СЕКЦІЯ 2

ГЛОБАЛЬНІ ВИКЛИКИ ТА СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ МІЖНАРОДНОГО ПРАВА

SECTION 2

GLOBAL CHALLENGES AND MODERNTRENDS IN THE DEVELOPMENT OF INTERNATIONAL LAW

Beska S. V.
PhD candidate at the
West Ukrainian National University,
Member of the European Law Institute (ELI),
Mentor Invisible University for Ukraine (CEU)

MECHANISMS OF APPLYING LEGISLATION IN INFORMATION PROTECTION WITHIN EUROPEAN INTEGRATION

Abstract: This research examines the mechanisms for applying information protection legislation during European integration, focusing on harmonization, directives and regulations, national implementation, cross-border cooperation, and awareness programs. The study aims to analyze the effectiveness of these mechanisms in creating a robust legal framework for information protection amidst European integration processes. European integration aims to create a unified legal framework across participating countries, including the field of information law. Harmonization is a crucial mechanism to ensure consistency in laws and regulations across participating countries. It involves aligning legislation related to data privacy, cybersecurity, and intellectual property rights. Harmonization helps create a level playing field for businesses and individuals operating within the integrated European market.

The European Union (EU) issues directives and regulations that member states must implement within a specified timeframe. In the field of information protection, directives and regulations such as the General Data Protection Regulation (GDPR) provide a comprehensive legal framework to regulate data privacy.

Member states are responsible for implementing and enforcing EU directives and regulations at a national level. This mechanism requires member states to pass new laws or amend existing ones to align with EU requirements. Given the interconnected nature of information relations, cross-border cooperation is essential.

Data protection authorities collaborate with each other and with relevant entities such as law enforcement agencies and judicial authorities to address cross-border data breaches, cybercrimes, and other information security concerns. This mechanism ensures effective collaboration and exchange of information to address transnational issues.

To ensure effective application of legislation in the field of information protection, awareness and education programs are essential. Member states, along with EU institutions, promote awareness campaigns, training, and educational initiatives to inform individuals, businesses, and organizations about their rights and obligations under the applicable legislation. This mechanism enhances compliance and empowers stakeholders to protect their information and privacy rights.

Main Question: How do the mechanisms of legislation application contribute to the protection of information relations in the context of European integration, and what is their effectiveness in creating a unified legal framework?

The key words for the research:

Legislation, Information law, European integration, Data protection, Mechanisms.

Methods of scientific research:

1. Comparative legal analysis of information protection laws across European Union member states
2. Examination of EU directives and regulations related to data privacy and cybersecurity
3. Case studies on the application and enforcement of data protection laws at the national level

Mechanism of application of the General Data Protection Regulation (GDPR).

In this regard, it should be noted that the European General Data Protection Regulation (GDPR) has entered into force. The first-of-its-kind policy showed great promise during development; it aimed to harmonize privacy and data protection laws across Europe, while helping EU citizens better understand how their personal information is used and encouraging them to lodge a complaint if their rights have been breached. As a new regulatory framework, GDPR was a confirmation that the digital economy—based on (personal) information—must work with informed consent from users and clear rules for companies seeking to do business in the European Union.

However, the implementation of this policy demonstrates how much more needs to be done before GDPR is fully operational. European citizens, corporations and data management systems still face many of the problems that the GDPR was intended to alleviate, as well as several new ones. Tougher fines, closer cooperation and recognition of some of the policy's flaws are desperately needed to make GDPR more effective in the coming months and years. [1].

Global concern for the protection of citizens' data

The political will and mandate of the GDPR was driven by concerns that people's personal information was being used in ways that undermined privacy and, by extension, democracy.

Austrian lawyer and privacy activist Max Schrems has been instrumental in raising both awareness of and legal response to the use of Europeans' personal information. After studying in the United States in 2011, Schrems returned to Europe and submitted a request to Facebook for all the information the company

had about him. Shocked by the 1,200-page response, Schrems founded the Europe Against Facebook group, which until 2017 helped build a popular case and support expanded privacy and data rights as outlined in the GDPR. Given that the GDPR is citizen-centric, the regulation's impact on individuals—in Europe and elsewhere—is an important guide to understanding its successes and failures.

