

อธิปไตยแห่งรัฐธรรมนูญในยุคดิจิทัล: บทวิเคราะห์นิติวิธีของสภา
แห่งรัฐฝรั่งเศสในคดี French Data Network สู่การถ่วงดุลระหว่าง
ความมั่นคงแห่งชาติกับสิทธิในข้อมูลส่วนบุคคล
Constitutional Sovereignty in the Digital Age: A Legal Analysis
of the French Council of State's Decision in the French
Data Network Case on Balancing
National Security and Data Privacy*

Received : 30 ม.ค. 2569

Revised : 12 มี.ค. 2569

Accepted : 13 มี.ค. 2569

อานันท์ กระบวนศรี**

Anan Krabuansri

สำนักงานศาลปกครอง

Administrative Court Office

บทคัดย่อ

บทความนี้มุ่งวิเคราะห์วิกฤตการณ์ความขัดแย้งของบรรทัดฐานกฎหมายระหว่างความมั่นคงของรัฐกับสิทธิความเป็นส่วนตัวในยุคดิจิทัล ผ่านกรณีศึกษาคำวินิจฉัยเชิงประวัติศาสตร์ของสภาแห่งรัฐฝรั่งเศส (Conseil d'État) ที่ประชุมใหญ่ ลงวันที่ 21 เมษายน 2021 ในคดี French Data Network et autres ซึ่งถือเป็นจุดเปลี่ยนสำคัญในการวางสถานะทางกฎหมายของการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Conservation des données de connexion) ท่ามกลางแรงกดดันจากศาลยุติธรรม

* บทความนี้เป็นความเห็นทางวิชาการของผู้เขียน ไม่ผูกพันหน่วยงานต้นสังกัด หน่วยงานต้นสังกัดไม่จำเป็นต้องเห็นพ้องด้วย.

เนื้อหาในบทความนี้สรุปและเรียบเรียงจากการวิเคราะห์เอกสารต้นฉบับภาษาฝรั่งเศสของสภาแห่งรัฐ (Conseil d'État) ในคดี French Data Network et autres (n° 393099) ลงวันที่ 21 เมษายน 2021 โดยครอบคลุมทั้งคำวินิจฉัยฉบับเต็ม (Décision) บทวิเคราะห์แนวบรรทัดฐาน (Analyse) และคำแถลงการณ์ของตุลาการผู้แถลงคดี (Conclusions du rapporteur public). สามารถสืบค้นข้อมูลฉบับเต็มได้ที่ : คำวินิจฉัย Conseil d'État, « Base de jurisprudence », 21 avril 2021. [ออนไลน์]. เข้าถึงได้ที่: <https://www.conseil-etat.fr/fr/>

แห่งสหภาพยุโรปที่มีแนวโน้มจะห้ามมิให้รัฐจัดเก็บข้อมูลเป็นการทั่วไปและไม่เจาะจง (Conservation généralisée et indifférenciée)

ผลการศึกษาพบว่า สภาแห่งรัฐได้ใช้นิติวิธีอันแยบยลในการหลีกเลี่ยงสงครามระหว่างตุลาการ โดยมิได้ประกาศตัดขาดอำนาจของศาลยุติธรรมแห่งสหภาพยุโรป แต่กลับเลือกใช้การตีความกฎหมายแบบประสานประโยชน์เพื่อยืนยันหลักความเป็นกฎหมายสูงสุดของรัฐธรรมนูญ (Primauté de la Constitution) เหนือกฎหมายลำดับรองของสหภาพยุโรป ในกรณีที่มีความเสี่ยงต่อการกระทบกระเทือนสาระสำคัญของเอกลักษณ์ทางรัฐธรรมนูญ พร้อมทั้งวางหลักกฎหมายใหม่โดยจำแนกประเภทความเข้มข้นของการจัดเก็บข้อมูลระหว่าง “เลขที่อยู่ไอพี” (Adresse IP) กับข้อมูลจราจรอื่น ๆ และนิยามเงื่อนไข “ภัยคุกคามร้ายแรงต่อความมั่นคงแห่งชาติ” (Menace grave pour la sécurité nationale) ให้สอดคล้องกับบริบทความเป็นจริง เพื่อรักษาไว้ซึ่งเครื่องมือในการสืบสวนสอบสวนทางอาญาและการป้องกันการก่อการร้าย

บทความนี้จึงนำเสนอข้อมูลและความเห็นทางวิชาการเพื่อเป็นกรณีศึกษาเปรียบเทียบกับแนวทางพิจารณาสำหรับประเทศไทยในการออกแบบกฎหมายความมั่นคงไซเบอร์และกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ให้มีดุลยภาพที่ยั่งยืนระหว่างอำนาจอธิปไตยของรัฐในการรักษาความสงบเรียบร้อยกับพันธกรณีในการคุ้มครองสิทธิข้อมูลส่วนบุคคลตามมาตรฐานสากล

คำสำคัญ

การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์, สภาแห่งรัฐฝรั่งเศส, หลักความเป็นกฎหมายสูงสุดของกฎหมายสหภาพยุโรป, หลักความเป็นกฎหมายสูงสุดของรัฐธรรมนูญ, นิติรัฐในยุคดิจิทัล, อธิปไตยทางดิจิทัล, ปัญญาประดิษฐ์และอัลกอริทึม, กฎหมายความมั่นคงไซเบอร์, การคุ้มครองข้อมูลส่วนบุคคล (PDPA), หลักความได้สัดส่วน, องค์การตรวจสอบอิสระที่มีอำนาจผูกพัน, การทำนายพฤติกรรมอาชญากรรม (Predictive Policing), นิติวิธีแบบ Solange

arianeweb/CE/decision/2021-04-21/393099 บทวิเคราะห์ Conseil d'État, Analyse de la décision. [ออนไลน์]. เข้าถึงได้ที่: <https://www.conseil-etat.fr/fr/arianeweb/CE/analyse/2021-04-21/393099>
คำแถลงการณ์ Alexandre LALLET, «Conclusions sur Conseil d'État, French Data Network et autres », n° 393099. [ออนไลน์]. เข้าถึงได้ที่: <https://www.conseil-etat.fr/fr/arianeweb/CRP/conclusion/2021-04-21/393099>.

** น.บ., น.ม. (กฎหมายมหาชน), มหาวิทยาลัยธรรมศาสตร์, ประกาศนียบัตรชั้นสูง (กฎหมายปกครอง) (เกียรตินิยม) มหาวิทยาลัย Paris Panthéon – Assas, นิติศาสตรมหาบัณฑิต (กฎหมายมหาชนทางธุรกิจ) มหาวิทยาลัย Paris - Saclay (เกียรตินิยม) (ทุนรัฐบาล ก.พ.), นิติศาสตรดุษฎีบัณฑิต (กฎหมายมหาชน) มหาวิทยาลัย Toulouse Capitole (ทุนรัฐบาลฝรั่งเศส) ประเทศฝรั่งเศส, พนักงานคดีปกครองชำนาญการ กลุ่มสนับสนุนวิชาการคดีปกครอง สำนักวิจัยและวิชาการ สำนักงานศาลปกครอง.

Abstract

This article analyzes the conflict of legal norms between national security imperatives and privacy rights in the digital age through the landmark decision of the French Council of State (*Conseil d'État*), sitting in Assembly, dated April 21, 2021, in the *French Data Network et autres* case. This ruling represents a critical turning point in determining the legal status of data retention (*conservation des données de connexion*) amidst pressure from the Court of Justice of the European Union (CJEU), which prohibits general and indiscriminate retention (*conservation généralisée et indifférenciée*).

The study reveals that the Council of State employed sophisticated legal reasoning to avert a “war of judges” without explicitly rejecting the CJEU’s authority. Instead, it adopted a constructive interpretation to assert the Primacy of the Constitution (*Primauté de la Constitution*) over EU secondary law whenever the essence of constitutional identity is at risk. Furthermore, the decision established a new legal framework by distinguishing the retention requirements between “IP addresses” (*Adresse IP*) and other traffic data, while redefining “serious threats to national security” (*menace grave pour la sécurité nationale*) to align with operational realities, thereby preserving essential tools for criminal investigation and counter-terrorism.

Consequently, this article presents academic insights and a comparative case study to serve as a guideline for Thailand in formulating cybersecurity and computer crime laws. It aims to achieve a sustainable equilibrium between the state’s sovereign power to maintain public order and the obligation to protect personal data rights in accordance with international standards.

Keywords

Data Retention, French Council of State (*Conseil d'État*), Primacy of European Union law, Primacy of the Constitution, Digital Rule of Law, Digital Sovereignty, Artificial Intelligence and Algorithms, Cybersecurity Law, Personal Data Protection (PDPA), Principle of Proportionality, Independent Oversight with Binding Power, Predictive Policing, Solange Doctrine

บทนำ

เหตุการณ์ก่อการร้ายกรุงปารีสเมื่อวันที่ 13 พฤศจิกายน 2015 ณ โรงละคร Bataclan และ สนามกีฬา Stade de France ซึ่งคร่าชีวิตผู้คนกว่า 130 ศพ มิได้เป็นเพียงหนึ่งในโศกนาฏกรรม ความมั่นคงครั้งร้ายแรงที่สุดในประวัติศาสตร์ฝรั่งเศสร่วมสมัยเท่านั้น หากแต่ยังเป็นปฐมบทที่เปิดเผยให้เห็นถึงรอยร้าวระหว่างแนวคิดเกี่ยวกับความมั่นคงปลอดภัยและเสรีภาพของประชาชนอย่างชัดเจน สาเหตุของรอยร้าวดังกล่าวมาจากข้อเท็จจริงที่ว่า ท่ามกลางความโกลาหลของสถานการณ์ที่น่าเศร้านี้ สิ่ง чтоช่วยให้เจ้าหน้าที่สามารถระบุตัวตนและหลายเครือข่ายผู้ก่อการร้ายได้ทันท่วงที มิใช่พยานบุคคล หรือลายนิ้วมือ หากแต่คือ “ร่องรอยทางดิจิทัล” (Traces numériques) โดยเฉพาะการวิเคราะห์ ข้อมูลพิกัดตำแหน่งจากโทรศัพท์มือถือที่คนร้ายทิ้งไว้ และการเชื่อมโยงข้อมูลการติดต่อสื่อสาร ในพื้นที่ที่เกิดเหตุ ซึ่งกลายเป็นหัวใจสำคัญในการไขปริศนาคดี

