

บทความวิชาการ (Academic Article)

ข้อวิจารณ์ด้านสิทธิมนุษยชนในเรื่องเสรีภาพในการพูด และเสรีภาพในการแสดงออกต่อร่างอนุสัญญาสหประชาชาติ ว่าด้วยการต่อต้านอาชญากรรมไซเบอร์

Human Right Criticism about Freedom of Speech and
Freedom of Expression on the draft United Nations Convention
Against Cybercrime

โชคชัย เนตรงามสว่าง*

อัยการประจำสำนักงานอัยการสูงสุด สำนักงานอัยการสูงสุด

Chokchai Netngamsawang

Public Prosecutor attached to the Office of the Attorney General

สุรวิช อคินธนโชติ**

นักวิชาการอิสระ

Surawit Akinthanachot

Independent Scholar

วันที่รับบทความ 16 ตุลาคม 2567; วันที่แก้ไขบทความ 12 พฤศจิกายน 2567; วันที่ตอบรับบทความ 17 พฤศจิกายน 2567

* นิติศาสตรบัณฑิต (เกียรตินิยมอันดับสอง) มหาวิทยาลัยธรรมศาสตร์; เนติบัณฑิตไทย สำนัก
อบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา; นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์; อีเมลติดต่อ
chokchai.ne@gmail.com

** Bachelor of Arts, International Liberal Studies (Concentration in Economics),
Waseda University; นิติศาสตรบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย; อีเมลติดต่อ surawit@asagi.waseda.jp

บทคัดย่อ

อาชญากรรมไซเบอร์เป็นภัยคุกคามต่อความมั่นคงของชาติและภูมิภาค อาชญากรรมไซเบอร์มีหลากหลายประเภทและภัยทางไซเบอร์เพิ่มขึ้นอย่างรวดเร็วตามการพัฒนาของเทคโนโลยี ซึ่งประเทศต่าง ๆ เคยได้ร่วมกันแก้ไขปัญหาดังกล่าว โดยเฉพาะสหภาพยุโรปได้มีการตกลงทำอนุสัญญาว่าด้วยอาชญากรรมไซเบอร์ อย่างไรก็ตาม อาชญากรรมไซเบอร์ยังเป็นปัญหาที่ทุกประเทศต่างเผชิญอยู่ในปัจจุบัน องค์การสหประชาชาติจึงมีแนวคิดในการทำกรอบความร่วมมือระหว่างประเทศเพื่อแก้ไขปัญหาดังกล่าว โดยมีการแต่งตั้งคณะกรรมการเฉพาะกิจเพื่อเจรจาอนุสัญญาเพื่อต่อต้านการใช้เทคโนโลยีสารสนเทศและการสื่อสารเพื่อวัตถุประสงค์ในการกระทำความผิดทางอาญา อย่างไรก็ตาม ประเด็นเรื่องสิทธิมนุษยชนในร่างอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมไซเบอร์ยังเป็นข้อที่ประชาคมโลกกังวล โดยเฉพาะที่เกี่ยวข้องกับเสรีภาพในการพูดหรือการแสดงออก โดยมีประเด็นปัญหาต่อร่างอนุสัญญากล่าวคือ ปัญหาเรื่องคำจำกัดความ ขอบเขต การยกเว้นการกระทำผิดของเด็ก การค้นและยึดข้อมูลที่เก็บไว้ และเงื่อนไขและการคุ้มครองกันสำหรับความร่วมมือระหว่างประเทศและความช่วยเหลือทางกฎหมาย ซึ่งสำนักงานข้าหลวงใหญ่เพื่อสิทธิมนุษยชนแห่งสหประชาชาติและองค์กรไม่แสวงหากำไรอื่น ๆ แนะนำให้มีการอ้างอิงอย่างชัดเจนถึงสนธิสัญญาสิทธิมนุษยชนที่เกี่ยวข้อง การมีข้อกำหนดการปกป้องหลักสิทธิมนุษยชน มีขอบเขตที่ชัดเจนและเป็นไปอย่างแคบของความผิดทางอาญาภายใต้อนุสัญญาว่าด้วยอาชญากรรมทางไซเบอร์ มีการยกเว้นการกระทำผิดของเด็ก และบทบัญญัติที่ชัดเจนเพื่อหลีกเลี่ยงการใช้มาตรการในทางที่มีขอบ

คำสำคัญ: อาชญากรรมไซเบอร์; สิทธิมนุษยชน; เสรีภาพในการพูด; เสรีภาพในการแสดงออก; ร่างอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมไซเบอร์

Abstract

Cybercrime is a threat to national and regional security. There are many types of cybercrime, and cyber threats are increasing rapidly with the development of technology. Many countries have worked together to solve the problem, especially the European Union, which has agreed to the Convention on Cybercrime. However, cybercrime is still a problem that all countries are currently facing. Therefore, the United Nations (UN) has proposed creating a framework for international cooperation to solve this issue by appointing the UN Ad Hoc Committee Negotiating a Treaty on Countering the Use of Information and Communications Technologies for Criminal Purposes: AHC. However, the human rights issue in the draft United Nations Convention against Cybercrime still concerns the international community, especially regarding freedom of speech or expression. There are problems with the draft convention, namely the problem of definition, scope, exemption from child offenses, search and seizure of stored data, and conditions and protections for international cooperation and legal assistance. The Office of the High Commissioner for Human Rights (OHCHR) and other NGOs recommend explicit references to relevant human rights treaties, provisions protecting human rights principles, a clear and narrow scope of criminal offenses under the Cybercrime Convention, an exception to child offenses, and clear provisions to avoid abusive measures.

Keywords: Cybercrime; Human Rights; Freedom of Speech; Freedom of Expression; Draft United Nations Convention against Cybercrime

1. ปัญหาอาชญากรรมไซเบอร์

เทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communications Technologies: ICT) ทำให้การเข้าถึงอินเทอร์เน็ตและโซเชียลมีเดียเพิ่มขึ้นอย่างรวดเร็ว ซึ่งส่งผลต่อระบบเศรษฐกิจ สังคม และการเมือง แม้ว่าเทคโนโลยีสารสนเทศและการสื่อสารจะมีประโยชน์อย่างมหาศาล¹ แต่ผลกระทบเชิงลบที่อาจเกิดขึ้นก็มีความสำคัญเช่นกัน โดยอาชญากรรมไซเบอร์ (Cybercrime) ถูกมองว่าเป็นภัยคุกคามที่ยิ่งใหญ่ที่สุดต่อความมั่นคงของชาติและภูมิภาค ความเจริญรุ่งเรืองทางเศรษฐกิจ และความปลอดภัยสาธารณะ² อาชญากรรมไซเบอร์ที่ปรากฏ เช่น สปแอม (Spam), การเจาะระบบ (Hacking), ไวรัส (Virus), สื่อกาฝาก, การขโมยตัวตน (Identity Theft), การขโมยข้อมูล, แรนซัมแวร์ (Ransomware), การโจมตีแบบปฏิเสธการให้บริการแบบวงกว้าง (DDoS), การแทรกแซงอีเมลธุรกิจ (Business E-Mail Compromise), การปลอมแปลงอีเมล (Email Spoofing), การฉ้อโกงการธนาคาร, การใช้โซเชียลมีเดียในทางที่ผิด (Social Media Abuse), การละเมิดสิทธิในทรัพย์สินทางปัญญา³, การฉ้อโกงบัตรเครดิต, การหลอกลวงทางการเงิน

¹ Michael Minges and Christoph Stork, **Economic and Social Impact of ICT in the Pacific** [Online], 5 October 2024. Source: <https://www.theprif.org/documents/regional/information-communication-technology-ict/economic-and-social-impact-ict-pacific-0>

² Commonwealth Secretariat, **Pacific to Establish Cybercrime Collaborative Platform as Threat Escalates** [Online], 5 October 2024. Source: <https://thecommonwealth.org/news/pacific-establish-cybercrime-collaborative-platform-threat-escalates>

³ ITU, **Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries (ICB4PAC)** [Online], 5 October 2024. Source: <https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/ICB4PAC/Pages/default.aspx>

(Cyber Fraud)⁴, การกลั่นแกล้งทางไซเบอร์ (Cyberbullying), การคุกคามทางไซเบอร์ และการเผยแพร่ข่าวปลอม (Fake News) ซึ่งภัยทางไซเบอร์เพิ่มขึ้นอย่างรวดเร็วตามการพัฒนาของเทคโนโลยี⁵

การที่เทคโนโลยีและบริการการสื่อสารเป็นมาตรฐานสากลและช่วยการเข้าถึงบริการอินเทอร์เน็ตจากทุกที่ทั่วโลกทำให้อาชญากรรมไซเบอร์ไม่มีพรมแดนทางกายภาพ ซึ่งประเทศกำลังพัฒนาที่มีพื้นฐานทางกฎหมายและทางเทคนิคไม่เพียงพอจะเสี่ยงต่อการถูกโจมตีทางไซเบอร์มากกว่า⁶ การมีมาตรการป้องกันที่เพียงพอและมีประสิทธิภาพในลักษณะเป็นกฎหมายภายในจึงเป็นสิ่งที่ทุกประเทศต้องมี โดยทุกประเทศควรตรากฎหมายเกี่ยวกับอาชญากรรมทางไซเบอร์ที่ครอบคลุมซึ่งสามารถบังคับใช้เพื่อกำจัดแหล่งหลบภัยสำหรับอาชญากร⁷

⁴ Natadola Jyoti Pratibha, **How Cyber Criminals Defraud Fijians** [Online], 5 October 2024. Source: <https://fijisun.com.fj/2018/12/08/how-cyber-criminals-defraud-fijians/>

⁵ Commonwealth Secretariat, **Report of the Commonwealth Working Group of Experts on Cybercrime (Meeting of Commonwealth Law Ministers and Senior Officials)** [Online], 5 October 2024. Source: <https://www.combatingcybercrime.org/files/virtual-library/international-cooperation/report-of-the-commonwealth-working-group-of-experts-on-cybercrime.pdf>, p. 16.

⁶ Telecommunication Development Sector ITU, **Understanding Cybercrime: Phenomena, Challenges and Legal Response** [Online], 5 October 2024. Source: <https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf>, p. 4-5.

