia. *AL-BAHTS: Jurnal Ilmu Sosial, Politik, dan Hukum*, 2(1), Article 1. <https://doi.org/10.32520/albahts.v2i1.3044>
- Napu, I. A., Supriatna, E., Safitri, C., & Destiana, R. (2024). Analisis Peran Keamanan Siber dan Keterampilan Digital dalam Pertumbuhan Usaha Kecil Menengah di Era Ekonomi Digital di Indonesia. *Sanskara Ekonomi dan Kewirausahaan*, 2(03), 156-167.
- Pancawati, A. P. A., & Widaswara, R. Y. (2023). Pengembangan Ekonomi Kreatif dalam Meningkatkan Potensi Pariwisata. *Jurnal Ekonomi Bisnis Dan Akuntansi*, 3(1), 166-178.
- Ramadhan, I. H., & Nurnawati, E. K. (2023). Analisis Kesadaran Mahasiswa Terhadap Bahaya Cybercrime Di Media Sosial. *JTKSI (Jurnal Teknologi Komputer dan Sistem Informasi)*, 6(1), 38-44.
- Rendie, M. S. P. (2024). *KEBIJAKAN INTEGRAL DALAM PENANGGULANGAN KEJAHATAN PELECEHAN SEKSUAL SECARA VERBAL BERBASIS TECHNO PREVENTION* [PhD Thesis, UNIVERSITAS LAMPUNG]. <http://digilib.unila.ac.id/78049/>
- Samsul Arifin. (2022, Mei 26). *Pamekasan Sangat Berpeluang Kembangkan Sektor Ekonomi Kreatif*. <https://beritajatim.com/pamekasan-sangat-berpeluang-kembangkan-sektor-ekonomi-kreatif>
- Sari, U. I. P. (2021). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *Jurnal Studia Legalia*, 2(01), 58-77.
- Siagian, L., Budiarto, A., & Simatupang, S. (2018). Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional. *Peperangan Asimetris (PA)*, 4(3). <https://www.academia.edu/download/101787688/288021744.pdf>
- Sintiya, T., & Yulianto, R. Y. (2024). ANALISIS KEBIJAKAN INDONESIA TERKAIT DENGAN PERLINDUNGAN DATA DIRI WARGA NEGARA INDONESIA. *Case Law: Journal of Law*, 5(1), 1-17.
- Soekanto Soerjono. (2020). *Pengantar Penelitian Hukum*. UI Publising.
- Sugihono, B., Ciang, D., & Yeo, J. A. (2024). Perlindungan Hukum Konten Hak Cipta dalam Ekonomi Kreatif Berbasis Teknologi Digital-Revolusi Industri dan Bisnis Indonesia Era 5.0. *Anthology: Inside Intellectual Property Rights*, 2(1), 49-72.
- Umra, S. I., Adhyaksa, A., & Putra, G. P. (2024). Strategi Pemerintah dalam Melindungi Hak Cipta di Era Globalisasi. *Innovative: Journal Of Social Science Research*, 4(4), 1875-1886.