ความจำเป็นอย่างยิ่งยวด ในการเข้าถึงข้อมูลดังกล่าวได้รับการยืนยันในเชิงประจักษ์ผ่านสถิติที่ M. Alexandre Lallet ตุลาการผู้แถลงคดี (Rapporteur public)¹ ได้นำเสนอ โดยระบุว่าในแต่ละปี ระบบยุติธรรมทางอาญาของฝรั่งเศสมีคำสั่งเรียก “ข้อมูลการเชื่อมต่อ” (Données de connexion) จากผู้ให้บริการมากกว่า 2.5 ล้านคำสั่ง ข้อมูลเหล่านี้ประกอบด้วยข้อมูลระบุตัวตน (Identité) ข้อมูล การติดต่อ (Trafic) และข้อมูลพิกัดตำแหน่ง (Localisation) ซึ่งถือเป็นเครื่องมือที่ขาดไม่ได้ ในการสืบสวนสอบสวนอาชญากรรมร้ายแรงและการต่อต้านการก่อการร้าย

การใช้อำนาจรัฐเพื่อจัดเก็บและเข้าถึงข้อมูลมหาศาลนี้ สร้างความกังวลว่ารัฐจะใช้อำนาจเข้าไป กระทบสิทธิความเป็นส่วนตัวของประชาชนเกินความพอดี กลายเป็นการสถาปนาระบอบกฎหมายใหม่ เปิดยุคสมัยแห่งการสอดแนมในนามของความมั่นคง วิวาทะดังกล่าวได้นำไปสู่จุดแตกหัก เมื่อศาลยุติธรรมแห่งสหภาพยุโรป (Cour de justice de l'Union européenne (CJUE)) ได้วางบรรทัดฐานที่เข้มงวดสูงสุดในคดี *La Quadrature du Net* (2020)² โดยวินิจฉัยว่า กฎหมายภายในของรัฐสมาชิกที่กำหนดหน้าที่ให้ผู้ให้บริการต้องจัดเก็บข้อมูลแบบทั่วไปและ ไม่เจาะจง (Conservation généralisée et indifférenciée) เป็นมาตรการที่ขัดต่อกฎหมาย

¹ ตุลาการผู้แถลงคดี (Rapporteur public) คือ ตุลาการอิสระผู้ทำหน้าที่เสนอความเห็นส่วนตัว (Conclusions) เพื่อเสนอแนะแนวทางวินิจฉัยคดี โดยมีได้เป็นองค์คณะพิจารณาพิพากษาและความคิดเห็นดังกล่าว ไม่มีผลผูกพัน องค์คณะแต่อย่างใด เอกสารนี้จึงมิใช่คำพิพากษา แต่มีความสำคัญยิ่งในการช่วยอธิบายตรรกะ ทางกฎหมาย เบื้องหลังคำวินิจฉัยของสภาแห่งรัฐที่มักเขียนอย่างสั้นกระชับ.

² CJUE, Gde ch., 6 octobre 2020, *La Quadrature du Net et autres*, aff. jointes C-511/18, C-512/18 et C-520/18, ECLI:EU:C:2020:791.

สหภาพยุโรปและกฎบัตรสิทธิพื้นฐานแห่งสหภาพยุโรป (Charte des droits fondamentaux de l'Union européenne)³ โดยศาลยุติธรรมแห่งสหภาพยุโรปยอมรับข้อยกเว้นเพียงกรณีเดียว คือสถานการณ์ที่รัฐเผชิญกับภัยคุกคามร้ายแรงต่อความมั่นคงแห่งชาติที่เกิดขึ้นจริงและเป็นปัจจุบัน

ผลสืบเนื่องจากคำวินิจฉัยดังกล่าว ได้สร้างแรงสนับสนุนต่อรากฐานของระบบกฎหมาย วิธีพิจารณาความอาญาและความมั่นคงของประเทศฝรั่งเศส ทำให้รัฐบาลตกอยู่ในสภาวะกลืนไม่เข้า คายไม่ออกในการบริหารราชการแผ่นดิน กล่าวคือ หากปฏิบัติตามแนวทางของศาลยุติธรรมแห่ง สหภาพยุโรปอย่างเคร่งครัด รัฐย่อมเสี่ยงต่อการสูญเสียกลไกสำคัญในการสืบสวนสอบสวนอาชญากรรม ทั่วไป แต่หากเพิกเฉยก็ย่อมเป็นการละเมิดพันธกรณีเหนือรัฐ

บทความนี้จึงมุ่งวิเคราะห์ทางออกของวิกฤตการณ์ดังกล่าว ผ่านคำวินิจฉัยประวัติศาสตร์ ของสภาแห่งรัฐ (Conseil d'État) ที่ประชุมใหญ่ ลงวันที่ 21 เมษายน 2021 ในคดี *French Data Network et autres* ซึ่งสภาแห่งรัฐต้องตัดสินใจครั้งสำคัญระหว่างการปฏิเสธพันธกรณีตามกฎหมาย ของสหภาพยุโรปหรือการใช้อำนาจตรวจสอบการกระทำนอกเหนืออำนาจ (*Ultra vires*) ดังเช่นกรณี ของศาลรัฐธรรมนูญเยอรมัน⁴ อย่างไรก็ตาม สภาแห่งรัฐได้หลีกเลี่ยงความขัดแย้งรุนแรงระหว่างศาล โดยเน้นการใช้เทคนิคการตีความกฎหมายเพื่อยืนยันหลักความเป็นกฎหมายสูงสุดของรัฐธรรมนูญ เหนือกฎหมายลำดับรองของสหภาพยุโรป ในกรณีที่กฎหมายดังกล่าวกระทบต่อสาระสำคัญของ

³ มาตรา 6 แห่งสนธิสัญญาว่าด้วยสหภาพยุโรปฯ (สนธิสัญญาลิสบอน) เป็นสนธิสัญญาที่กำหนดให้กฎบัตรสิทธิ ขั้นพื้นฐานฯ มีคุณค่าทางกฎหมายเทียบเท่ากับสนธิสัญญาของสหภาพยุโรป ส่งผลให้กฎบัตรมีผลผูกพันต่อรัฐสมาชิก ต้องเคารพและปฏิบัติตาม, โปรดดู Vie-publique, « Qu'est-ce que la Charte des droits fondamentaux de l'Union européenne ? », 9 août 2024, [en ligne], disponible sur : <https://www.vie-publique.fr/fiches/20322-quest-ce-que-la-charte-des-droits-fondamentaux-de-lunion-europeenne>.

⁴ ในคำแถลงการณ์ของตุลาการผู้แถลงคดี Alexandre Lallet ได้หยิบยกสถานการณ์ในประเทศเยอรมนีขึ้นมา เปรียบเทียบ โดยอ้างถึงคำวินิจฉัยของศาลรัฐธรรมนูญกลางแห่งเยอรมนี (Bundesverfassungsgericht) เมื่อวันที่ 5 พฤษภาคม 2020 ซึ่งสร้างแรงสนับสนุนด้วยการวินิจฉัยว่าคำพิพากษาของศาลยุติธรรมแห่ง สหภาพยุโรปเป็นการกระทำโดยนอกเหนือขอบเขตอำนาจ (*Ultra vires*) โดยศาลเยอรมันให้เหตุผลว่าการตีความ กฎหมายของศาลยุโรปนั้นขาดความสมเหตุสมผลจนไม่สามารถทำความเข้าใจได้อีกต่อไป (n'est tout simplement plus compréhensible) และมีลักษณะเป็นอำเภอใจโดยแท้ (objectivement arbitraire) ซึ่งแนวคิดนี้มีรากฐานมาจากหลักการตรวจสอบเอกลักษณ์ทางรัฐธรรมนูญ (Identitätskontrolle) ที่ศาลเยอรมัน สแกนอำนาจที่จะไม่ปฏิบัติตามกฎหมายของสหภาพยุโรปหากกระทบกระเทือนต่อหลักการพื้นฐานของกฎหมาย พื้นฐาน (Grundgesetz) การยกกรณีความแตกหักนี้ขึ้นมาอ้างอิง มีนัยสำคัญเพื่อชี้ให้สภาแห่งรัฐเห็นถึงทางเลือก ที่รุนแรงในการจัดการกับความขัดแย้งระหว่างระบอบกฎหมาย อย่างไรก็ตาม ตุลาการผู้แถลงคดีเสนอแนะว่า แม้จะมีตัวอย่างของการปฏิเสธอำนาจอย่างชัดเจนจากประเทศเพื่อนบ้าน แต่สภาแห่งรัฐฝรั่งเศสไม่ควรเลือกเดิน ตามรอยความขัดแย้งเช่นนั้น หากแต่ควรเลือกใช้นิติวิธีที่ประนีประนอมและสร้างสรรค์กว่า เพื่อรักษาคุณภาพของ อำนาจระหว่างรัฐและสหภาพยุโรปได้อย่างยั่งยืน.

รัฐธรรมนูญควบคู่ไปกับการวางหลักเกณฑ์ใหม่ที่กำหนดประเภทความเข้มข้นของการจัดเก็บข้อมูลระหว่าง “เลขที่อยู่ไอพี” (Adresse IP) กับข้อมูลจราจรประเภทอื่น และการนิยามเงื่อนไข “ภัยคุกคามร้ายแรง” ให้สอดคล้องกับความเป็นจริง เพื่อเป็นแนวทางพิจารณาสำหรับประเทศไทย ในการออกแบบกฎหมายดิจิทัลที่สามารถสร้างดุลยภาพที่ยั่งยืนระหว่างอำนาจอธิปไตยของรัฐ ในการรักษาความสงบเรียบร้อย กับพันธกรณีในการคุ้มครองสิทธิส่วนบุคคลตามมาตรฐานสากล

บทที่ 1 ความขัดแย้งของบรรทัดฐานทางกฎหมายในยุคแห่งการสอดแนม

สถานการณ์ความขัดแย้งทางกฎหมายในคดี *French Data Network et autres* มีรากฐานมาจากความจำเป็นในการรักษาความสงบเรียบร้อยของรัฐ ที่ต้องเผชิญหน้ากับข้อจำกัดทางกฎหมาย สิทธิมนุษยชนระดับกฎหมายของสหภาพยุโรปอย่างรุนแรง เนื้อหาในส่วนนี้จะมุ่งวิเคราะห์ความเป็นจริง ในทางปฏิบัติและนัยสำคัญของพยานหลักฐานดิจิทัล ตลอดจนพลวัตทางกฎหมายที่นำไปสู่สถานะทางแพร่ของกระบวนการยุติธรรม