⁷ Chat Le Nguyen and Wilfred Golman, **Diffusion of the Budapest Convention on Cybercrime and the Development of Cybercrime Legislation in Pacific Island Countries: 'Law on the Books' vs 'Law in Action'**, Computer Law & Security Review, Volume 40 (April 2021), p. 2.

ในอดีต เมื่อปี พ.ศ. 2544 (ค.ศ. 2001) หรือ 20 กว่าปีมาแล้ว ประเทศต่าง ๆ ได้ร่วมกันแก้ไขปัญหอาชญากรรมไซเบอร์ โดยได้มีการตกลงทำอนุสัญญาว่าด้วยอาชญากรรมไซเบอร์ (Convention on Cybercrime) ซึ่งถูกลงมติยอมรับโดยสภายุโรป (Council of Europe) หรือที่รู้จักกันในชื่ออนุสัญญาบูดาเปสต์ว่าด้วยอาชญากรรมไซเบอร์ (Budapest Convention on Cybercrime) ซึ่งเป็นการมุ่งเน้นจัดการกับปัญหาอาชญากรรมทางอินเทอร์เน็ตและคอมพิวเตอร์ โดยใช้กระบวนการทางอาญาเพื่อช่วยในการจับกุม สืบสวนสอบสวน และดำเนินคดี กับการกระทำที่เกี่ยวข้องกับระบบ เครือข่าย และข้อมูลคอมพิวเตอร์ รวมทั้งมีประเด็นของเรื่องการแสวงหาประโยชน์ทางเพศจากเด็กออนไลน์ อนุสัญญาดังกล่าวได้เผยแพร่ไปทั่วโลก และทำหน้าที่เป็นมาตรฐานหรือกฎหมายตัวอย่าง (Model Law) สำหรับการร่างกฎหมายอาชญากรรมไซเบอร์ระดับชาติในหลายประเทศทั่วโลก⁸ แม้ว่าประเทศไทยไม่ได้เป็นภาคีของอนุสัญญานี้ แต่หลักการหลายอย่างได้ถูกนำมาช่วยในการใช้การตีความและมีส่วนในการประกอบเป็นพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของไทย⁹

ปัญหาอาชญากรรมไซเบอร์เมื่อพิจารณาจากลักษณะของการกระทำความผิดแล้ว¹⁰ สามารถแบ่งออกเป็น 2 ลักษณะ คือ 1) อาชญากรรมไซเบอร์หลัก หรือที่เกี่ยวข้องกับไซเบอร์ (Core or Cyber-dependent crimes) เป็นความผิดที่ระบบคอมพิวเตอร์เป็นวัตถุที่ถูกกระทำหรือเป็นเครื่องมือโดยตรง อันหมายถึงอาชญากรรมที่ไม่สามารถดำรงอยู่ได้หากไม่มีระบบ ICT เช่น การเจาะระบบ (Hacking), การดักเก็บข้อมูลที่ผิดกฎหมาย (Illegal Interception), การทำลาย การลบ การทำให้เสื่อมสภาพ การเปลี่ยนแปลงหรือการระงับข้อมูลอิเล็กทรอนิกส์ หรือการขัดขวางการทำงานของระบบ และ 2) อาชญากรรมไซเบอร์ที่เกิดขึ้นจากการใช้ไซเบอร์ขยายขอบเขตออกไป (Cyber-Enabled crimes) เป็น

⁸ Ibid.

⁹ ilaw, **เปิดนิยาม-แยกองค์ประกอบ “ความผิดฐานนำเข้าสู่ข้อมูลเท็จ” ตาม พ.ร.บ. คอมพิวเตอร์ฯ** [ออนไลน์], 5 ตุลาคม 2567. แหล่งที่มา: <https://www.ilaw.or.th/articles/4748>

¹⁰ European Parliament, **Understanding Cybercrime** [Online], 5 October 2024. Source: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI\(2024\)760356_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf), p. 2.

อาชญากรรมแบบดั้งเดิมที่ใช้ประโยชน์จากเทคโนโลยี เช่น การเข้าถึง ความรวดเร็ว และการไม่เปิดเผยตัวตนของระบบอินเทอร์เน็ตและแพลตฟอร์มดิจิทัลไปเพิ่มผลกระทบอาชญากรรมไซเบอร์ประเภทนี้ เช่น การโจรกรรมหรือการฉ้อโกงที่เกี่ยวข้องกับ ICT และการชักชวนหรือล่อลวงให้เกิดการล่วงละเมิดทางเพศเด็ก ซึ่งจะเห็นได้ว่าปัญหาอาชญากรรมไซเบอร์ยังคงมีอยู่ในปัจจุบันและทวีความรุนแรงมากขึ้นเพราะการใช้เทคโนโลยีทำให้การกระทำความผิดใหญ่ขึ้น เร็วขึ้น และขยายไปยังความผิดหลายแขนง เช่น ก่อการร้าย ยาเสพติด นอกจากนี้ยังมีปัญหาที่เกี่ยวกับความร่วมมือกันระหว่างประเทศในการป้องกันและปราบปรามอาชญากรรมทางไซเบอร์ ดังนั้น องค์การสหประชาชาติ (United Nations: UN) จึงได้มีความพยายามในการร่างอนุสัญญาว่าด้วยการต่อต้านอาชญากรรมไซเบอร์ (Convention against Cybercrime) ขึ้นมา

บทความนี้มีวัตถุประสงค์หลักเพื่อทำความเข้าใจเบื้องต้นเกี่ยวกับปัญหาอาชญากรรมไซเบอร์ อันนำมาสู่ความร่วมมือระหว่างประเทศในการร่างอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมไซเบอร์ และนำเสนอประเด็นข้อกังวลในเรื่องสิทธิมนุษยชน โดยเฉพาะที่เกี่ยวข้องกับเสรีภาพในการพูดหรือการแสดงออก โดยแบ่งการนำเสนอเนื้อหาออกเป็น 5 หัวข้อ ได้แก่ 1. ปัญหาอาชญากรรมไซเบอร์, 2. ความเป็นมาของร่างอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมไซเบอร์, 3. หลักการสิทธิมนุษยชนและปัญหาที่เกิดขึ้น โดยเฉพาะที่เกี่ยวข้องกับเสรีภาพในการพูดหรือการแสดงออก, 4. ข้อกังวลในประเด็นสิทธิมนุษยชนที่เกี่ยวข้องกับเสรีภาพในการพูดหรือการแสดงออก ในร่างอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมไซเบอร์ และ 5. บทสรุปและข้อเสนอแนะ

2. ความเป็นมาของร่างอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมไซเบอร์

ปัญหาอาชญากรรมไซเบอร์เป็นปัญหาที่ทุกประเทศต่างเผชิญอยู่ในปัจจุบัน และเนื่องจากอาชญากรรมประเภทนี้เป็นอาชญากรรมไร้พรมแดน¹¹ ทำให้ปัญหาที่เกิดขึ้น

¹¹ Telecommunication Development Sector ITU, **Understanding Cybercrime: Phenomena, Challenges and Legal Response** [Online], 5 October 2024. Source:

เกี่ยวกับการดำเนินการหาตัวผู้กระทำความผิด การนำผู้กระทำความผิดมาลงโทษ และปัญหาเกี่ยวกับพยานหลักฐาน ต้องอาศัยการประสานความร่วมมือระหว่างประเทศในการดำเนินการต่างๆ แต่ด้วยกฎหมายภายในของแต่ละประเทศในเรื่องกระบวนการทางอาญาเกี่ยวกับอาชญากรรมไซเบอร์ยังมีความแตกต่างกัน ทำให้การดำเนินการในทางระหว่างประเทศเกิดปัญหาจำนวนมาก ด้วยเหตุนี้ UN จึงมีแนวคิดในการทำกรอบความร่วมมือระหว่างประเทศเพื่อแก้ไขปัญหาดังกล่าว โดยมีการแต่งตั้งคณะกรรมการเฉพาะกิจเพื่อเจรจาอนุสัญญาเพื่อต่อต้านการใช้เทคโนโลยีสารสนเทศและการสื่อสารเพื่อวัตถุประสงค์ในการกระทำความผิดทางอาญา (UN Ad Hoc Committee Negotiating a Treaty on Countering the Use of Information and Communications Technologies for Criminal Purposes: AHC) ซึ่งเป็นคณะกรรมการผู้เชี่ยวชาญระหว่างรัฐบาลที่เป็นตัวแทนของทุกภูมิภาค¹²

ในการแต่งตั้ง AHC สมัชชาใหญ่รับทราบว่าการใช้เทคโนโลยีสารสนเทศและการสื่อสารมีศักยภาพมหาศาลสำหรับการพัฒนาประเทศ แต่ในขณะเดียวกันก็สร้างโอกาสใหม่ ๆ ให้กับผู้กระทำความผิด และอาจส่งผลให้ปริมาณและความซับซ้อนของอาชญากรรมเพิ่มขึ้นที่ประชุมจึงรับทราบความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีใหม่ ๆ ในทางที่ผิด รวมทั้งปัญญาประดิษฐ์ (Artificial Intelligence: AI) พร้อมทั้งรับทราบถึงความจำเป็นในการป้องกันและปราบปรามการใช้เทคโนโลยีสารสนเทศและการสื่อสารเพื่อวัตถุประสงค์ทางอาญา นอกจากนี้ ที่ประชุมยังรับทราบถึงความกังวลในอัตราและความหลากหลายของอาชญากรรมที่เกิดขึ้นในโลกดิจิทัลที่เพิ่มขึ้น และผลกระทบต่อเสถียรภาพของโครงสร้างพื้นฐานที่สำคัญของรัฐและองค์กร ตลอดจนต่อความเป็นอยู่ที่ดีของบุคคลทุกคน ซึ่งที่ประชุมรับทราบว่ามีความเสี่ยงหลายประเภท เช่น ผู้กระทำความผิดเรื่องการค้ำมนุษย์กำลังใช้ประโยชน์จากเทคโนโลยีสารสนเทศและการสื่อสารเพื่อกระทำความผิดในทางอาญา โดยที่ประชุมเน้นย้ำถึงความจำเป็นในการเพิ่มการประสานงานและความร่วมมือระหว่างรัฐ

<https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf>, p. 4-5.