The issue of the mechanism of application of legislation on data protection, as a key concept in the field of information protection in Ukraine is formed by bodies and officials persons authorized to perform state functions in this area. By law, they are empowered to protect personal data, control compliance with legislation in the field of personal data. In Art. 22 of the Law of Ukraine "On Personal Data Protection" an exhaustive list of bodies that monitor compliance with the legislation has been determined on the protection of personal data within the limits of the powers provided for by law. These include:

Commissioner of the Verkhovna Rada of Ukraine for human rights and courts.

Since the Regulation of the European Parliament and the Council (EU) 216/679 of 27.04.2016 on the protection of natural persons in the processing of personal data and on the free movement of such data, and on the repeal of Directive 95/46/EU (General Data Protection Regulation) [2]. It is implemented in the legislation of Ukraine as an international legal act in the field of personal data protection on the Internet consent to the mandatory application of which was granted by the Verkhovna Rada of Ukraine. This document is

relevant today, Given that the GDPR is citizen-centric, the regulation's impact on individuals—in Europe and elsewhere—is an important guide to understanding its successes and failures.

Informed consent: However, success must first be defined. Since the implementation of GDPR, more people have clicked "I agree" and "I accept" than in previous years. In fact, for most people, pop-up buttons and constant emails asking for consent were the main interactions with the new legislation; providing a privacy notice and asking for user consent were the dominant compliance approaches used by most organizations. However, the act of quickly clicking a button is quite incompatible with the concept of meaningful consent, especially when there is "consent fatigue" in the face of an endless stream of vaguely worded, often illegible notifications. For this reason, allowing organizations to use this form of individual consent to signal compliance may not be the most effective means of reducing the use of individuals' data without their knowledge.

First, the legal framework plays a key role in establishing standards, rules and guarantees to ensure the confidentiality, integrity and availability of information in accordance with European norms. Effective implementation and enforcement of these laws are essential to build trust, compliance and harmonization with EU directives.

Secondly, the effectiveness of legislative mechanisms in creating a unified legal framework lies in their ability to solve emerging challenges in the field of information security, data privacy and cross-border data flows. By harmonizing European standards and practices, Ukraine can improve its legal environment to facilitate seamless integration and cooperation in the digital sphere.

In addition, the study highlights the importance of continually evaluating, adapting and improving legislative measures to keep pace with technological advances, new threats and the changing regulatory landscape. A proactive approach to the

application of legislation based on best practices and international standards can strengthen Ukraine's position in the European integration process and contribute to the construction of a reliable information security system.

SCIENTIFIC SOURCES:

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). In force: This act has been changed. Current consolidated version: 04/05/2016. ELI: http://data.europa.eu/eli/reg/2016/679/oj
2. Law of Ukraine "On Information" No. 2657-XI of October 2, 1992 // Bulletin of the Verkhovna Rada of Ukraine (VVR). – 1992. – No. 48. – Art. 650.

Roman Maydanyk
Prof. Dr., Professor at the Department of Civil Law
Taras Shevchenko National University of Kyiv

DOCTRINE OF COUNTER-MEASURES IN THE INTERNATIONAL LAW

This study focuses on the doctrine of retaliation against armed aggression in international law. One of the prerequisites for the early cessation of the armed aggression of the Russian Federation is the creation of effective self-defence of Ukraine and third states against this gross violation of international law, which necessitates the introduction of the provisions of the doctrine of retaliation against armed aggression into international law. This study will characterise the doctrine of counter-measures against armed aggression in international law. This study focuses on the development of the guiding principle of counter-measures against armed aggression.

Compensation for damage caused by armed aggression is the result of the exercise, in response to armed aggression, of the right to self-defense enshrined in Article 51 of the UN Charter, according to which a UN Member has the inherent right to individual or collective self-defense in the event of an armed attack.

In this context, the idea of the right of the injured person, including the state and injured individuals and legal entities of the state, to countermeasures as a means of self-defense and a universal basis for property liability for damage caused by armed aggression is worthy of attention. By their legal nature, these retaliatory measures by private legal entities and individuals are a measure of property liability based on tort principles and the tort exception to the rule of state immunity for claims and recoveries on sovereign property for damage caused by armed aggression.

The argument about the inadmissibility of direct claims of injured individuals and legal entities against the aggressor state for the recovery of damages and confiscation of the aggressor state's property for the purposes of compensation for