1.1 บทบาทของพยานหลักฐานดิจิทัล

M. Alexandre Lallet ตุลาการผู้แถลงคดีได้ยกตัวอย่างเหตุการณ์เมื่อวันที่ 13 พฤศจิกายน 2015 หรือการก่อการร้ายที่บาตาคล็อง (Attentats du Bataclan) ซึ่งมีผู้เสียชีวิต 130 ศพ และบาดเจ็บกว่า 350 คน การสืบสวนเพื่อระบุตัวคนร้ายและเครือข่ายผู้กระทำความผิดมิได้อาศัยเพียงพยานบุคคล แต่เกิดจากการรวบรวมข้อมูลการเชื่อมต่อ (Données de connexion) ในพื้นที่เกิดเหตุ โดยเฉพาะการตรวจสอบภาพจากกล้องวงจรปิด (Vidéo - surveillance) ที่แสดงให้เห็นผู้ก่อการร้ายใช้โทรศัพท์ก่อนจุดชนวนระเบิด และการนำข้อมูลการโทรทั้งหมดในพื้นที่มาสอบทานกับข้อมูลในโทรศัพท์ที่ถูกทิ้งไว้ในถังขยะ ซึ่งนำไปสู่การจับกุมผู้เกี่ยวข้องได้ในที่สุด

กรณีดังกล่าวสะท้อนให้เห็นถึงความจริงอันน่าตื่นตะลึงของตัวเลข (Impressionnante réalité des chiffres) กล่าวคือ ข้อมูลการเชื่อมต่อ หรือที่เรียกว่า “เมทาเดตา” (Métadonnées) ซึ่งแตกต่างจากข้อมูลเนื้อหาของการสื่อสาร (Contenu des échanges) ได้กลายเป็นเครื่องมือหลักในกระบวนการยุติธรรม โดยสถิติบ่งชี้ว่ามีคำสั่งเรียกพยานหลักฐานผ่านระบบศูนย์กลางโครงข่ายแห่งชาติสำหรับการดักจับข้อมูลในกระบวนการยุติธรรม (Plateforme nationale des interceptions judiciaires (PNIJ)) มากกว่า 2 ล้านคำสั่งต่อปี (และสูงถึง 2.5 ล้านคำสั่งในปี 2020)

ข้อมูลเหล่านี้ถูกใช้ในการสืบสวนสอบสวนคดีอาญามากกว่า 4 ใน 5 ของคดีทั้งหมด และที่สำคัญที่สุดคือ ถูกใช้ในทุกกรณีของการสืบสวนคดีอาชญากรรมและการกระทำผิดที่เป็นขบวนการ (Criminalité et délinquance en bande organisée) นอกจากนี้ ในมิติของงานข่าวกรอง หน่วยงานบริการข่าวกรอง (Services de renseignement) ได้ยื่นคำขออนุมัติมากกว่า 50,000 ครั้งต่อปี โดยผ่านการตรวจสอบของคณะกรรมการควบคุมเทคนิคการข่าวกรองแห่งชาติ (Commission

nationale de contrôle des techniques de renseignement (CNCTR)) เพื่อวัตถุประสงค์ในการต่อต้านการก่อการร้าย (Lutte contre le terrorisme) การต่อต้านการจารกรรม (Contre-espionnage) และการตรวจจับขบวนการค้ายาเสพติด

1.2 การจำแนกประเภทของข้อมูล

ตามคำแถลงการณ์ของตุลาการผู้แถลงคดี ข้อมูลการเชื่อมต่อที่ถูกจัดเก็บและนำมาใช้ประโยชน์ภายใต้กรอบกฎหมายของฝรั่งเศสอาจแบ่งออกเป็น 3 ประเภทหลัก ได้แก่

1. ข้อมูลระบุตัวตน (Données d'identité) คือ ข้อมูลที่ทำให้ทราบว่าใครอยู่เบื้องหลังหมายเลขโทรศัพท์ หรือหมายเลขซิมการ์ด (IMSI) หรือรหัสประจำเครื่องโทรศัพท์ (IMEI) รวมถึงที่อยู่ไอพี (Adresse IP)

2. ข้อมูลเกี่ยวกับการจราจร (Données relatives au trafic) คือ ข้อมูลที่เปิดเผยถึงคู่สนทนา (Contacts) วันเวลา และระยะเวลาของการติดต่อ (หรือที่เรียกกันทั่วไปว่า “Fadettes”) รวมถึงประวัติการส่งและรับอีเมล แต่ไม่รวมถึงเนื้อหา

3. ข้อมูลระบุตำแหน่ง (Données de localisation) คือ ข้อมูลที่ทำให้ทราบถึงพื้นที่การส่งและรับสัญญาณ (Zones d'émission et de réception) หรือเสาสัญญาณที่การสื่อสารนั้นวิ่งผ่าน (Borne) ซึ่งนำไปสู่การระบุพิกัด (Bornage) ของบุคคล

พันธกรณีในการจัดเก็บข้อมูลเหล่านี้ ถูกบัญญัติไว้ในประมวลกฎหมายไปรษณีย์และการสื่อสารอิเล็กทรอนิกส์ (Code des postes et des communications électroniques (CPCE)) มาตรา L. 34 - 1⁵ และกฎหมายเพื่อความเชื่อมั่นในเศรษฐกิจดิจิทัล (Loi pour la confiance dans l'économie numérique (LCEN)) มาตรา 6⁶ ซึ่งกำหนดให้ผู้ให้บริการเครือข่าย (Opérateurs) และผู้ให้บริการอินเทอร์เน็ต ต้องทำการเก็บรักษาข้อมูลดังกล่าวเป็นระยะเวลา 1 ปี เพื่อวัตถุประสงค์ในการสืบสวนสอบสวนทางอาญาและการรักษาความมั่นคง ซึ่งเป็นการจัดเก็บในลักษณะ “ทั่วไปและไม่เจาะจง” (Généralisée et indifférenciée) หรือที่เรียกอย่างเข้าใจได้ง่ายว่าแบบหว่านแหหรือแบบเหมาเข่งนั่นเอง

⁵ Article L. 34 - 1 du Code des postes et des communications électroniques (Version en vigueur du 20 décembre 2013 au 31 juillet 2021) : « ... Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales... il peut être différé *pour une durée maximale d'un an* aux opérations tendant à effacer..... ».

⁶ Article 6 de la Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (Version en vigueur du 26 juin 2020 au 31 juillet 2021) : « ... II. - Les personnes mentionnées aux 1 et 2 du I détiennent et conservent les données de nature à permettre l'identification de *quiconque* a contribué à la création du contenu... ».

1.3 คำวินิจฉัยของศาลยุติธรรมแห่งสหภาพยุโรป

กฎหมายภายในของประเทศฝรั่งเศสได้เผชิญกับแรงกดดันครั้งใหญ่จากการตีความกฎหมายสหภาพยุโรปโดยเฉพาะข้อบังคับที่ 2002/58/CE ว่าด้วยการประมวลผลข้อมูลส่วนบุคคล และการคุ้มครองความเป็นส่วนตัวทางอิเล็กทรอนิกส์⁷ และระเบียบที่ (UE) 2016/679 ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (RGPD)⁸ ผ่านแนวบรรทัดฐานของศาลยุติธรรมแห่งสหภาพยุโรป ในคดี *La Quadrature du Net et autres* (2020) ศาลยุติธรรมแห่งสหภาพยุโรปได้วางหลักการสำคัญว่า มาตรา 15 วรรค 1 ของ Directive 2002/58/CE⁹ เมื่ออ่านประกอบกับกฎบัตรสิทธิพื้นฐานแห่งสหภาพยุโรป มาตรา 7 ที่รับรองสิทธิของปัจเจกชนในการได้รับความเคารพในชีวิตส่วนตัวและการสื่อสาร ซึ่งทำหน้าที่เป็นเกราะป้องกันการแทรกแซงโดยรัฐ ควบคู่ไปกับมาตรา 8 ที่วางหลักการคุ้มครองข้อมูลส่วนบุคคล โดยกำหนดให้การประมวลผลข้อมูลต้องเป็นไปอย่างเป็นธรรม เพื่อวัตถุประสงค์ที่เฉพาะเจาะจง และต้องอยู่ภายใต้การกำกับดูแลขององค์กรอิสระ และมาตรา 11 ที่รับรองเสรีภาพในการแสดงออกและเสรีภาพในการรับหรือส่งข้อมูลข่าวสารโดยปราศจากการแทรกแซงจากอำนาจสาธารณะ ซึ่งศาลยุติธรรมแห่งสหภาพยุโรปได้วางแนววินิจฉัยว่า การจัดเก็บข้อมูลจราจร

⁷ Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

⁸ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

⁹ Article 15 de Directive 2002/58/CE : « Application de certaines dispositions de la directive 95/46/CE 1. Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ... ».

Charte des droits fondamentaux de l'Union européenne

แบบเหวี่ยงแหย่อมกระทบกระเทือนต่อสาระสำคัญของสิทธิเหล่านี้อย่างยิ่งร้ายแรง¹⁰ หลักกฎหมายของยุโรปจึงเข้ามา “ขัดขวาง” (S’oppose) กฎหมายของรัฐสมาชิกไม่ให้มีการจัดเก็บข้อมูลจราจรและข้อมูลระบุตำแหน่งแบบ “ทั่วไปและไม่เจาะจง” ในลักษณะที่เป็นมาตรการป้องกันล่วงหน้า (À titre préventif) สะท้อนให้เห็นว่ากฎหมายและองค์กรผู้ใช้กฎหมายของสหภาพยุโรปได้เข้มงวดกับเรื่องการจัดเก็บข้อมูลเป็นอย่างมาก¹¹