¹² United Nations, **A/RES/74/247, Countering the Use of Information and Communications Technologies for Criminal Purposes** [Online], 5 October 2024. Source: <https://documents.un.org/doc/undoc/gen/n19/440/28/pdf/n1944028.pdf>

ในการปราบปรามการใช้เทคโนโลยีสารสนเทศและการสื่อสารเพื่อวัตถุประสงค์ทางอาญารวมถึงการให้ความช่วยเหลือทางเทคนิคแก่ประเทศกำลังพัฒนาตามคำร้องขอเพื่อปรับปรุงกฎหมายและกรอบการทำงานระดับชาติ และสร้างศักยภาพของหน่วยงานระดับชาติในการจัดการกับการใช้เทคโนโลยีดังกล่าวในทุกรูปแบบ รวมถึงการป้องกันการตรวจจับ การสืบสวน และการดำเนินคดี โดยเน้นย้ำบทบาทของ UN โดยเฉพาะคณะกรรมการว่าด้วยการป้องกันอาชญากรรมและความยุติธรรมทางอาญา และการทำงานของสำนักงานว่าด้วยยาเสพติดและอาชญากรรมแห่งสหประชาชาติ (United Nations Office on Drugs and Crime: UNODC) ในการปฏิบัติหน้าที่เพื่อให้ความช่วยเหลือทางเทคนิคและสร้างศักยภาพด้านอาชญากรรมทางไซเบอร์¹³

ในปัจจุบันร่างอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมไซเบอร์ภายหลังจากที่ผ่านการพิจารณาถึง 3 ปี ได้รับการผ่านร่างเนื้อหาโดย AHC และจะนำเข้าสู่การพิจารณาของที่ประชุมสมัชชาสหประชาชาติ (General Assembly)¹⁴ ต่อไป อย่างไรก็ตามประเด็นเรื่องสิทธิมนุษยชนในร่างอนุสัญญาดังกล่าวยังเป็นเรื่องที่มีความท้าทายและยังมีความกังวลจำนวนมากซึ่งผู้เขียนจะได้กล่าวถึงต่อไป

3. หลักการสิทธิมนุษยชนและปัญหาที่เกิดขึ้น โดยเฉพาะที่เกี่ยวข้องกับเสรีภาพในการพูดหรือการแสดงออก

สิทธิมนุษยชนเป็นสิทธิขั้นพื้นฐานของมนุษย์ทุกคน โดยสิทธิมนุษยชนได้ทวีความสำคัญยิ่งขึ้น เมื่อ UN ได้ยกระดับประเด็นเรื่องสิทธิมนุษยชน ให้เป็นหนึ่งในสามเสาหลักร่วมกับประเด็นความมั่นคงและประเด็นการพัฒนา และให้ผนวกมิติสิทธิมนุษยชนเข้าไว้ใน การดำเนินงานของ UN ในทุกด้าน และได้มีการพัฒนากลไกเพื่อส่งเสริมและคุ้มครองสิทธิมนุษยชนทั่วโลกโดยการยกระดับคณะกรรมการสิทธิมนุษยชน

¹³ Ibid., p. 3.

¹⁴ Reka Furtos, Press Release United Nations: Member States Finalize a New Cybercrime Convention New York, 9 August 2024 [Online], 5 October 2024. Source: https://www.unodc.org/unodc/frontpage/2024/August/united-nations_-member-states-finalize-a-new-cybercrime-convention.html

แห่งสหประชาชาติ (Commission on Human Rights: CHR) ขึ้นเป็นคณะมนตรีสิทธิมนุษยชน (United Nations Human Rights Council: HRC) ซึ่งมีสถานะเท่าเทียมกับคณะมนตรีความมั่นคง และคณะมนตรีเศรษฐกิจและสังคมของสหประชาชาติ¹⁵ และมีหน่วยงานที่ดูแลประเด็นเรื่องสิทธิมนุษยชน เช่น สำนักงานข้าหลวงใหญ่เพื่อสิทธิมนุษยชนแห่งสหประชาชาติ (The Office of the High Commissioner for Human Rights: OHCHR) และสำนักงานข้าหลวงใหญ่ผู้ลี้ภัยแห่งสหประชาชาติ (United Nations High Commissioner for Refugees: UNHCR)

หลักการสิทธิมนุษยชนมีประเด็นที่หลากหลาย เช่น สิทธิทางเศรษฐกิจ สังคมและวัฒนธรรม สิทธิพลเมืองและสิทธิทางการเมือง โดยสิทธิมนุษยชนในเรื่องที่มีความเกี่ยวข้องกับร่างอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมไซเบอร์ และเป็นประเด็นหนึ่งที่ทั่วโลกให้ความสำคัญคือเรื่องที่เกี่ยวข้องกับเสรีภาพในการพูด (Freedom of Speech) หรือเสรีภาพในการแสดงออก (Freedom of Expression) ซึ่งตราสารระหว่างประเทศเรื่องสิทธิมนุษยชนที่เกี่ยวข้องกับเสรีภาพในการพูดหรือเสรีภาพในการแสดงออก ปรากฏอยู่ในปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights: UDHR) อนุสัญญาว่าด้วยสิทธิเด็ก (Convention on the Rights of the Child: CRC) และกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (International Covenant on Civil and Political Rights: ICCPR)

เสรีภาพในการพูดและการแสดงออกได้รับการยอมรับเป็นสิทธิมนุษยชนภายใต้ข้อ 19¹⁶ ของ UDHR

¹⁵ กระทรวงการต่างประเทศ, คณะมนตรีสิทธิมนุษยชน แห่งสหประชาชาติ คำมั่นด้านสิทธิมนุษยชนของไทย และกระบวนการ UPR ฉบับประชาชน [ออนไลน์], 5 ตุลาคม 2567. แหล่งที่มา: <https://humanrights.mfa.go.th/upload/pdf/hrcth.pdf>, หน้า 10.

¹⁶ Universal Declaration of Human Rights “Article 19

Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.”

“ทุกคนมีสิทธิในอิสรภาพแห่งความเห็นและการแสดงออก ทั้งนี้สิทธินี้รวมถึงอิสรภาพที่จะถือเอาความเห็นโดยปราศจากการแทรกแซง และที่จะแสวงหา รับและส่งข้อมูลข่าวสาร และข้อคิดผ่านสื่อใด และโดยไม่คำนึงถึงพรมแดน”¹⁷

และได้รับการยอมรับใน ICCPR ข้อ 19¹⁸ ซึ่งบัญญัติว่า

“1. บุคคลทุกคนมีสิทธิที่จะมีความคิดเห็นโดยปราศจากการแทรกแซง

2. บุคคลทุกคนมีสิทธิในเสรีภาพแห่งการแสดงออก สิทธินี้รวมถึงเสรีภาพที่จะแสวงหา รับและเผยแพร่ข้อมูล ข่าวสารและความคิดทุกประเภท โดยไม่คำนึงถึงพรมแดน ทั้งนี้ไม่ว่าด้วยวาจา เป็นลายลักษณ์อักษร หรือการตีพิมพ์ในรูปแบบของศิลปะ หรือโดยอาศัยสื่อประการอื่นตามที่ตนเลือก

3. การใช้สิทธิตามที่บัญญัติในวรรคสองของข้อนี้ต้องมีหน้าที่และความรับผิดชอบพิเศษควบคู่ไปด้วย การใช้สิทธิดังกล่าวอาจมีข้อจำกัดในบางเรื่องแต่ทั้งนี้ข้อจำกัดนั้นต้องบัญญัติไว้ในกฎหมายและจำเป็นต่อ

(ก) การเคารพในสิทธิหรือชื่อเสียงของบุคคลอื่น

¹⁷ กระทรวงการต่างประเทศ, **ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights)** [ออนไลน์], 5 ตุลาคม 2567. แหล่งที่มา: <https://humanrights.mfa.go.th/upload/pdf/udhr-th-en.pdf>

¹⁸ International Covenant on Civil and Political Rights “Article 19

1. Everyone shall have the right to hold opinions without interference.

2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

(a) For respect of the rights or reputations of others;

(b) For the protection of national security or of public order (ordre public), or of public health or morals.”

(ข) การรักษาความมั่นคงของชาติ หรือความสงบเรียบร้อย หรือการสาธารณสุข หรือศีลธรรมของประชาชน”¹⁹

นอกจากนั้นเสรีภาพในการพูดหรือการแสดงออกสำหรับเด็กยังได้รับการยอมรับโดยเฉพาะด้วยปรากฏอยู่ใน CRC ข้อ 13

“1. เด็กจะมีสิทธิที่จะมีเสรีภาพในการแสดงออก สิทธินี้จะรวมถึงเสรีภาพที่จะแสวงหา ได้รับ หรือถ่ายทอดข้อมูลข่าวสาร และความคิดทุกลักษณะ โดยไม่ถูกจำกัดโดยเขตแดน ไม่ว่าจะโดยวาจา ลายลักษณ์อักษร หรือการตีพิมพ์ในรูปแบบของศิลปะหรือผ่านสื่ออื่นใดตามที่เด็กเลือก

2. การใช้สิทธิดังกล่าวนี้อาจอยู่ภายใต้ข้อจำกัดบางประการ แต่ข้อจำกัดเหล่านี้ต้องเป็นข้อจำกัดเช่นที่บัญญัติตามกฎหมาย และเช่นที่จำเป็นเท่านั้น

(ก) เพื่อการเคารพต่อสิทธิและชื่อเสียงของบุคคลอื่น หรือ

(ข) เพื่อการรักษาความมั่นคงแห่งชาติ หรือความสงบเรียบร้อย หรือสาธารณสุข หรือศีลธรรมของประชาชน”²⁰

¹⁹ กระทรวงการต่างประเทศ, **กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (International Covenant on Civil and Political Rights: ICCPR)** [ออนไลน์], 5 ตุลาคม 2567. แหล่งที่มา: <https://humanrights.mfa.go.th/th/humanrights/obligation/international-human-rights-mechanism/ICCPR.php>

²⁰ United Nations, Convention on the Rights of the Child [Online], 5 October 2024. Source: <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child>, “Article 13

1. The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice.

2. The exercise of this right may be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

(a) For respect of the rights or reputations of others; or

อย่างไรก็ตาม เสรีภาพในการพูดหรือการแสดงออกเกิดปัญหาขึ้นอยู่บ่อยครั้ง โดยเฉพาะในประเทศกำลังพัฒนา เช่น การละเมิดสิทธิส่วนบุคคลโดยพลการหรือมิชอบด้วยกฎหมาย การจำกัดเสรีภาพในการแสดงความคิดเห็นและสื่ออย่างเคร่งครัด การจับกุมและดำเนินคดีกับผู้วิจารณ์รัฐบาล การตรวจสอบเนื้อหา ก่อนเผยแพร่ การจำกัดเสรีภาพทางอินเทอร์เน็ตอย่างเคร่งครัด และการจำกัดการมีส่วนร่วมทางการเมือง²¹ ปัจจุบันการแสดงความคิดเห็นทางการเมืองจากหนังสือพิมพ์ และโทรทัศน์ได้ถูกปิดกั้นมากขึ้น จึงทำให้ประชาชนใช้ช่องทางอินเทอร์เน็ตเป็นช่องทางแสดงความคิดเห็นแทน²² ประชาชนที่แสดงออกอย่างสงบอาจตกเป็นเป้าหมายเพื่อปิดปาก โดยอาจถูกตั้งข้อหา ลอบทำร้าย ทรมาณ หรืออุ้มหาย ซึ่งเป็นแนวโน้มที่รัฐบาลต่าง ๆ ในทวีปเอเชียใช้เพื่อจำกัดการแสดงออก ซึ่งข้อหาส่วนใหญ่เป็นข้อหาด้านความมั่นคงแห่งชาติ และข้อหาอื่น ๆ เช่น การยุยงปลุกปั่นทำให้เกิดความแตกแยกเป็นอาชญากรรมคอมพิวเตอร์ หรือเป็นการหมิ่นประมาทต่อบุคคลหรือสถาบันสำคัญของประเทศ จะเห็นได้ว่าแม้เสรีภาพในการพูดหรือการแสดงออก เป็นสิทธิในระดับสากลที่ได้รับการรับรองตามกฎหมายระหว่างประเทศซึ่งรัฐบาลมีหน้าที่ต้องคุ้มครอง แต่เมื่อพิจารณาในทางปฏิบัติแล้วกลับไม่เป็นเช่นนั้น²³ ทำให้ประชาคมระหว่างประเทศมีความกังวลเกี่ยวกับประเด็นสิทธิมนุษยชนโดยเฉพาะเสรีภาพในการพูดหรือการแสดงออก อันนำไปสู่ประเด็นข้อกังวลที่เกิดขึ้นต่อร่างอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมไซเบอร์

(b) For the protection of national security or of public order (ordre public), or of public health or morals.”

²¹ สถานทูตสหรัฐฯ และสถานกงสุลในประเทศไทย, รายงานด้านสิทธิมนุษยชนประจำปี พ.ศ. 2565 ประเทศไทย [ออนไลน์], 5 ตุลาคม 2567. แหล่งที่มา: <https://th.usembassy.gov/th/our-relationship-th/official-reports-th/2022-human-rights-reports-thailand-th/>

²² สิงหนาท พงศ์ภิญโญศักดิ์, ปัญหาทางกฎหมายเกี่ยวกับการนำข้อมูลบิดเบือนเข้าสู่ระบบคอมพิวเตอร์ : ศึกษากรณีการเผยแพร่ข้อมูลทางการเมือง [ออนไลน์], 5 ตุลาคม 2567. แหล่งที่มา: <http://law.master.kbu.ac.th/StudentTheses/2562/05.pdf>, หน้า 2.

²³ แอมเนสตี้, เสรีภาพในการแสดงออก [ออนไลน์], 5 ตุลาคม 2567. แหล่งที่มา: <https://www.amnesty.or.th/our-work/freedom-expression/>

4. ข้อกังวลในประเด็นสิทธิมนุษยชนที่เกี่ยวข้องกับเสรีภาพในการพูดหรือการแสดงออก ในร่างอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมทางไซเบอร์

ในคราวการแต่งตั้ง AHC ที่ประชุมเองได้เน้นย้ำถึงความสำคัญของการเคารพสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานในการใช้เทคโนโลยีสารสนเทศและการสื่อสาร²⁴ นอกจากนี้ ตลอดการเจรจาที่ผ่านมา กลุ่มประชาสังคมและผู้มีส่วนได้ส่วนเสียอื่น ๆ เน้นย้ำอย่างสม่ำเสมอว่าการต่อสู้กับอาชญากรรมทางไซเบอร์ไม่ควรแลกมาด้วยสิทธิมนุษยชน ความเท่าเทียมทางเพศ และศักดิ์ศรีความเป็นมนุษย์ที่จะได้รับผลกระทบจากร่างอนุสัญญานี้ ทั้งไม่ควรส่งผลให้การวิจัยด้านความปลอดภัยหยุดชะงักและส่งผลทำให้ความปลอดภัยของทุกคนน้อยลง การคุ้มกันและข้อจำกัดต่าง ๆ ที่เข้มงวดและสำคัญจึงจำเป็นต้องกำหนดไว้เพื่อหลีกเลี่ยงการใช้บทบัญญัติของอนุสัญญานี้โดยไม่ชอบโดยใช่ข้ออ้างเรื่องการต่อสู้กับอาชญากรรมทางไซเบอร์²⁵

แม้ในปัจจุบันร่างอนุสัญญาจะผ่านร่างเนื้อหาโดย AHC และนำเข้าสู่การพิจารณาของที่ประชุมสมัชชาสหประชาชาติแล้ว แต่ตลอดเวลาที่ผ่านมาและกระบวนการในขั้นตอนต่อ ๆ ไป จนถึงการใช้ร่างอนุสัญญาดังกล่าวไม่ได้ไร้อุปสรรคอุปสรรคหลาย เนื่องจากความเห็นที่แตกต่างกันจำนวนมาก โดยเฉพาะประเด็นในเรื่องสิทธิมนุษยชน ซึ่งร่างอนุสัญญาดังกล่าวยังมีข้อวิพากษ์วิจารณ์ถึงความเหมาะสมในด้านสิทธิมนุษยชนที่เกี่ยวข้องกับคำจำกัดความ เนื้อหาของอนุสัญญา และปัญหาเรื่องข้อมูลส่วนบุคคล โดยในหัวข้อนี้จะกล่าวถึงข้อกังวลต่าง ๆ ที่ประชาคมโลกและหน่วยงาน NGO ได้ให้ข้อคิดเห็นไว้เพื่อประกอบการพิจารณาร่างอนุสัญญานี้

²⁴ United Nations, *A/RES/74/247, Countering the Use of Information and Communications Technologies for Criminal Purposes* [Online], 5 October 2024. Source: <https://documents.un.org/doc/undoc/gen/n19/440/28/pdf/n1944028.pdf>, p. 3.

²⁵ Joint Statement, *Joint Statement on the Proposed Cybercrime Treaty Ahead of the Concluding Session January 23, 2024* [Online], 5 October 2024. Source: <https://cdt.org/wp-content/uploads/2024/01/Joint-Advocacy-Statement-Cybercrime-Convention-Jan-23-2024.pdf>

4.1 ปัญหาเรื่องคำจำกัดความ ขอบเขตแคบและกว้าง

ปัญหาเรื่องชื่อและคำจำกัดความของร่างอนุสัญญาเป็นปัญหาใหญ่เนื่องจากการกำหนดคำจำกัดความจะมีผลถึงขอบเขตของอาชญากรรมไซเบอร์ตามร่างอนุสัญญา OHCHR สนับสนุนให้จำกัดขอบเขตของร่างอนุสัญญาให้แคบลงเฉพาะการทำให้อาชญากรรมที่เกี่ยวข้องกับไซเบอร์บางประเภทเป็นอาชญากรรมเท่านั้น กล่าวโดยเฉพาะคือความผิดที่เชื่อมโยงกับข้อมูลหรือระบบคอมพิวเตอร์เท่านั้น เช่น เจตนาเข้าถึงระบบคอมพิวเตอร์โดยไม่มีสิทธิ การขยายขอบเขตของการกำหนดความผิดทางอาญาให้กว้างขึ้นกว่าอาชญากรรมที่เกี่ยวข้องกับไซเบอร์อาจเป็นปัญหาได้ โดยเฉพาะอย่างยิ่งหากมีการรวมความผิดที่เกี่ยวข้องกับการแสดงเนื้อหาผ่านทางออนไลน์เข้าไปด้วย กฎหมายอาชญากรรมไซเบอร์ที่มีบทบัญญัติดังกล่าวมักใช้เพื่อจำกัดเสรีภาพในการแสดงออกอย่างไม่เหมาะสมปราบปรามความคิดเห็นทางการเมืองที่ไม่เห็นด้วย และมักใช้เป็นอาวุธโจมตีเสียงข้างน้อย ซึ่งกรณีเหล่านี้มีข้อกังวลว่าอาจนำไปสู่การทำให้คำพูดที่ได้รับการคุ้มครองกลายเป็นอาชญากรรมมากเกินไป²⁶ ตัวอย่างของขอบเขตที่กว้างของการกำหนดความรับผิดทางอาญา เช่น การรวม “การก่อการร้าย” ให้เป็นอาชญากรรมไซเบอร์ตามร่างอนุสัญญาเนื่องจากอาชญากรรมดังกล่าวเกิดขึ้นโดยใช้ระบบคอมพิวเตอร์ ไม่ใช่อาชญากรรมที่จะเกิดขึ้นโดยขึ้นอยู่กับระบบคอมพิวเตอร์เท่านั้น โดยร่างอนุสัญญาควรจำกัดเฉพาะอาชญากรรมหลักหรือที่เกี่ยวข้องกับไซเบอร์เท่านั้น²⁷ การกำหนดลักษณะที่กว้างและไม่ชัดเจนของ “การก่อการร้าย” อาจทำให้มีการนำบทบัญญัติของร่างอนุสัญญามาใช้ทำให้

²⁶ Katitza Rodriguez, **The UN Cybercrime Draft Convention Remains Too Flawed to Adopt** [Online], 5 October 2024. Source: <https://www.eff.org/deeplinks/2024/06/un-cybercrime-draft-convention-remains-too-flawed-adopt>

²⁷ EFF, Privacy International and Electronic Frontier Foundations’ **Comments on the Consolidated Negotiating Document of the UN Cybercrime Treaty** [Online], 5 October 2024. Source: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/Multi-stakeholders/PI-EFF_comments_on_consolidated_text_December_2022.pdf, p. 3.