ศาลยุติธรรมแห่งสหภาพยุโรปเห็นว่าการจัดเก็บข้อมูลในลักษณะดังกล่าวของประเทศฝรั่งเศสก่อให้เกิดการแทรกแซงที่ร้ายแรง (Ingérence grave) ต่อสิทธิพื้นฐาน กรณีจะจัดเก็บข้อมูลในลักษณะเช่นนี้ได้ก็ต้องเข้าข้อยกเว้นที่จำกัด ได้แก่ 1) เพื่อความมั่นคงแห่งชาติ (Sécurité nationale) ศาลอนุญาตให้จัดเก็บแบบทั่วไปและไม่เจาะจงได้ ก็ต่อเมื่อรัฐเผชิญกับภัยคุกคามร้ายแรงต่อความมั่นคงแห่งชาติ ที่เกิดขึ้นจริงและเป็นปัจจุบัน หรือที่คาดการณ์ได้ (Menace grave pour la sécurité nationale qui s’avère réelle et actuelle ou prévisible) โดยต้องมีการกำหนดระยะเวลาจำกัดเท่าที่จำเป็นอย่างเคร่งครัด (Strictement nécessaire) และอยู่ภายใต้การควบคุมที่มีประสิทธิภาพ 2) เพื่อการต่อสู้กับอาชญากรรมร้ายแรง (Criminalité grave) ศาลยุติธรรมแห่งสหภาพยุโรปได้วางบรรทัดฐานห้ามมิให้รัฐกำหนดมาตรการจัดเก็บข้อมูลจราจรในลักษณะ “การจัดเก็บเป็นการทั่วไปโดยปราศจากการจำแนกแยกแยะ” (Conservation généralisée et indifférenciée) ซึ่งมีผลเป็นการกวาดต้อนเก็บข้อมูลของประชาชนทุกคนโดยปราศจากเหตุอันควร แต่ศาลได้เปิดช่องให้รัฐใช้อำนาจจำกัดสิทธิได้เพียง 2 กรณี ภายใต้เงื่อนไขที่เคร่งครัด ได้แก่ 1) การจัดเก็บข้อมูลแบบเจาะจงเป้าหมาย (Conservation ciblée) คือการอนุญาตให้รัฐจัดเก็บข้อมูลได้เฉพาะกับกลุ่มบุคคลหรือพื้นที่ทางภูมิศาสตร์ที่มีความเสี่ยงอย่างแท้จริงเท่านั้น ตัวอย่างเช่น รัฐอาจออกกฎหมายให้เฉพาะเสาสัญญาณโทรศัพท์ในบริเวณจุดยุทธศาสตร์ เช่น สนามบิน ท่าเรือ หรือพื้นที่ชายแดนที่มีสถิติการก่อความไม่สงบ ต้องทำการบันทึกข้อมูลการติดต่อสื่อสารไว้ ในขณะที่พื้นที่พักอาศัยทั่วไปของประชาชน ผู้บริสุทธิ์ย่อมไม่อยู่ภายใต้ภาระหน้าที่ในการถูกจัดเก็บข้อมูลดังกล่าว 2) มาตรการรักษาสภาพข้อมูลไว้อย่างเร่งด่วน (Conservation rapide หรือ Quick freeze ในภาษาอังกฤษ) เป็นกลไกที่ให้อำนาจเจ้าหน้าที่สั่งระงับการลบทำลายข้อมูลที่มีอยู่แล้วในระบบเมื่อเกิดเหตุอาชญากรรมขึ้น เพื่อมิให้

¹⁰ Article 7 : « Toute personne a droit au respect de sa vie privée et familiale... et de ses communications. ».

Article 8 : « 1. Toute personne a droit à la protection des données à caractère personnel la concernant... 3. Le respect de ces règles est soumis au contrôle d’une autorité indépendante. ».

Article 11 : « 1. Toute personne a droit à la liberté d’expression. Ce droit comprend... la liberté de recevoir ou de communiquer des informations ou des idées sans qu’il puisse y avoir ingérence d’autorités publiques... ».

¹¹ Luc Grynbaum, Droit des activités numériques, (Daloz 2^e éd, 2023), 820 - 821.

พยานหลักฐานสูญหายไป ตัวอย่างเช่น เมื่อเกิดเหตุระเบิด เจ้าหน้าที่สามารถออกคำสั่งไปยังผู้ให้บริการเพื่อขอให้ “แช่แข็ง” หรือหยุดวงจรการลบข้อมูลอัตโนมัติ (Data retention cycle) เฉพาะส่วนที่เกี่ยวข้องกับผู้ต้องสงสัยหรือช่วงเวลาที่เกิดเหตุไว้เป็นการชั่วคราว เพื่อรอการตรวจสอบโดยศาล โดยไม่จำเป็นต้องเก็บสะสมข้อมูลของประชาชนทั้งประเทศไว้ล่วงหน้าตลอดเวลา

ความขัดแย้งนี้สร้างสภาวะกลืนไม่เข้าคายไม่ออกให้กับรัฐฝรั่งเศส เนื่องจากระบบการสืบสวนสอบสวนทางอาญาและการข่าวกรองของฝรั่งเศสพึ่งพาดูแลข้อมูลที่ถูกเก็บแบบทั่วไป (Mass retention) เป็นหลัก การปฏิบัติตามคำวินิจฉัยของศาลยุติธรรมแห่งสหภาพยุโรปอย่างเคร่งครัดย่อมหมายถึงความเสี่ยงที่จะสูญเสียความสามารถในการปฏิบัติการเพื่อประโยชน์สาธารณะในการคุ้มครองความปลอดภัยของประชาชน ซึ่งถือเป็นวัตถุประสงค์ที่มีคุณค่าระดับรัฐธรรมนูญ (Objectifs de valeur constitutionnelle) ตามที่รัฐบาลฝรั่งเศสได้ยกขึ้นต่อสู้ในคดีนี้

บทที่ 2 ศิลปะแห่งการตีความของสภาแห่งรัฐเพื่อสร้างเกราะป้องกันทางรัฐธรรมนูญ

ท่ามกลางแรงกดดันจากคำพิพากษาของศาลยุติธรรมแห่งสหภาพยุโรปในคดี La Quadrature du Net (2020) ที่วางหลักห้ามการเก็บข้อมูลแบบเป็นการทั่วไปและไม่เจาะจง สภาแห่งรัฐต้องเผชิญกับสภาวะกลืนไม่เข้าคายไม่ออกทางกฎหมายที่แหลมคมที่สุด ด้านหนึ่งคือพันธกรณีในการเคารพกฎหมายสหภาพยุโรปที่มีสถานะเหนือกว่ากฎหมายภายในตามมาตรา 88 - 1¹² ของรัฐธรรมนูญแห่งสาธารณรัฐฝรั่งเศส แต่อีกด้านหนึ่งคือความจำเป็นอันไม่อาจหลีกเลี่ยงได้ในการรักษาความมั่นคงแห่งชาติและความสงบเรียบร้อยของบ้านเมืองซึ่งเป็นเงื่อนไขความอยู่รอดของรัฐ ในบทนี้จะวิเคราะห์นิติวิธีอันแยบยลที่สภาแห่งรัฐนำมาใช้เพื่อฝ่าทางตันดังกล่าว โดยมีได้เลือกหนทางแห่งการแตกหัก แต่กลับเลือกใช้ยุทธวิธีทางตุลาการขั้นสูงเพื่อยืนยันความเป็นกฎหมายสูงสุดของรัฐธรรมนูญในระบบกฎหมายภายในพร้อมกับการประสานรอยร้าวกับระบบกฎหมายยุโรปไปพร้อมกัน

2.1 การยืนยันความเป็นกฎหมายสูงสุดของรัฐธรรมนูญในระบบกฎหมายภายใน

จุดเริ่มต้นของกระบวนการถ่วงดุลอำนาจในคดีนี้ เริ่มต้นจากการที่สภาแห่งรัฐได้วางหลักการพื้นฐานทางรัฐธรรมนูญใหม่อย่างชัดเจน โดยอาศัยการตีความ มาตรา 88 - 1 ของรัฐธรรมนูญ สภาแห่งรัฐได้วินิจฉัยวางหลักการว่า แม้มาตรา 88 - 1 จะรับรองการดำรงอยู่ของระบอบกฎหมายของสหภาพยุโรป (Ordre juridique de l'Union européenne) ที่บูรณาการเข้ากับระบอบกฎหมายภายใน แต่บทบัญญัติเดียวกันนี้ก็ยืนยันในตัวเองว่ารัฐธรรมนูญยังคงดำรงสถานะอยู่ ณ จุดสูงสุด (La place de la Constitution au sommet) ของระบอบกฎหมายภายใน

¹² Article 88 - 1 de la Constitution du 4 octobre 1958 : « La République participe à l'Union européenne constituée d'États qui ont choisi librement d'exercer en commun certaines de leurs compétences en vertu du traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne, tels qu'ils résultent du traité signé à Lisbonne le 13 décembre 2007 ».

นัยสำคัญทางนิติศาสตร์ของคำวินิจฉัยส่วนนี้คือ การประกาศว่า “หลักความเป็นกฎหมายสูงสุดของกฎหมายสหภาพยุโรป” (Primauté du droit de l’Union) มีใช้หลักการที่เบ็ดเสร็จเด็ดขาดเสมอไป หากกรณีใดที่การบังคับใช้กฎหมายยุโรปขัดแย้งหรือกระทบกระเทือนต่อ “เอกลักษณ์หรือข้อเรียกร้องสำคัญทางรัฐธรรมนูญ” (Exigences constitutionnelles) เช่น ความมั่นคงแห่งรัฐ หากปรากฏว่าระบบกฎหมายของสหภาพยุโรป มิได้มีกลไกการคุ้มครองหรือให้ความสำคัญกับเรื่องดังกล่าวในระดับที่ทัดเทียมกัน (Equivalent protection) กับที่รัฐธรรมนูญฝรั่งเศสได้วางมาตรฐานไว้แล้ว สภาแห่งรัฐย่อมมีอำนาจและหน้าที่ที่จะ “งดเว้นการบังคับใช้” (Écarter) กฎหมายยุโรปในส่วนนั้น เพื่อพิทักษ์ไว้ซึ่งคุณค่าสูงสุดของรัฐธรรมนูญแห่งชาติ

2.2 การปฏิเสธการตรวจสอบแบบ *Ultra Vires* เพื่อหลีกเลี่ยงสงครามตุลาการ

ประเด็นที่น่าสนใจที่สุดประการหนึ่งในคดีนี้ คือข้อเสนอของรัฐบาลฝรั่งเศสที่เชิญชวนให้สภาแห่งรัฐเดินตามรอยศาลรัฐธรรมนูญเยอรมัน (Bundesverfassungsgericht) ในคดี *Weiss* (2020)¹³ ที่ได้วินิจฉัยว่าศาลยุติธรรมแห่งสหภาพยุโรปกระทำการนอกเหนือขอบเขตอำนาจ (*Ultra vires*) โดยก้าวล่วงเข้าไปในแดนอำนาจของรัฐสมาชิก ซึ่งหากสภาแห่งรัฐยอมรับข้อเสนอนี้ จะเท่ากับเป็นการประกาศสงครามทางกฎหมายอย่างเปิดเผยกับศาลยุติธรรมแห่งสหภาพยุโรป อย่างไรก็ตาม M. Alexandre Lallet ตุลาการผู้แถลงคดี ได้เสนอแนะให้สภาแห่งรัฐหลีกเลี่ยงหนทางแห่งความขัดแย้งดังกล่าว โดยชี้ให้เห็นว่าการตรวจสอบว่าศาลยุติธรรมแห่งสหภาพยุโรปทำเกินหน้าที่หรือไม่นั้นมีใช้หน้าที่ของศาลปกครอง การประกาศตัดขาดอำนาจศาลยุติธรรมแห่งสหภาพยุโรปจะนำไปสู่ความระส่ำระสายของระบบกฎหมายและความไม่แน่นอนชัดเจนในนิติฐานะ (Insécurité juridique) ซึ่งจะทำลายเอกภาพของกฎหมายสหภาพยุโรปในระยะยาว

หลังจากรับฟังพยานหลักฐาน เหตุผลของคู่กรณีและรวมถึงคำแถลงของตุลาการผู้แถลงคดีแล้ว สภาแห่งรัฐจึงตัดสินใจปฏิเสธที่จะใช้อำนาจตรวจสอบแบบ *Ultra vires* โดยยืนยันว่าศาลปกครองไม่มีอำนาจไปตรวจสอบความชอบด้วยกฎหมายของคำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรป เป็นการเลือกแนวทางการทูตที่ประนีประนอมแต่ยังคงรักษาเป้าหมายในการปกป้องผลประโยชน์แห่งชาติไว้ได้ นี่คือการ “รักษาน้ำ” ให้ทั้งสองฝ่าย ทั้งสหภาพยุโรปและประเทศฝรั่งเศส มากกว่าการยอมแพ้หรือการหลีกเลี่ยงสงครามเพียงอย่างเดียว แต่เป็นการวางเกมอำนาจใหม่ทางกฎหมาย¹⁴

¹³ BVerfG, Urteil des Zweiten Senats vom 5. Mai 2020 - 2 BvR 859/15 - (Weiss / PSPP).