การวิพากษ์วิจารณ์รัฐหรือผู้มีอำนาจโดยชอบธรรมที่สอดคล้องกับเสรีภาพในการแสดงออก กลายเป็นการกระทำที่ผิดกฎหมายโดยใช้ร่างอนุสัญญาว่าด้วยอาชญากรรมทางไซเบอร์ ฉบับนี้เป็นข้ออ้างในการดำเนินคดีทางอาญาได้

จากเหตุผลดังกล่าว OHCHR จึงมีข้อสังเกตด้วยความกังวลถึงชื่อใหม่ของร่าง อนุสัญญาว่า “อนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมทางไซเบอร์ (อาชญากรรมที่กระทำผ่านระบบเทคโนโลยีสารสนเทศและการสื่อสาร)” “United Nations Convention against Cybercrime (Crimes Committed through the Use of an Information and Communications Technology System)” ซึ่งอาจตีความได้ว่าการกระทำผิดทางอาญาใด ๆ ที่ทำผ่านระบบ ICT เป็นอาชญากรรมทางไซเบอร์ แนวทางดังกล่าวอาจสร้างปัญหาโดยเฉพาะอย่างยิ่งเมื่อพิจารณาจากมาตรา 1 ที่กำหนดจุดประสงค์ของร่างอนุสัญญาว่าเป็นการต่อสู้และป้องกัน “อาชญากรรม ไซเบอร์” และเมื่ออ่านร่วมกับชื่อร่างอนุสัญญาแล้ว อาจทำให้มีการตีความจุดประสงค์ในแนวทางที่กว้างขวาง ซึ่งจะขัดแย้งกับความพยายามที่จะจำกัดขอบเขตการกำหนดความผิดทางอาญาภายใต้ร่าง อนุสัญญาเฉพาะความผิดที่ได้กำหนดไว้ชัดเจนและมีขอบเขตอย่างแคบเท่านั้น²⁸

OHCHR ยังกังวลเกี่ยวกับลักษณะที่ไม่จำกัดขอบเขตของมาตรา 4 ที่กำหนดให้รัฐต่าง ๆ ต้องใช้มาตรการเพื่อขยายขอบเขตความครอบคลุมของร่างอนุสัญญาให้ครอบคลุมถึงความผิดภายใต้ตราสารระหว่างประเทศอื่น ๆ ด้วย เมื่อมีการกระทำผ่านระบบคอมพิวเตอร์ ดังนั้น ขอบเขตที่แท้จริงของบทบัญญัตินี้จึงยังไม่ชัดเจน เนื่องจากไม่มีรายการความผิดที่เกี่ยวข้องอย่างครบถ้วนสมบูรณ์ จึงทำให้ไม่สามารถประเมินผลกระทบในอนาคตได้ บทบัญญัตินี้ยังมีความเสี่ยงที่อาจขยายปัญหาที่กล่าวไปแล้วไปยังการใช้สนธิสัญญาอื่น ๆ เช่น คำจำกัดความของการก่อการร้ายที่กว้างเกินไป และบทบัญญัตินี้ยังอาจนำไปสู่การกำหนดความรับผิดที่ไม่ได้สัดส่วนสำหรับผู้ให้บริการ ซึ่งจะคุกคามเสรีภาพในการแสดงออก การลบมาตรา 4 จะช่วยทำให้การใช้ร่างอนุสัญญานี้มีขอบเขตที่แคบลงและชัดเจนขึ้น

²⁸ OHCHR, **Human Rights and the Draft Cybercrime Convention** [Online], 5 October 2024. Source: <https://www.ohchr.org/sites/default/files/documents/issues/civicspace/DRAFT-CYBERCRIME-CONVENTION.pdf>, p. 3.

นอกจากนั้น แผนสำหรับการรับพิธีสารทางเลือกเพิ่มเติมเพื่อครอบคลุมความผิดทางอาญาอื่น ๆ นั้นมีความเสี่ยงอย่างมากต่อการขยายขอบเขตของการกระทำความผิดทางอาญาซึ่งจะไม่เป็นไปตามข้อกำหนดของกฎหมายสิทธิมนุษยชนระหว่างประเทศ รวมถึงหลักความจำเป็นและความได้สัดส่วน²⁹

ปัญหาที่เกี่ยวข้องกับคำจำกัดความนี้ยังมีความเชื่อมโยงกับมาตรา 6 ในเรื่องการเคารพหลักสิทธิมนุษยชน³⁰ อนุสัญญาควรกำหนดให้รัฐต้องปฏิบัติตามพันธกรณีด้านสิทธิมนุษยชน ไม่ใช่เพียงสอดคล้อง (Consistent) เท่านั้น ถ้อยคำที่ไม่เข้มงวดนี้จะทำให้รัฐสามารถตีความได้กว้างและอาจใช้บังคับได้หลวมขึ้น ซึ่งอาจนำไปสู่การคุ้มครองที่ไม่สอดคล้องกันในเขตอำนาจศาลต่าง ๆ เนื่องจากรัฐที่มีประวัติด้านสิทธิมนุษยชนอ่อนแอกว่าอาจตีความคำว่าสอดคล้องในลักษณะที่ตอบสนองภาระผูกพันของตนได้เพียงเล็กน้อยโดยไม่ได้ปกป้องสิทธิของบุคคลอย่างเต็มที่ นอกจากนี้ มาตรานี้ยังไม่ได้กล่าวถึงหลักการพื้นฐานของสิทธิมนุษยชน อาทิ หลักความชอบด้วยกฎหมาย หลักความจำเป็น หลักความได้สัดส่วน และหลักการไม่เลือกปฏิบัติ และข้อจำกัดโดยทั่วไปที่ชัดเจน ในทางปฏิบัติแล้ว

²⁹ Ibid.

³⁰ United Nations, *A/AC.291/L.15, Draft United Nations Convention Against Cybercrime Strengthening International Cooperation for Combating Certain Crimes Committed by means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes* [Online], 5 October 2024. Source: <https://documents.un.org/doc/undoc/gen/v24/055/06/pdf/v2405506.pdf>, “Article 6. Respect for human rights

1. States Parties shall ensure that the implementation of their obligations under this Convention is consistent with their obligations under international human rights law.

2. Nothing in this Convention shall be interpreted as permitting suppression of human rights or fundamental freedoms, including the rights related to the freedoms of expression, conscience, opinion, religion or belief, peaceful assembly and association, in accordance and in a manner consistent with applicable international human rights law.”

องค์ประกอบหลายอย่างของร่างอนุสัญญานี้จึงมีแนวโน้มที่จะได้รับการนำไปปฏิบัติในลักษณะที่ไม่เป็นไปตามมาตรฐานสิทธิมนุษยชนระหว่างประเทศ โดยเฉพาะอย่างยิ่งรัฐที่จะลงนามในร่างอนุสัญญานี้บางรัฐยังปฏิเสธที่จะลงนามและให้สัตยาบันต่อตราสารสิทธิมนุษยชนพื้นฐาน เช่น ICCPR³¹

4.2 การยกเว้นการกระทำผิดของเด็ก

การคุ้มครองเด็กอายุต่ำกว่า 18 ปี³²จากการล่วงละเมิดทางเพศมีความสำคัญอย่างยิ่งและเป็นไปตามกฎหมายสิทธิมนุษยชนระหว่างประเทศ ในขณะเดียวกัน กฎหมายสิทธิมนุษยชนระหว่างประเทศก็คุ้มครองเสรีภาพในการแสดงออกของเด็กด้วย ดังนั้น แม้ว่าการกำหนดให้การกระทำผิดทางเพศเด็กที่เกี่ยวข้องกับไซเบอร์ (cyber-related) เป็นอาชญากรรมจะเป็นสิ่งที่สมเหตุสมผล แต่การกำหนดความผิดดังกล่าวควรทำอย่างถูกต้อง และหลีกเลี่ยงการทำให้การแสดงออกโดยชอบธรรมกลายเป็นอาชญากรรม รวมทั้งการแบ่งปันเนื้อหาที่สร้างขึ้นอย่างอิสระโดยเด็กเอง

OHCHR ระบุว่ามาตรา 14 ที่เกี่ยวข้องกับการล่วงละเมิดทางเพศเด็กทางออนไลน์หรือเนื้อหานั้นยังไม่ถูกต้องเพียงพอ

มาตรา 14 (4) ของร่างปัจจุบันระบุว่า รัฐต่าง ๆ “อาจ (may) ดำเนินการเพื่อยกเว้นการกระทำผิดของเด็กสำหรับเนื้อหาที่สร้างขึ้นเอง” และสำหรับเนื้อหาที่ผลิตขึ้นเป็นส่วนหนึ่งของการมีเพศสัมพันธ์โดยสมัครใจ โดยคำว่า “อาจ” มีลักษณะเป็นทางเลือกซึ่งทำให้ข้อยกเว้นนี้ไม่ชัดเจน และไม่ได้ให้การคุ้มครองสิทธิของเด็กอย่างเพียงพอตามที่

³¹ Katitza Rodriguez, **The UN Cybercrime Draft Convention Remains Too Flawed to Adopt** [Online], 5 October 2024. Source: <https://www.eff.org/deeplinks/2024/06/un-cybercrime-draft-convention-remains-too-flawed-adopt>

³² United Nations, Convention on the Rights of the Child [Online], 5 October 2024. Source: <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child>, “Article 1 For the purposes of the present Convention, a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier.”

กฎหมายระหว่างประเทศกำหนด³³ ดังเช่นที่คณะกรรมการว่าด้วยสิทธิเด็ก (Committee on the Rights of the Child) ได้กล่าวไว้ว่า “สื่อทางเพศที่เด็กสร้างขึ้นเองและครอบครองและ/หรือแบ่งปันด้วยความยินยอมและเพื่อการใช้ส่วนตัวเท่านั้น ไม่ควรถือเป็นสิ่งผิดกฎหมาย”³⁴

OHCHR เสนอข้อความของมาตรา 14 (4)³⁵ ดังนี้

“4. ตามกฎหมายในประเทศและสอดคล้องกับข้อผูกพันระหว่างประเทศที่บังคับใช้ รัฐภาคี**ต้อง (shall)** ดำเนินการเพื่อยกเว้นการดำเนินคดีอาญากับ:

(a) การกระทำของเด็กต่อสื่อที่เด็กสร้างขึ้นเอง หรือ

(b) การผลิต การส่งต่อ หรือการครอบครองโดยได้รับความยินยอมของสื่อที่อธิบายไว้ในวรรคสอง (a) ถึง (c) ของมาตรานี้ โดยที่พฤติกรรมพื้นฐานที่บรรยายไว้เป็นไปตามกฎหมายในประเทศ และสื่อดังกล่าวได้รับการเก็บรักษาไว้เพื่อใช้ส่วนตัวโดยสมัครใจของบุคคลที่เกี่ยวข้องเท่านั้น”

นอกจากนั้น ในร่างดังกล่าวยังไม่มีกำหนดข้อยกเว้นโดยชัดแจ้งสำหรับสื่อศิลปะ การศึกษา และวิทยาศาสตร์ที่เกี่ยวข้องกับคำว่า “สื่อล่วงละเมิดทางเพศเด็ก” ซึ่งทำให้เนื้อหาที่แสดงถึงเด็กเป็นสิ่งผิดกฎหมายในมาตรา 14 (2) อาจครอบคลุมไปถึงการแสดงออกอย่างชอบธรรมในกรณีที่เป็นงานศิลปะ วรรณกรรม และวิทยาศาสตร์ที่

³³ OHCHR, **Human Rights and the Draft Cybercrime Convention** [Online], 5 October 2024. Source: <https://www.ohchr.org/sites/default/files/documents/issues/civicspace/DRAFT-CYBERCRIME-CONVENTION.pdf>, p. 4.

³⁴ United Nations, **CRC/C/GC/25, General Comment No. 25 (2021) on Children’s Rights in Relation to the Digital Environment** [Online], 5 October 2024. Source: <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>, “Self-generated sexual material by children that they possess and/or share with their consent and solely for their own private use should not be criminalized”

³⁵ OHCHR, **Human Rights and the Draft Cybercrime Convention** [Online], 5 October 2024. Source: <https://www.ohchr.org/sites/default/files/documents/issues/civicspace/DRAFT-CYBERCRIME-CONVENTION.pdf>, p. 4, 13.

พรรณนาถึงบุคคลสมมติ ตลอดจนการรายงานข่าวหรือการวิจัยทางประวัติศาสตร์เกี่ยวกับกรณีล่วงละเมิดทางเพศเด็ก ดังนั้น สิ่งที่สำคัญคือการหลีกเลี่ยงไม่ให้ร่างอนุสัญญานี้ถูกใช้เป็นข้ออ้างสำหรับการปิดกั้นสื่อโดยไม่เหมาะสม และเพื่อกำหนดประเภทและขอบเขตของเนื้อหาที่ถือว่าเป็น “สื่อล่วงละเมิดทางเพศเด็ก” OHCHR แนะนำให้มีข้อยกเว้นโดยชัดแจ้งสำหรับสื่อศิลปะ การศึกษา และวิทยาศาสตร์ โดยให้เป็นมาตราใหม่ตามมาตรา 14 (2): สื่อที่มีลักษณะทางศิลปะ การศึกษา หรือวิทยาศาสตร์อย่างชัดเจน และไม่มีบุคคลอายุต่ำกว่า 18 ปี เข้ามาเกี่ยวข้อง จะได้รับการยกเว้นจากมาตรา 14 (1)³⁶

4.3 การค้นและยึดข้อมูลที่เก็บไว้

มาตรา 28 กำหนดเงื่อนไขในการให้อำนาจหน่วยงานที่เกี่ยวข้องในการค้นและเข้าถึงระบบคอมพิวเตอร์และข้อมูลที่เก็บไว้ โดยมาตรา 28 (4) กำหนดให้มีมาตรการที่อนุญาตให้หน่วยงานที่เกี่ยวข้องสั่งให้บุคคลให้ข้อมูลเพื่อให้สามารถทำการค้นและยึดดังกล่าวได้

มาตรการนี้มีความเสี่ยงต่อการที่จะปกป้องสิทธิมนุษยชนได้อย่างมีประสิทธิภาพ โดยเฉพาะสิทธิในความเป็นอยู่ส่วนตัว (Right to Privacy) เช่น บทบัญญัติดังกล่าวอาจอนุญาตให้รัฐบาลบังคับให้บุคคลภายนอกเปิดเผยช่องโหว่หรือจุดบกพร่องของซอฟต์แวร์ กล่าวอีกนัยหนึ่งคือ ช่วยให้รัฐหาวิธีเข้าสู่ระบบคอมพิวเตอร์ได้ ในทำนองเดียวกัน รัฐอาจบังคับให้บุคคลภายนอกช่วยเหลือให้รัฐเข้าถึงการสื่อสารที่เข้ารหัสได้ บุคคลภายนอกดังกล่าวนี้ นอกจากรวมถึงตัวผู้ให้บริการระบบ ICT ที่เป็นปัญหาแล้ว ยังรวมถึงบุคคลใด ๆ เช่น พนักงานของผู้ให้บริการด้วย

มาตรการดังกล่าวอาจเปิดช่องให้มีการติดตามการสื่อสารประเภทต่าง ๆ ได้ ซึ่งนำไปสู่การแทรกแซงเรื่องการรักษาความลับในการสื่อสารอย่างไม่ได้สัดส่วน นอกจากนั้น รัฐยังสามารถเปลี่ยนแปลงเนื้อหาของการสื่อสารได้ ซึ่งถือเป็นการแทรกแซงเสรีภาพในการแสดงออกและสิทธิอื่น ๆ

กฎหมายสิทธิมนุษยชนระหว่างประเทศกำหนดให้รัฐต้องละเว้นจากการแทรกแซงสิทธิความเป็นส่วนตัวโดยไม่เหมาะสม และต้องดำเนินมาตรการเพื่อให้แน่ใจว่าการสื่อสาร

³⁶ Ibid., p. 13.

มีความปลอดภัย ครอบคลุม และมีการรักษาความลับอย่างเพียงพอ เพื่อให้บุคคลได้ใช้สิทธิ ความเป็นส่วนตัว ซึ่งหากหน่วยงานได้รับอนุญาตให้บังคับให้บุคคลภายนอกทำตามทีเสนอไว้ในมาตรา 28 (4) การเข้าถึงดังกล่าวจะสามารถนำไปใช้อย่างกว้างขวางเพื่อวัตถุประสงค์อื่นที่ไม่เกี่ยวข้อง เช่น การเฝ้าติดตามโดยไม่ต้องได้รับอนุญาตจากศาล³⁷ ดังนั้น OHCHR จึงแนะนำให้ตัดมาตรา 28 (4) นี้ออกจากร่างอนุสัญญา³⁸

4.4 เจื่อนไขและการคุ้มครองกันสำหรับความร่วมมือระหว่างประเทศและความช่วยเหลือทางกฎหมาย

ข้อกังวลสำหรับบทบัญญัตินี้มีความสำคัญ กล่าวคือ การต้องทำให้มั่นใจว่า บทบัญญัติเกี่ยวกับความร่วมมือระหว่างประเทศและความช่วยเหลือทางกฎหมายนั้น สอดคล้องกับกฎหมายสิทธิมนุษยชนระหว่างประเทศ และหลักเสียงสถานการณ์ที่รัฐอาจ ถูกขอให้ร่วมมือกับรัฐอื่นในลักษณะที่อาจกระทบต่อพันธกรณีด้านสิทธิมนุษยชน ตัวอย่างเช่น รัฐใช้กฎหมายอาญาเพื่อดำเนินคดีกับฝ่ายตรงข้ามทางการเมืองสำหรับการใช้ สิทธิและเสรีภาพในการแสดงออกโดยชอบธรรม โดยพยายามเข้าถึงข้อมูลอิเล็กทรอนิกส์ที่ จัดเก็บไว้ เช่น อีเมลหรือบัญชี โดยที่ไม่อธิบายให้รัฐที่ถูกร้องขอทราบ ซึ่งบทบัญญัติเกี่ยวกับการแบ่งปันข้อมูลข้ามพรมแดนนี้ไม่จำเป็นต้องได้รับการตรวจสอบจากหน่วยงานอิสระหรือ มีการคุ้มครองอื่น ๆ ดังนั้น หน่วยงานที่บังคับใช้กฎหมายในรัฐที่ถูกร้องขอจึงสามารถส่ง มอบข้อมูลส่วนตัวเกี่ยวกับบุคคลนี้ได้โดยที่คำขอไม่ต้องอยู่ภายใต้การตรวจสอบจาก หน่วยงานอิสระ และรัฐที่ร้องขอไม่จำเป็นต้องแสดงให้เห็นว่าข้อมูลนั้นจำเป็นต่อการ สืบสวนคดีอาญาใดโดยเฉพาะเจาะจง

ดังนั้น จึงมีความจำเป็นอย่างยิ่งที่ร่างอนุสัญญาจะต้องกำหนดเจื่อนไขและการคุ้มครอง ในการดำเนินการเกี่ยวกับความร่วมมือระหว่างประเทศ ซึ่งปรากฏอยู่ในมาตรา 24 (4)³⁹

³⁷ Ibid., p. 7.

³⁸ Ibid., p. 13.