¹⁴ M.-C. de Montecler, « Conservation des données : la guerre des juges n’aura pas lieu », *Dalloz actualité*, 26 avril 2021, [en ligne], disponible sur : <https://www.dalloz-actualite.fr/flash/conservation-des-donnees-guerre-des-juges-n-aura-pas-lieu>.

2.3 เทคนิคการตีความกฎหมายเชิงยุทธศาสตร์เพื่อคุ้มครองความมั่นคง

สภาแห่งรัฐได้เลือกใช้นิติวิธีที่ซับซ้อนกว่าการปฏิเสธหักดิบแบบเยอรมัน คือการนำ “มาตรการปกป้อง” (Clause de sauvegarde) หรือที่รู้จักกันในชื่อ “หลัก Arcelor” มาปรับใช้ในบริบทใหม่¹⁵ โดยกลไกนี้ทำงานโดยการตรวจสอบสองขั้นตอน คือ 1) การตรวจสอบระดับของกลไกป้องกันสิทธิ (Contrôle de l'équivalence des protections) โดยศาลจะตรวจสอบว่ากฎหมายของสหภาพยุโรปมีกลไกการคุ้มครองสิทธิหรือหลักการที่เทียบเท่ากับรัฐธรรมนูญฝรั่งเศสหรือไม่ และ 2) การตีความประสานประโยชน์ (Interprétation conciliatrice) หากพบว่ากฎหมายของสหภาพยุโรปอาจขัดแย้งกับรัฐธรรมนูญ ศาลจะไม่สั่งเพิกถอนกฎหมายของสหภาพยุโรปทันที แต่จะพยายามตีความกฎหมายของสหภาพยุโรปไปในทิศทางที่สอดคล้องกับข้อเรียกร้องสำคัญทางรัฐธรรมนูญมากที่สุด

ในคดีนี้ สภาแห่งรัฐได้ใช้ศิลปะแห่งการตีความกฎหมายอย่างชาญฉลาดโดยนำข้อยกเว้นที่ศาลยุติธรรมแห่งสหภาพยุโรปเปิดช่องไว้เพียงเล็กน้อยเรื่องความมั่นคงแห่งชาติ (Sécurité nationale) มาขยายความให้ครอบคลุมบริบทของฝรั่งเศส โดยวินิจฉัยว่า การต่อต้านการก่อการร้ายและการจารกรรม ถือเป็นภัยคุกคามร้ายแรง (Menace grave) ที่เกิดขึ้นจริงและเป็นปัจจุบัน ดังนั้นรัฐจึงสามารถใช้อำนาจตามข้อยกเว้นของกฎหมายของสหภาพยุโรป ในการสั่งให้ผู้ให้บริการจัดเก็บข้อมูลแบบทั่วไปและไม่เจาะจงต่อไปได้โดยไม่ขัดต่อกฎหมายของสหภาพยุโรป ผลลัพธ์ของนิติวิธีนี้คือการรักษาสถานะเดิม (Statu quo) ของระบบการจัดเก็บข้อมูลเพื่อความมั่นคงของฝรั่งเศสเอาไว้ได้เกือบทั้งหมด โดยไม่ต้องประกาศสงครามกับสหภาพยุโรปและไม่ต้องแก้รัฐธรรมนูญ เป็นชัยชนะของนักกฎหมายมหาชนฝรั่งเศสที่ผสมผสานสองหลักการที่ดูเหมือนจะขัดแย้งกันเข้ากับความเป็นทางปฏิบัติได้อย่างลงตัว

¹⁵ ชื่อของหลักการนี้มีได้เป็นศัพท์กฎหมายเทคนิคแต่มีที่มาจากชื่อคู่ความในคดีประวัติศาสตร์ของสภาแห่งรัฐ คือคำวินิจฉัยเมื่อวันที่ 8 กุมภาพันธ์ 2007 คดี Société Arcelor Atlantique et Lorraine ซึ่งในขณะนั้นเป็นคดีที่บริษัทเหล็ก อาร์เซลอร์ (Arcelor) และบริษัทย่อยฟ้องเพิกถอนกฎหมายที่กำหนดโควตาการปล่อยก๊าซเรือนกระจก โดยอ้างว่าขัดต่อหลักความเสมอภาคในรัฐธรรมนูญ, โปรดดู CE, Ass., 8 février 2007, Société Arcelor Atlantique et Lorraine et autres, n° 287110 และดูบทวิเคราะห์ความสำคัญของคดี (Analyse) ได้ที่ Conseil d'État, « Conseil d'État, 8 février 2007, Société Arcelor Atlantique et Lorraine et autres, Articulation entre l'ordre juridique national et celui de l'Union européenne », [en ligne], disponible sur : <https://www.conseil-etat.fr/decisions-de-justice/jurisprudence/les-grandes-decisions-depuis-1873/conseil-d-etat-8-fevrier-2007-societe-arcelor-atlantique-et-lorraine-et-autres>.

บทที่ 3 การจำแนกประเภทข้อมูลและการตรวจสอบภายใต้วิธีแบบ “Solange”

ภายหลังจากที่สภาแห่งรัฐได้ยืนยันหลักความเป็นกฎหมายสูงสุดของรัฐธรรมนูญแล้ว ขั้นตอนต่อไปคือการสร้างกลไกทางกฎหมายเพื่อรองรับการทำงานของเจ้าหน้าที่ บทนี้จะเจาะลึกถึงนิติวิธีอันชาญฉลาดที่ตุลาการแถลงคดี (Rapporteur public) ได้เสนอแนะต่อสภาแห่งรัฐ โดยเปรียบเทียบว่าเป็น “หลักโซลางเงอในแบบฉบับของเราเอง” (Votre jurisprudence « solange » à vous) ชื่อเรียกนี้เป็นการยืมถ้อยคำมาจากแนวคำวินิจฉัยระดับตำนานของศาลรัฐธรรมนูญเยอรมัน (Bundesverfassungsgericht) ในคดี *Solange I* (1974) ซึ่งศาลเยอรมันได้วางหลักการยอมรับอย่างมีเงื่อนไขโดยประกาศว่าจะยอมลดราวาศอกให้กฎหมายประชาคมยุโรปก็ต่อเมื่อและ “ตราบเท่าที่” (Solange) ประชาคมยุโรปยังคงรักษามาตรฐานการคุ้มครองสิทธิขั้นพื้นฐานไว้ได้¹⁶ คำว่า “Solange” ในบริบทของคดีฝรั่งเศสนี้ จึงถูกนำมาปรับใช้เพื่อแก้ปัญหาภาวะกลืนไม่เข้าคายไม่ออกในลักษณะเดียวกัน กล่าวคือ สภาแห่งรัฐเลือกที่จะยอมรับข้อจำกัดของกฎหมายสหภาพยุโรป “ตราบเท่าที่” (Aussi longtemps que) ประเทศฝรั่งเศสยังคงเผชิญกับภัยคุกคามร้ายแรงต่อความมั่นคงแห่งชาติ เช่น การก่อการร้าย นิติวิธีนี้ตั้งอยู่บนสมมติฐานเชิงปฏิบัติการที่ว่า “ตราบเท่าที่” ภัยคุกคามยังดำรงอยู่ รัฐย่อมมีความชอบธรรมที่จะสั่งให้เก็บรักษาข้อมูลไว้ใน “คลังข้อมูลดิบขนาดใหญ่” (Lac de données) เพื่อความมั่นคง ซึ่งเปรียบเสมือนทะเลสาบข้อมูลที่กักเก็บข้อมูลจรรยาบรรณทั้งหมดของประชาชนไว้อย่างไม่จำกัด รวมทั้งทุกอย่างไว้ในที่เดียวโดยยังไม่ได้คัดแยก และเมื่อข้อมูลเหล่านี้มีอยู่จริง เจ้าหน้าที่ตำรวจย่อมสามารถเข้าถึงข้อมูลดังกล่าวเพื่อนำไปใช้ในการปราบปรามอาชญากรรมทั่วไปได้ผ่านการเก็บรักษาแบบเร่งด่วน (Quick freeze) โดยถือว่าข้อเรียกร้องทางรัฐธรรมนูญในการรักษาความสงบเรียบร้อย ยังคงได้รับการตอบสนอง ตราบเท่าที่เงื่อนไขแห่งภัยคุกคามนี้ยังไม่หมดไป วิธีการนี้คือการซื้อเวลา และการบริหารความเสี่ยงทางกฎหมาย โดยไม่ต้องประกาศแตกหักกับศาลยุติธรรมแห่งสหภาพยุโรปในทันที แต่ใช้วิธีเกาะเกี่ยวเงื่อนไขสถานการณ์ปัจจุบันเพื่อรักษาสถานะเดิม (*Statu quo*) ของระบบการข่าวกรองเอาไว้

¹⁶ หลักการนี้มีที่มาจากคำวินิจฉัยศาลรัฐธรรมนูญแห่งสหพันธ์รัฐเยอรมนี (Bundesverfassungsgericht) ในคดี Internationale Handelsgesellschaft mbH หรือที่รู้จักกันโดยทั่วไปในชื่อคดี Solange I ซึ่งศาลได้วางหลักว่า ศาลรัฐธรรมนูญเยอรมันจะยังคงไว้ซึ่งอำนาจในการตรวจสอบกฎหมายประชาคมยุโรปว่าขัดต่อสิทธิขั้นพื้นฐานตามรัฐธรรมนูญเยอรมันหรือไม่ “ตราบเท่าที่” (Solange) ประชาคมยุโรปยังไม่มีมาตรฐานการคุ้มครองสิทธิขั้นพื้นฐานที่เพียงพอและทัดเทียมกับรัฐธรรมนูญเยอรมัน โปรดดู BVerfGE 37, 271 (280) - Solange I.

3.1 การนิยามความมั่นคงแห่งชาติและภัยคุกคามร้ายแรง

หัวใจสำคัญของการฝ่าทางตันในคดีนี้อยู่ที่การตีความข้อยกเว้นเรื่องความมั่นคงแห่งชาติที่ศาลยุติธรรมแห่งสหภาพยุโรปเปิดช่องไว้เพียงน้อยนิด โดยสภาแห่งรัฐได้ขยายความให้สอดคล้องกับบริบทความเป็นจริงของฝรั่งเศส ดังนี้ 1) *ขอบเขตของความมั่นคงแห่งชาติ* สภาแห่งรัฐยืนยันว่าการกิจในการปกป้องผลประโยชน์พื้นฐานของชาติ ตามที่ระบุไว้ในมาตรา L. 811 - 3 ของประมวลกฎหมายความมั่นคงภายใน (Code de la sécurité intérieure (CSI)) ล้วนจัดอยู่ในนิยามของ “ความมั่นคงแห่งชาติ” ตามความหมายของกฎหมายของสหภาพยุโรป ทั้งสิ้น ซึ่งรวมถึงการปกป้องเอกราชและบูรณภาพแห่งดินแดน การป้องกันการก่อการร้าย การต่อต้านการจารกรรมและการแทรกแซงจากต่างชาติ การปกป้องความสงบเรียบร้อยจากกลุ่มความรุนแรงสุดโต่ง¹⁷ 2) *สถานะของภัยคุกคาม* ศาลยอมรับข้อเท็จจริงที่รัฐบาลนำเสนอว่าฝรั่งเศสกำลังเผชิญกับภัยคุกคามร้ายแรง (Menace grave) ที่เกิดขึ้นจริง เป็นปัจจุบัน และคาดการณ์ได้ โดยอ้างอิงสถิติเหตุการณ์ก่อการร้ายในปี 2020 ที่มีการโจมตีสำเร็จถึง 6 ครั้ง และถูกยับยั้งได้ 2 ครั้ง รวมถึงสถานการณ์ประกาศเตือนภัยระดับสูงที่บังคับใช้อย่างต่อเนื่อง

ด้วยเหตุผลดังกล่าว สภาแห่งรัฐจึงวินิจฉัยว่า รัฐบาลมีความชอบธรรมทางกฎหมายที่จะคงคำสั่งให้ผู้ให้บริการจัดเก็บข้อมูลแบบทั่วไปและไม่เจาะจงของข้อมูลจราจรและข้อมูลระบุตำแหน่งต่อไปได้ เพื่อวัตถุประสงค์ในการรักษาความมั่นคงแห่งชาติ “ตราบเท่าที่” ภัยคุกคามดังกล่าวยังคงดำรงอยู่ อย่างไรก็ตาม เพื่อให้สอดคล้องกับมาตรฐานของศาลยุติธรรมแห่งสหภาพยุโรป สภาแห่งรัฐได้สั่งให้รัฐบาลต้องปรับแก้กฎหมายให้มีการทบทวนสถานการณ์ภัยคุกคามเป็นระยะ (Réexamen périodique) อย่างสม่ำเสมอ แทนที่จะปล่อยให้เป็นการถาวรโดยอัตโนมัติ

เพื่อให้เข้าใจถึงนัยทางยุทธศาสตร์ของข้อเสนอนี้ได้ดียิ่งขึ้น จำเป็นต้องวิเคราะห์เปรียบเทียบเพื่อเห็นความแตกต่างระหว่าง “หลักโซลางเงอ” (Solange) ในต้นฉบับของเยอรมันกับ “หลักโซลางเงอบัฝรั่งเศส” ที่ถูกประดิษฐ์ขึ้นใหม่ในคดีนี้ เมื่อพิจารณาว่า “หลักโซลางเงอ” ของศาลรัฐธรรมนูญเยอรมัน คือการประกาศจุดยืนเพื่อปกป้อง “สิทธิขั้นพื้นฐาน” โดยวางเงื่อนไขว่าเยอรมนีจะยอมรับอำนาจของกฎหมายสหภาพยุโรปก็ต่อเมื่อและ “ตราบเท่าที่” สหภาพยุโรปยังคงรักษามาตรฐานการคุ้มครองสิทธิมนุษยชนไว้อย่างดีพอ สิ่งที่ตุลาการผู้แถลงคดีนำเสนอต่อสภาแห่งรัฐ

¹⁷ Article L. 811 - 3 du Code de la sécurité intérieure : « ... les services spécialisés de renseignement peuvent recourir... au recueil des renseignements relatifs à la défense et à la promotion des intérêts fondamentaux de la Nation suivants : 1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ; 2°... la prévention de toute forme d'ingérence étrangère ; ... 4° La prévention du terrorisme ; 5° La prévention : ... c) Des violences collectives de nature à porter gravement atteinte à la paix publique... ».

ในคดีนี้ กลับเป็นการพลิกแพลงหลักการดังกล่าวมาใช้เพื่อปกป้องอำนาจอรัฐและความมั่นคงแทน โดยวางเงื่อนไขบนฐานของข้อเท็จจริงมากกว่าบรรทัดฐานทางกฎหมาย กล่าวคือ ประเทศฝรั่งเศส จะยอมรับสภาพการจำกัดสิทธิและคงไว้ซึ่งระบบการจัดเก็บข้อมูลแบบเหมาแข่งได้ “ตราบเท่าที่” ประเทศยังคงเผชิญกับสถานการณ์ภัยคุกคามร้ายแรงจากการก่อการร้ายอยู่เท่านั้น

นิติวิธีเช่นนี้ แม้ผู้แถลงคดีจะยอมรับอย่างตรงไปตรงมาว่าเป็นวิธีแก้ปัญหามี ความเปราะบาง (Précarité) เพราะความชอบธรรมทางกฎหมายของระบบการจัดเก็บข้อมูลจะดำรง อยู่ได้ก็เพียงแค่วาระเวลาที่ยังมีภัยคุกคามดำรงอยู่จริงเท่านั้น หากวันใดที่คลังข้อมูลดิบขนาดใหญ่ หมดลงไปหรือภัยคุกคามหมดสิ้นไป ความชอบธรรมในการจัดเก็บข้อมูลลักษณะนี้ย่อมสิ้นสุดลงด้วย ทว่าในมุมมองเชิงปฏิบัติการ นี่คือทางออกที่สมเหตุสมผลที่สุดในการ “ซื้อเวลา” และบริหารความเสี่ยง เพื่อให้รัฐธรรมนูญยังคงทำงานได้ตามกลางวิกฤต โดยไม่ต้องเลือกระหว่างการละเมิดกฎหมายยุโรป หรือการปล่อยให้ประเทศไร้ทางสู้ ยุทธวิธีนี้จึงเปรียบเสมือนการสร้างหลักโฆลาเงอในแบบฉบับของ ฝรั่งเศสเอง (Votre jurisprudence « solange » à vous) ที่เน้นความยืดหยุ่นตามสถานการณ์จริง มากกว่าการยึดติดกับทฤษฎีที่ตายตัว

ตารางที่ 1 ตารางเปรียบเทียบวิวัฒนาการจาก Solange เยอรมัน สู่ Solange ฝรั่งเศส¹⁸

เกณฑ์ การเปรียบเทียบ	หลัก Solange แบบเยอรมัน (Original) (คดี Solange I ปี 1974)	หลัก Solange แบบฝรั่งเศส (New/Adapted) (คดี French Data Network ปี 2021)
1. ผู้สร้างนวัตกรรม	ศาลรัฐธรรมนูญแห่งสหพันธ์รัฐเยอรมนี (Bundesverfassungsgericht)	สภาแห่งรัฐฝรั่งเศส (Conseil d'État) ตามคำเสนอของตุลาการ แถลงคดี
2. วัตถุประสงค์หลัก	เพื่อปกป้อง “สิทธิขั้นพื้นฐาน” (กลัว EU ละเมิดสิทธิประชาชน)	เพื่อปกป้อง “ความมั่นคงแห่งรัฐ” (กลัว EU เข้มงวดเรื่องสิทธิฯ จนรัฐ ทำงานไม่ได้)
3. เงื่อนไข “ตราบเท่าที่” (Solange/As long as)	จะไม่ยอมรับอำนาจกฎหมาย EU ตราบ เท่าที่ EU ยังไม่มีมาตรฐานการคุ้มครอง สิทธิฯ ที่ดีพอ	จะไม่ยอมรับข้อห้ามของศาล EU ตราบเท่าที่ ฝรั่งเศสยังเผชิญกับ ภัยคุกคามความมั่นคงร้ายแรง

¹⁸ ตารางที่ 1 จัดทำโดยอานันท์ กระบวนศรี.

เกณฑ์ การเปรียบเทียบ	หลัก Solange แบบเยอรมัน (Original) (คดี Solange I ปี 1974)	หลัก Solange แบบฝรั่งเศส (New/Adapted) (คดี French Data Network ปี 2021)
4. ฐานของเงื่อนไข	เชิงโครงสร้าง/สถาบัน (Structural) เรียกร้องให้ EU มีรัฐสภาและกฎหมาย สิทธิฯ	เชิงข้อเท็จจริง/สถานการณ์ (Factual) อ้างอิงสถานการณ์ ก่อการร้ายที่เป็นอยู่ในปัจจุบัน
5. ความยั่งยืนของ หลักการ	ค่อนข้างถาวรจนกว่าโครงสร้างของ EU จะเปลี่ยนแปลง (ซึ่งต่อมาเปลี่ยนใน Solange II)	เปราะบาง/ชั่วคราว (Précaire) ดำรงอยู่ได้เฉพาะช่วงเวลาที่มียก คุกคาม (คลังข้อมูลดิบขนาดใหญ่ ยังไม่หมดลง) เท่านั้น
6. ผลลัพธ์ทาง กฎหมาย	การตั้งการ์ดสูง (Defensive): ศาล เยอรมันสงวนอำนาจในการตรวจสอบ ความชอบด้วยรัฐธรรมนูญของกฎหมาย EU	การซื้อเวลา (Pragmatic): รัฐบาล ฝรั่งเศสสามารถกระบบการจัด เก็บข้อมูลแบบเหมาเช่า (<i>Statu quo</i>) ไว้ได้ต่อไป

อย่างไรก็ตาม นิติวิธีของสภาแห่งรัฐในการตีความคำวินิจฉัยของศาลยุติธรรมแห่งสหภาพยุโรปก็มิได้รอดพ้นจากการถูกวิพากษ์วิจารณ์ในทางวิชาการ มีความเห็นที่น่าสนใจระบุน่าว่าการที่สภาแห่งรัฐพยายามอธิบายว่ามาตรการของตนสอดคล้องกับข้อยกเว้นของศาลยุติธรรมแห่งสหภาพยุโรปนั้น อาจเปรียบได้กับการแกล้งทำเป็นไม่เข้าใจ (*Fait semblant de ne pas avoir compris*) ถึงเจตนารมณ์ที่แท้จริงของศาลยุติธรรมแห่งสหภาพยุโรปที่ต้องการจำกัดข้อยกเว้นเรื่องความมั่นคงให้แคบที่สุด¹⁹ “ตราบเท่าที่” มีภัยคุกคามเท่านั้น ไม่ใช่ “ตราบนานเท่านั้น” แต่อย่างไรก็ตาม เปรียบเสมือนการ “เล่นแร่แปรธาตุ” หรือ “มายากล” ที่แสดงให้เห็นว่าประเทศฝรั่งเศสเคารพกฎหมายของสหภาพยุโรปแค่เพียงในนาม แต่แท้จริงแล้วไม่ได้นำแนวทางจากคดี *Quadrature du Net* มาใช้ในเนื้อหาอย่างเต็มที่²⁰

¹⁹ X. Dupré de Boulois (coord.), « Les grands arrêts du droit des libertés fondamentales », (Daloz, 5e éd., 2025), 261 - 262.