³⁹ United Nations, A/AC.291/L.15, Draft United Nations Convention Against Cybercrime Strengthening International Cooperation for Combating Certain Crimes Committed by means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes [Online],5

ของร่างอนุสัญญานี้ อย่างไรก็ตาม กรอบการทำงานที่จัดทำขึ้นยังขาดความชัดเจนและความเฉพาะเจาะจง ข้อเสนอสำหรับข้อกำหนดการคุ้มกันทั่วไปดังที่ไว้ข้างต้นจะช่วยให้กรอบการทำงานด้านการคุ้มครองสิทธิมนุษยชนมีความเข้มแข็งยิ่งขึ้น⁴⁰

นอกจากนั้น ขั้นตอนก่อนการได้รับอนุญาตจากศาล ความโปร่งใส การแจ้งให้ผู้เสียหาย และสิทธิในการได้รับการเยียวยาที่มีประสิทธิภาพ ยังเป็นองค์ประกอบที่สำคัญหนึ่งของการคุ้มครองสิทธิมนุษยชน ซึ่งแม้มาตรา 24 (2) จะกำหนดเงื่อนไขและการคุ้มกันไว้⁴¹ อย่างไรก็ตาม การให้การคุ้มครองนี้ขึ้นอยู่กับกฎหมายภายในอาจทำให้ประสิทธิภาพของการคุ้มครองลดน้อยลง เนื่องจากกฎหมายในประเทศแตกต่างกันอย่างมากและอาจไม่ให้การคุ้มครองที่เหมาะสม และมาตรา 24 ไม่ได้ระบุหลักการแห่งความถูกต้องตามกฎหมายและ

October 2024. Source: <https://documents.un.org/doc/undoc/gen/v24/055/06/pdf/v2405506.pdf>, “Article 24. Conditions and safeguards

4. The conditions and safeguards established in accordance with this article shall apply at the domestic level to the powers and procedures set forth in this chapter, both for the purpose of domestic criminal investigations and proceedings and for the purpose of rendering international cooperation by the requested State Party.”

⁴⁰ OHCHR, **Human Rights and the Draft Cybercrime Convention** [Online], 5 October 2024. Source: <https://www.ohchr.org/sites/default/files/documents/issues/civicspace/DRAFT-CYBERCRIME-CONVENTION.pdf>, p. 10

⁴¹ United Nations, **A/AC.291/L.15, Draft United Nations Convention Against Cybercrime Strengthening International Cooperation for Combating Certain Crimes Committed by means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes** [Online], 5 October 2024. Source: <https://documents.un.org/doc/undoc/gen/v24/055/06/pdf/v2405506.pdf>, “Article 24. Conditions and safeguards

2. In accordance with and pursuant to the domestic law of each State Party, such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, include, inter alia, judicial or other independent review, the right to an effective remedy, grounds justifying application, and limitation of the scope and the duration of such power or procedure.”

หลักความจำเป็นไว้อย่างชัดเจน การมอบอำนาจที่กว้างขวางแก่รัฐทำให้ร่างอนุสัญญาไม่สามารถรับประกันได้ว่าข้อความดังกล่าวจะถูกนำไปปฏิบัติในลักษณะที่สอดคล้องกับสิทธิมนุษยชน และเสี่ยงที่จะกลายเป็นเครื่องมือสำหรับการละเมิดสิทธิมนุษยชนและการปราบปรามข้ามชาติที่จะกลายเป็นการทำลายความมั่นคงทางไซเบอร์และหลักการที่มุ่งจะคุ้มครองได้⁴²

ขณะที่ปัญหาเรื่องการกำหนดพันธกรณีหรือข้อผูกพันที่อาจจะทำไม่ได้ในทางปฏิบัติซึ่งเคยปรากฏขึ้นในหลายประเทศตอนที่มีการร่วมลงนามในอนุสัญญาบูดาเปสต์⁴³ สำหรับร่างอนุสัญญานี้แคนาดาให้ความเห็นว่าคำขอส่วนใหญ่ที่ได้รับนั้นเป็นคำขอข้อมูลสำหรับอาชญากรรมที่ไม่ระบุขอบเขตชัดเจน และต้องใช้ทรัพยากรในการจัดการกับคำขอเหล่านี้ รวมถึงการอธิบายให้ประเทศภาคีทราบถึงวิธีการปฏิบัติตามเกณฑ์การแบ่งปันข้อมูล หากสนธิสัญญามีขอบเขตกว้าง การนำไปปฏิบัติจริงอาจเป็นเรื่องยากและอาจขัดขวางการใช้ร่างอนุสัญญาได้ ส่วนอิตาลีระบุว่าความร่วมมือสำหรับอาชญากรรมทั้งหมดที่กระทำโดยใช้ ICT จะทำให้เกิดข้อจำกัดด้านงบประมาณ⁴⁴

⁴² Katitza Rodriguez, **The UN Cybercrime Draft Convention Remains Too Flawed to Adopt** [Online], 5 October 2024. Source: <https://www EFF.ORG/deeplinks/2024/06/un-cybercrime-draft-convention-remains-too-flawed-adopt>

⁴³ Chat Le Nguyen and Wilfred Golman, **Diffusion of the Budapest Convention on Cybercrime and the Development of Cybercrime Legislation in Pacific Island Countries: ‘Law on the Books’ vs ‘Law in Action’**, Computer Law & Security Review, Volume 40 (April 2021), p. 12..

⁴⁴ Summer Walker, **Still Poles Apart UN Cybercrime Treaty Negotiation, June 2023** [Online], 5 October 2024. Source: <https://globalinitiative.net/wp-content/uploads/2023/06/Summer-Walker-Poles-apart-UN-cybercrime-treaty-negotiations-GI-TOC-June-2023.pdf>, p. 8.

5. บทสรุปและข้อเสนอแนะ

ปัญหาอาชญากรรมไซเบอร์เป็นปัญหาใหญ่ที่ทั่วโลกต่างให้ความสำคัญ เนื่องจากเป็นปัญหาที่กระทบต่อความมั่นคงและเศรษฐกิจ อาชญากรรมไซเบอร์เพิ่มขึ้นอย่างรวดเร็วตามการพัฒนาของเทคโนโลยีและมีความซับซ้อนทั้งในเชิงเทคนิคและในมุมมองของกฎหมาย ดังนั้น มาตรการทางกฎหมายที่ครอบคลุมเพื่อให้ตามทันความก้าวหน้าของเทคโนโลยีและการพัฒนาไปของอาชญากรรมต่าง ๆ จึงมีความจำเป็นอย่างยิ่ง แม้ในปัจจุบันจะมีอนุสัญญาบูดาเปสต์ว่าด้วยอาชญากรรมไซเบอร์ หรือในประเทศไทยที่มีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แต่การแก้ปัญหาในระดับระหว่างประเทศอย่างแท้จริงยังขาดกฎเกณฑ์ที่ชัดเจน ดังนั้นร่างอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมไซเบอร์ จึงจะเข้ามาช่วยอุดช่องว่างดังกล่าว โดยเฉพาะการประสานความร่วมมือระหว่างประเทศในการดำเนินการต่าง ๆ ทั้งในเชิงป้องกันการกระทำความผิด และการนำตัวผู้กระทำความผิดมาลงโทษ

อย่างไรก็ตาม หลักการสิทธิมนุษยชน ซึ่งเป็นหลักการที่ได้รับการยอมรับร่วมกันของประเทศต่าง ๆ เป็นเรื่องที่ไม่อาจละเลยได้ ไม่ว่าจะเป็นความพยายามในการร่างกฎหมายใด ๆ ซึ่งสหประชาชาติเอง รวมถึงองค์กรไม่แสวงหากำไรต่าง ๆ ที่มีวัตถุประสงค์ในการคุ้มครองสิทธิมนุษยชน ยังมีความเห็นว่า ร่างอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมไซเบอร์ยังมีปัญหาในประเด็นสิทธิมนุษยชน และโดยเฉพาะที่เกี่ยวข้องกับเสรีภาพในการพูดหรือการแสดงออก ซึ่งปัญหาการนำกฎหมายมาใช้เพื่อจำกัดเสรีภาพในการพูดหรือการแสดงออกเกิดขึ้นบ่อยครั้งกับการดำเนินคดีกับผู้ที่วิจารณ์รัฐบาลและการจำกัดการมีส่วนร่วมทางการเมือง ซึ่งเป็นการนำกฎหมายมาใช้เพื่อวัตถุประสงค์ที่ไม่ถูกต้อง ดังนั้น เพื่อป้องกันการนำกฎหมายไปใช้เพื่อวัตถุประสงค์อื่นอันเป็นการกระทบต่อเสรีภาพในการพูดหรือการแสดงออก ร่างอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมไซเบอร์ ควรมีการพิจารณาถึงประเด็นต่าง ๆ ดังต่อไปนี้ คือ 1. ปัญหาเรื่องคำจำกัดความของความผิดว่าควรมีขอบเขตแคบและกว้างอย่างไร 2. ปัญหาเกี่ยวกับการกระทำของเด็กและการยกเว้นการกระทำผิดของเด็กที่จะขัดขวางเสรีภาพในการพูดหรือการแสดงออกของเด็ก 3. ปัญหาการค้นและยึดข้อมูลที่เก็บไว้ ซึ่งจะนำไปสู่การแทรกแซงเสรีภาพในการแสดงออกและสิทธิอื่น ๆ 4. ปัญหาเกี่ยวกับเงื่อนไขและการคุ้มครอง

สำหรับความร่วมมือระหว่างประเทศและความช่วยเหลือทางกฎหมายที่ยังขาดความชัดเจน และความเฉพาะเจาะจง ซึ่งอาจนำไปสู่ปัญหาในทางปฏิบัติ

เมื่อพิจารณาประเด็นด้านสิทธิมนุษยชนที่มีปัญหาแล้ว OHCHR และองค์กรที่ไม่แสวงหากำไรต่าง ๆ ได้มีคำแนะนำเกี่ยวกับการแก้ไขปัญหาต่าง ๆ⁴⁵ เช่น

1) การอ้างอิงอย่างชัดเจนถึงสนธิสัญญาสิทธิมนุษยชนที่เกี่ยวข้อง และให้มีบทบัญญัติที่ชัดเจนเพื่อชี้แจงว่าไม่มีสิ่งใดในร่างอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมไซเบอร์ที่จะตีความว่าทำให้ขอบเขตของภาระผูกพันของรัฐภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศลดลงหรือลดน้อยลง

2) การมีข้อกำหนดการปกป้องหลักสิทธิมนุษยชนทั่วไปเพื่อให้แน่ใจว่ารัฐที่ปฏิบัติตามภาระผูกพันภายใต้ร่างอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมไซเบอร์จะปฏิบัติโดยสอดคล้องกับภาระผูกพันภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศ โดยร่างอนุสัญญาจะต้องรวมการคุ้มครองสิทธิมนุษยชนที่ครอบคลุม รวมถึงหลักการของความถูกต้องตามกฎหมาย การไม่เลือกปฏิบัติ จุดประสงค์ที่ถูกต้อง ความจำเป็น ความสมส่วน ความโปร่งใส การเยียวยาที่มีประสิทธิภาพ และการอนุญาตจากศาลล่วงหน้าที่ใช้ได้ตลอดทั้งร่างอนุสัญญา