²⁰ Brunessen Bertrand, « L'arrêt French Data Network du Conseil d'Etat : un dialogue des juges en trompe l'œil », Le Club des juristes, 7 mai 2021, [en ligne], disponible sur : <https://www.leclubdesjuristes.com/archives-cdj/larret-french-data-network-du-conseil-detat-un-dialogue-des-juges-en-trompe-loeil-3538/>.

ประเด็นที่น่ากังวลยิ่งกว่าคือ คำวินิจฉัยของสภาแห่งรัฐในปี 2021 มิได้เป็นเพียงการแก้ไขปัญหาคือกฎหมายเฉพาะหน้า แต่กลับกลายเป็นการเปิดประตูบานใหญ่ให้ฝ่ายนิติบัญญัติอาศัยโอกาสนี้ขยายขอบเขตอำนาจรัฐให้กว้างขวางยิ่งขึ้น เห็นได้ชัดจากการตรากฎหมายในปี ค.ศ. 2024 ซึ่งได้แก้ไขมาตรา L. 851 - 3 โดยขยายวัตถุประสงค์ของการใช้อัลกอริทึมจากการจำกัดเฉพาะเรื่อง “การก่อการร้าย” ไปสู่เรื่อง “การป้องกันประเทศ” และ “การแทรกแซงจากต่างชาติ” ซึ่งเป็นการตอกย้ำข้อวิจารณ์ที่ว่า เมื่อช้อยกเว้นความมั่นคงได้รับการยอมรับจากตุลาการแล้ว มันย่อมมีแนวโน้มที่จะถูกขยายขอบเขตออกไป²¹ อย่างไรก็ตาม พลวัตของการขยายอำนาจนี้มีได้มีลักษณะเบ็ดเสร็จถาวร แต่กลับสะท้อนถึงสภาวะการต้อรองที่ไม่หยุดนิ่งระหว่างความมั่นคงกับสิทธิมนุษยชน เห็นได้จากบทบัญญัติในกฎหมายฉบับเดียวกันที่กำหนดเงื่อนไขเวลาสิ้นสุดไว้ โดยอำนาจพิเศษที่ขยายออกไปนี้จะมีผลบังคับใช้ชั่วคราวและจะหวนกลับไปสู่มาตรฐานเดิมที่จำกัดเฉพาะเรื่องการก่อการร้ายตั้งแต่วันที่ 1 กรกฎาคม 2028 เป็นต้นไป²² นอกจากนี้ ยังปรากฏบทบาทของคณะตุลาการรัฐธรรมนูญในการปฏิบัติหน้าที่เป็นผู้พิทักษ์สิทธิเสรีภาพของประชาชนในปี 2025 คณะตุลาการรัฐธรรมนูญฝรั่งเศสได้มีคำวินิจฉัยเพิกถอนความพยายามของรัฐที่จะจัดเก็บข้อมูลที่อยู่เว็บไซต์ (URL) อย่างละเอียด²³ ซึ่งชี้ให้เห็นว่า แม้ในยุคที่ความมั่นคงเฟื่องฟู เส้นแบ่งทางรัฐธรรมนูญบางประการกับการคุ้มครองสิทธิในความเป็นส่วนตัวในข้อมูลที่สามารถสะท้อนถึงพฤติกรรมหรือแม้กระทั่งความนึกคิดภายในจิตใจของประชาชนก็ยังคงเป็นเขตหวงห้ามที่รัฐไม่อาจล่วงละเมิดได้

²¹ Article L. 851 - 3, I du Code de la sécurité intérieure (Version en vigueur du 27 juillet 2024 au 01 juillet 2028) : « ...destinés [...] à détecter des connexions susceptibles de révéler des ingérences étrangères, des menaces pour la défense nationale ou des menaces terroristes. ».

²² Article L. 851 - 3, I du Code de la sécurité intérieure (Version en vigueur à partir du 01 juillet 2028) : « ...pour les seuls besoins de la prévention du terrorisme [...] destinés [...] à détecter des connexions susceptibles de révéler une menace terroriste. ».

²³ คณะตุลาการรัฐธรรมนูญฝรั่งเศสได้วางหลักประกันสำคัญเพิ่มเติมเกี่ยวกับขอบเขตของข้อมูลที่สามารถนำมาใช้ในการประมวลผลตามมาตรา L. 851 - 3 โดยวินิจฉัยว่าบทบัญญัติที่อนุญาตให้เข้าถึงและจัดเก็บที่อยู่เว็บไซต์ฉบับเต็ม (Adresses complètes de ressources utilisées sur internet หรือ URL) นั้น ขัดต่อรัฐธรรมนูญเนื่องจาก URL ในทางเทคนิคปัจจุบันสามารถสะท้อนถึงเนื้อหาของการสื่อสารหรือพฤติกรรมการสืบค้นข้อมูลในระดับที่กระทบต่อสิทธิในความเป็นส่วนตัวอย่างรุนแรงเกินความจำเป็น (Disproportionate) อันเป็นการล่วงละเมิดต่อหลักความไม่ละเมิดได้ของสิทธิพื้นฐาน โปรดดู Cons. const., 12 juin 2025, n° 2025-885 DC, Loi visant à sortir la France du piège du narcotrafic.

3.2 การจำแนกเลขที่อยู่ไอพีและการเก็บรักษาแบบเร่งด่วน

สำหรับประเด็นการปราบปรามอาชญากรรมทั่วไปที่มีใช้การก่อการร้าย ซึ่งศาลยุติธรรมแห่งสหภาพยุโรปวางหลักห้ามมิให้รัฐจัดเก็บข้อมูลแบบหว่านแหไว้ล่วงหน้า นั้น สภาแห่งรัฐได้ใช้วิธีการในการจำแนกประเภทข้อมูลเพื่อหาทางออก โดยเริ่มต้นจากการกำหนดสถานะพิเศษให้กับเลขที่อยู่ไอพี (Adresses IP) สภาแห่งรัฐวินิจฉัยสอดคล้องกับแนวทางของศาลยุติธรรมแห่งสหภาพยุโรปว่า ข้อมูลประเภทเลขที่อยู่ไอพีนั้นมีความละเอียดอ่อนน้อยกว่าข้อมูลจราจรประเภทอื่น ๆ เนื่องจากถ้าเพียงตัวเลขไอพีไม่สามารถเปิดเผยข้อมูลคู่สนทนาหรือระบุตำแหน่งที่อยู่ได้อย่างแม่นยำเท่ากับข้อมูลโทรศัพท์ แต่ในขณะเดียวกัน ข้อมูลนี้ก็กลับมีความจำเป็นอย่างยิ่งในการระบุตัวต้นผู้กระทำความผิดในโลกออนไลน์ โดยเฉพาะในกรณีอาชญากรรมทางเทคโนโลยีหรือสื่อลามกอนาจารเด็ก ด้วยเหตุผลดังกล่าว รัฐจึงยังคงมีอำนาจในการบังคับให้ผู้ให้บริการจัดเก็บข้อมูลเลขที่อยู่ไอพีของประชาชนทุกคนแบบเป็นการทั่วไปได้ เพื่อใช้เป็นฐานข้อมูลในการปราบปรามอาชญากรรมร้ายแรงและป้องกันภัยคุกคามต่อความสงบเรียบร้อย โดยไม่จำเป็นต้องรอให้เกิดเหตุขึ้นก่อน

ในส่วนของคุณข้อมูลจราจรประเภทอื่น ๆ อาทิ ประวัติการโทรหรือข้อมูลระบุเสาสัญญาณ ซึ่งศาลยุติธรรมแห่งสหภาพยุโรปห้ามมิให้เก็บสะสมไว้ล่วงหน้า นั้น สภาแห่งรัฐได้นำกลไกการเก็บรักษาแบบเร่งด่วน (Quick Freeze) มาใช้เป็นทางเลือกในการแก้ปัญหา หลักการทำงานของกลไกนี้คือ เมื่อเจ้าหน้าที่ตำรวจหรือหน่วยงานรัฐมีเหตุสงสัยว่ามีการกระทำความผิดเกิดขึ้น ก็สามารถออกคำสั่งไปยังผู้ให้บริการเพื่อทำการ “แช่แข็ง” ข้อมูลของผู้ต้องสงสัยและบุคคลที่เกี่ยวข้องไว้ทันที เพื่อป้องกันมิให้ข้อมูลเหล่านั้นถูกลบทำลายตามวงจรปกติ และสามารถนำมาใช้เป็นพยานหลักฐานในการสืบสวนสอบสวนได้ทันที ความแยบยลของวิธีนี้นี้อยู่ที่กลไกในทางปฏิบัติ กล่าวคือ แม้มาตรการการเก็บรักษาแบบเร่งด่วนจะดูเหมือนเป็นมาตรการเฉพาะหน้าที่จะเริ่มเก็บข้อมูลเมื่อมีเหตุสงสัยเท่านั้น แต่ในความเป็นจริงแล้ว กลไกนี้ทำงานโดยการผนวกเข้ากับอำนาจที่รัฐสั่งให้เก็บข้อมูลเพื่อความมั่นคงแห่งชาติไว้อยู่แล้ว