3) การมีขอบเขตที่ชัดเจนและเป็นไปอย่างแคบของความผิดทางอาญาภายใต้ร่างอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมไซเบอร์ ที่หลีกเลี่ยงการทำให้การกระทำที่ได้รับการคุ้มครองภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศเป็นความผิดทางอาญา เช่น การใช้เสรีภาพในการแสดงออก นอกจากนี้ ร่างอนุสัญญาจะต้องรวมการคุ้มครองที่เข้มงวดสำหรับนักวิจัยด้านความปลอดภัย ผู้แจ้งเบาะแส นักเคลื่อนไหว และนักข่าว เพื่อป้องกันไม่ให้ถูกดำเนินคดีอย่างไม่เป็นธรรมเนื่องจากปฏิบัติหน้าที่

4) การมีบทบัญญัติที่ชัดเจนเพื่อหลีกเลี่ยงการใช้มาตรการในทางที่มีขอบ เช่น การแบ่งปันข้อมูลส่วนบุคคลโดยตรงต้องจำกัดเฉพาะการสืบสวนคดีอาญาโดยเฉพาะ และต้องอยู่ภายใต้มาตรการป้องกันขั้นต่ำที่เข้มงวด เช่น ความถูกต้องตามกฎหมาย

⁴⁵ OHCHR, **Human Rights and the Draft Cybercrime Convention** [Online], 5 October 2024. Source: <https://www.ohchr.org/sites/default/files/documents/issues/civicspace/DRAFT-CYBERCRIME-CONVENTION.pdf>

ความจำเป็น ความได้สัดส่วน ความโปร่งใส การแจ้งให้ผู้ใช้ทราบ และการได้รับอนุญาตจากศาลก่อน หรือขอบเขตและความร่วมมือระหว่างประเทศจะต้องจำกัดอยู่เฉพาะอาชญากรรมที่เกี่ยวข้องกับไซเบอร์ที่กำหนดไว้

5) การกำหนดบทบัญญัติเกี่ยวกับความร่วมมือระหว่างประเทศและความช่วยเหลือทางกฎหมายซึ่งกันและกันเพื่อหลีกเลี่ยงความขัดแย้งที่อาจเกิดขึ้นกับภาระผูกพันของรัฐภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศ

ซึ่งการแก้ปัญหาต่าง ๆ เหล่านี้ ผู้เขียนเห็นว่าจะช่วยให้หลักการสิทธิมนุษยชนได้รับการคุ้มครองอย่างแท้จริง โดยกระบวนการของ UN หลังจากผ่านร่างอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมไซเบอร์ โดย AHC แล้ว จะเป็นขั้นตอนต่าง ๆ เกี่ยวกับการทำให้ร่างอนุสัญญานี้ได้บังคับใช้ ซึ่งประเด็นสิทธิมนุษยชนยังคงเป็นปัญหาที่มีข้อวิจารณ์อยู่ และเป็นประเด็นที่ UN เองให้ความสำคัญเป็นอย่างยิ่ง สำหรับในมุมมองของประเทศไทยเองมีความจำเป็นต้องศึกษาและทำความเข้าใจกับรายละเอียดของร่างอนุสัญญาดังกล่าวเพื่อเตรียมความพร้อมและพิจารณาดำเนินการต่าง ๆ ต่อไป ร่างอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมไซเบอร์นี้อาจกล่าวได้ว่าจะเป็นหมุดหมายในการการต่อต้านอาชญากรรมไซเบอร์ที่กำลังทวีความรุนแรงและสร้างความเสียหายต่อระบบเศรษฐกิจและสังคมเป็นอย่างมาก แต่ก็ต้องตระหนักว่าไม่ควรละทิ้งประเด็นสิทธิมนุษยชนซึ่งเป็นหนึ่งในหลักการหลักร่วมกันของประชาคมระหว่างประเทศ

รายการอ้างอิง

- แอมเนสตี้, เสรีภาพในการแสดงออก [ออนไลน์], แหล่งที่มา: <https://www.amnesty.or.th/our-work/freedom-expression/>
- กระทรวงการต่างประเทศ, กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (International Covenant on Civil and Political Rights: ICCPR) [ออนไลน์], แหล่งที่มา: <https://humanrights.mfa.go.th/th/humanrights/obligation/international-human-rights-mechanism/ICCPR.php>
- กระทรวงการต่างประเทศ, คณะมนตรีสิทธิมนุษยชน แห่งสหประชาชาติ คำมั่นด้านสิทธิมนุษยชนของไทย และกระบวนการ UPR ฉบับประชาชน [ออนไลน์], แหล่งที่มา: <https://humanrights.mfa.go.th/upload/pdf/hrcth.pdf>
- กระทรวงการต่างประเทศ, ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights) [ออนไลน์], แหล่งที่มา: <https://humanrights.mfa.go.th/upload/pdf/udhr-th-en.pdf>
- สถานทูตสหรัฐฯ และสถานกงสุลในประเทศไทย, รายงานด้านสิทธิมนุษยชน ประจำปี พ.ศ. 2565 ประเทศไทย [ออนไลน์], แหล่งที่มา: <https://th.usembassy.gov/th/our-relationship-th/official-reports-th/2022-human-rights-reports-thailand-th/>
- สิงหนาท พงศ์ภิญโญศักดิ์, ปัญหาทางกฎหมายเกี่ยวกับการนำข้อมูลบิดเบือนเข้าสู่ระบบคอมพิวเตอร์: ศึกษากรณีการเผยแพร่ข้อมูลทางการเมือง [ออนไลน์], แหล่งที่มา: <http://law.master.kbu.ac.th/StudentTheses/2562/05.pdf>
- ilaw, เป็ดนิยาม-แยกองค์ประกอบ “ความผิดฐานนำเข้าข้อมูลเท็จ” ตาม พ.ร.บ.คอมพิวเตอร์ฯ [ออนไลน์], แหล่งที่มา: <https://www.ilaw.or.th/articles/4748>
- Chat Le Nguyen and Wilfred Golman, Diffusion of the Budapest Convention on Cybercrime and the Development of Cybercrime Legislation in Pacific Island Countries: ‘Law on the Books’ vs ‘Law in Action’, Computer Law & Security Review Volume 40 (April 2021).

- Commonwealth Secretariat, **Pacific to Establish Cybercrime Collaborative Platform as Threat Escalates** [Online], Source: <https://thecommonwealth.org/news/pacific-establish-cybercrime-collaborative-platform-threat-escalates>

- Commonwealth Secretariat, **Report of the Commonwealth Working Group of Experts on Cybercrime (Meeting of Commonwealth Law Ministers and Senior Officials)** [Online], Source: <https://www.combattingcybercrime.org/files/virtual-library/international-cooperation/report-of-the-commonwealth-working-group-of-experts-on-cybercrime.pdf>

- EFF, Privacy International and Electronic Frontier Foundations' **Comments on the Consolidated Negotiating Document of the UN Cybercrime Treaty** [Online], Source: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/Multi-stakeholders/PI-EFF_comments_on_consolidated_text_December_2022.pdf

- European Parliament, **Understanding Cybercrime** [Online], Source: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI\(2024\)760356_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf)

- ITU, **Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries (ICB4PAC)** [Online], Source: <https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/ICB4PAC/Pages/default.aspx>

- Joint Statement, **Joint Statement on the Proposed Cybercrime Treaty Ahead of the Concluding Session January 23, 2024** [Online], Source: <https://cdt.org/wp-content/uploads/2024/01/Joint-Advocacy-Statement-Cybercrime-Convention-Jan-23-2024.pdf>

- Katitza Rodriguez, **The UN Cybercrime Draft Convention Remains Too Flawed to Adopt** [Online], Source: <https://www.eff.org/deeplinks/2024/06/un-cybercrime-draft-convention-remains-too-flawed-adopt>

- Michael Minges and Christoph Stork, **Economic and Social Impact of ICT in the Pacific** [Online], Source: <https://www.theprif.org/documents/regional/information-communication-technology-ict/economic-and-social-impact-ict-pacific-0>

- Natadola Jyoti Pratibha, **How Cyber Criminals Defraud Fijians** [Online], Source: <https://fjisisun.com.fj/2018/12/08/how-cyber-criminals-defraud-fijians/>

- OHCHR, **Human Rights and the Draft Cybercrime Convention** [Online], Source: <https://www.ohchr.org/sites/default/files/documents/issues/civicspace/DRAFT-CYBERCRIME-CONVENTION.pdf>

- Reka Furtos, **Press Release United Nations: Member States Finalize a New Cybercrime Convention New York, 9 August 2024** [Online], Source: https://www.unodc.org/unodc/frontpage/2024/August/united-nations_-member-states-finalize-a-new-cybercrime-convention.html

- Summer Walker, **Still Poles Apart UN Cybercrime Treaty Negotiation, June 2023** [Online], Source: <https://globalinitiative.net/wp-content/uploads/2023/06/Summer-Walker-Poles-apart-UN-cybercrime-treaty-negotiations-GI-TOC-June-2023.pdf>

- Telecommunication Development Sector ITU, **Understanding Cybercrime: Phenomena, Challenges and Legal Response** [Online], Source: <https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf>

- United Nations, **A/AC.291/L.15, Draft United Nations Convention Against Cybercrime Strengthening International Cooperation for Combating Certain Crimes Committed by means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes** [Online], Source: <https://documents.un.org/doc/undoc/gen/v24/055/06/pdf/v2405506.pdf>

- United Nations, **A/RES/74/247, Countering the Use of Information and Communications Technologies for Criminal Purposes** [Online], Source: <https://documents.un.org/doc/undoc/gen/n19/440/28/pdf/n1944028.pdf>

- United Nations, **Convention on the Rights of the Child** [Online], Source: <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child>

- United Nations, **CRC/C/GC/25, General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment** [Online], Source: <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>