นัยประการสำคัญของวิธีนี้ดังกล่าว เปรียบได้กับ “กระบวนการแปลงรูปทางกฎหมายเพื่อรักษาสถานะเดิม” กล่าวคือ แม้ในทางหลักการศาลยุติธรรมแห่งสหภาพยุโรปจะมีคำวินิจฉัยห้ามมิให้รัฐจัดเก็บข้อมูลเป็นการทั่วไปเพื่อวัตถุประสงค์ในการปราบปรามอาชญากรรม แต่สภาแห่งรัฐได้เลือกที่จะปรับเปลี่ยน “ฐานอำนาจรองรับ” (Base légale) ของการจัดเก็บข้อมูลเสียใหม่ โดยย้ายฐานความชอบธรรมจากการอ้างเหตุผลด้านการปราบปรามอาชญากรรม (ซึ่งถูกห้าม) ไปสู่การอ้างเหตุผลด้าน “ความมั่นคงแห่งชาติ” (ซึ่งเป็นข้อยกเว้นที่กระทำได้) แทน

ผลสัมฤทธิ์ในทางปฏิบัติคือ รัฐยังคงดำรงไว้ซึ่ง “คลังข้อมูลดิบขนาดใหญ่” (Lac de données) ที่กักเก็บข้อมูลจราจรของประชาชนทั้งหมดไว้อย่างต่อเนื่องเสมือนเดิม เพียงแต่เปลี่ยนฉลากกำกับวัตถุประสงค์เป็นเรื่องความมั่นคงแห่งชาติ ดังนั้น เมื่อเกิดคดีอาชญากรรมทั่วไปขึ้น

กลไก “การเก็บรักษาแบบเร่งด่วน” (Quick Freeze) จึงมิได้ทำหน้าที่เพียงแค่เริ่มเก็บข้อมูล นับแต่มีเหตุสงสัยตามชื่อเรียก หากแต่ทำหน้าที่เป็นเสมือนท่อเชื่อมที่อนุญาตให้เจ้าหน้าที่สามารถ “ดึง” ข้อมูลย้อนหลังที่ถูกจัดเก็บสำรองไว้แล้วในถังข้อมูลความมั่นคง ออกมาใช้ประโยชน์ในการสืบสวน สอบสวนทางอาญาได้ภายใต้เงื่อนไขและการตรวจสอบที่กำหนด สภาแห่งรัฐพยายามสร้างเขตแดน ทางกฎหมายที่ศาลยุติธรรมแห่งสหภาพยุโรปเข้าไม่ถึง โดยอ้างสถานะความมั่นคงแห่งชาติเป็นเกราะกำบัง ซึ่งแท้จริงแล้วคือคลังข้อมูลดิบขนาดใหญ่คือแหล่งทรัพยากรสำคัญที่รัฐใช้สนับสนุน การสืบสวนสอบสวนคดีอาญาปกติ จึงเป็นการ “เลี้ยวบาลี” มาตรฐานของศาลยุติธรรมแห่ง สหภาพยุโรปที่ห้ามเก็บข้อมูลย้อนหลังในการสอบสวนคดีอาญาทั่วไป²⁴

ข้อสังเกตประการสำคัญคือ ความสำเร็จของโมเดลกลไกการเก็บรักษาแบบเร่งด่วน ในแบบฉบับของฝรั่งเศสนั้น แท้จริงแล้วคือการ “เกาะหลัง” อำนาจการจัดเก็บข้อมูลเพื่อความมั่นคง แห่งชาติอยู่นั่นเอง หากปราศจากข้ออ้างเรื่องความมั่นคงแห่งชาติที่อนุญาตให้เข้าถึงข้อมูลรวมศูนย์ อยู่ก่อนแล้ว ระบบกลไกการเก็บรักษาแบบเร่งด่วนสำหรับอาชญากรรมทั่วไปอาจล้มเหลวในการสืบสวน หายานหลักฐานสำหรับคดีที่เกิดขึ้นในอดีต ประเด็นนี้จึงเป็นกุญแจสำคัญที่ไขคำตอบว่า เหตุใด สภาแห่งรัฐจึงต้องพยายามรักษาหลักการจัดเก็บข้อมูลเพื่อความมั่นคงแห่งชาติไว้อย่างสุดชีวิต เพราะมันคือฐานรากที่ค้ำจุนระบบการสืบสวนสอบสวนทั้งหมดของประเทศไว้นั่นเอง

3.3 บทบาทใหม่ของคณะกรรมการควบคุมเทคนิคการข่าวกรองแห่งชาติ

ประเด็นสุดท้ายที่สภาแห่งรัฐจำเป็นต้องจัดการเพื่อสร้างความชอบธรรมให้แก่ระบบ การจัดเก็บข้อมูล คือการแก้ไขความบกพร่องของกลไกการตรวจสอบการใช้อำนาจรัฐ ซึ่งศาลยุติธรรม แห่งสหภาพยุโรปได้กำหนดมาตรฐานไว้ในระดับที่สูงมาก โดยวางหลักการว่าการเข้าถึงข้อมูลส่วนบุคคล ของประชาชนจะต้องผ่านขั้นตอนการตรวจสอบล่วงหน้า (Contrôle préalable) โดยองค์กรอิสระ ที่มีอำนาจผูกพันทางกฎหมาย (Effet contraignant) อย่างเคร่งครัด ซึ่งจากการพิจารณาข้อกฎหมาย ภายใน สภาแห่งรัฐยอมรับว่ากลไกปัจจุบันของฝรั่งเศสยังมีความล้าสมัยและไม่สอดคล้องกับมาตรฐาน ดังกล่าวในสองจุดสำคัญ

ประการแรก คือ ปัญหาเรื่องสถานะและอำนาจของคณะกรรมการควบคุมเทคนิค การข่าวกรองแห่งชาติ หรือ CNCTR ซึ่งในปัจจุบันมีอำนาจเพียงแค่การให้ความเห็น (Avis) เท่านั้น ซึ่งไม่มีผลผูกพันทางกฎหมาย ส่งผลให้นายกรัฐมนตรีในฐานะหัวหน้าฝ่ายบริหารยังคงไว้ซึ่งอำนาจ ที่จะสั่งการฝ่าฝืนความเห็นของ CNCTR ได้ แม้ว่าในทางปฏิบัติจะไม่เคยปรากฏกรณีดังกล่าวก็ตาม เพื่อปิดช่องโหว่นี้ สภาแห่งรัฐจึงมีคำวินิจฉัยสั่งการให้รัฐบาลต้องดำเนินการแก้ไขกฎหมายหรือ

²⁴ AZOULAI, L. et RITLENG, D. « “L’État, c’est moi”. Le Conseil d’État, la sécurité et la conservation des données », Revue trimestrielle de droit européen (RTD eur.), 2021, pp. 349-374.

ระเบียบปฏิบัติที่เกี่ยวข้อง เพื่อยกระดับให้ความเห็นของ CNCTR มีผลผูกพันทางกฎหมาย หรือหากนายกรัฐมนตรีประสงค์จะฝ่าฝืนความเห็นดังกล่าว ก็จำเป็นต้องยื่นเรื่องให้สภาแห่งรัฐวินิจฉัยชี้ขาดก่อนการดำเนินการเสมอ เว้นแต่จะเป็นกรณีที่มีความจำเป็นเร่งด่วนที่สุดเท่านั้น

ประการที่สอง คือการควบคุมการใช้เทคนิคอัลกอริทึม (Technique de l'algorithme) หรือกล่องดำที่เป็นระบบประมวลผลอัตโนมัติ (Boîtes noires)²⁵ เพื่อตรวจจับพฤติกรรมต้องสงสัยที่อาจเกี่ยวเนื่องกับการก่อการร้ายตามมาตรา L. 851 - 3 ของประมวลกฎหมายความมั่นคงภายใน (CSI) สภาแห่งรัฐได้วางบรรทัดฐานว่า ขั้นตอนการระบุตัวตน (Identification) ของบุคคลที่ถูกระบบปัญญาประดิษฐ์แจ้งเตือนนั้น จะกระทำได้อีกต่อเมื่อผ่านการตรวจสอบจากคณะกรรมการควบคุมเทคนิคการข่าวกรองแห่งชาติ (Commission nationale de contrôle des techniques de renseignement) ซึ่งเป็นองค์กรอิสระก่อนเสมอ ทั้งนี้ เพื่อเป็นหลักประกันป้องกันมิให้เกิดการละเมิดสิทธิของผู้บริสุทธิ์จากความผิดพลาดของระบบอัลกอริทึม²⁶

คำวินิจฉัยในส่วนนี้ได้สะท้อนให้เห็นถึงความพยายามอันแน่วแน่ของสภาแห่งรัฐในการสร้างระบบคู่ขนานขึ้นมาในระบบกฎหมาย กล่าวคือ ในยามปกติ รัฐมีหน้าที่ต้องเคารพสิทธิส่วนบุคคลตามมาตรฐานของสหภาพยุโรปอย่างเคร่งครัด แต่ในยามวิกฤตที่ “ความมั่นคงแห่งชาติ” ถูกคุกคาม รัฐย่อมมีความชอบธรรมและอำนาจเต็มที่ในการใช้เครื่องมือดิจิทัลเพื่อปกป้องความปลอดภัยของสาธารณชน โดยมีสภาแห่งรัฐและ CNCTR ทำหน้าที่เสมือนผู้พิทักษ์ที่คอยตรวจสอบถ่วงดุลความสมดุลอย่างใกล้ชิด นิติวิธีเช่นนี้เปรียบได้กับการนำแนวคิดแบบ “Solange” ของศาลรัฐธรรมนูญเยอรมันมาปรับใช้ในบริบทของฝรั่งเศส นั่นคือการยอมรับอำนาจของกฎหมายยุโรป “ตราบเท่าที่” (As long as) การยอมรับนั้นไม่กระทบกระเทือนต่อความอยู่รอดและสาระสำคัญของชาติ

²⁵ คำว่า “กล่องดำ” (Boîtes noires) ในที่นี้ มิได้หมายถึงเพียงแค่อุปกรณ์บันทึกข้อมูลการบิน หากแต่เปรียบเปรยถึง “ความมืดบอด” ของกระบวนการตรวจสอบ กล่าวคือ รัฐได้นำอัลกอริทึมที่เป็นความลับไปติดตั้งไว้ในเครือข่ายอินเทอร์เน็ตเพื่อคัดกรองพฤติกรรมของประชาชน โดยที่ไม่มีใครล่วงรู้ได้ว่า “เงื่อนไข” ที่ AI ใช้ตัดสินว่าใครคือผู้ก่อการร้ายนั้นคืออะไร เปรียบเสมือนการนำโลกภาพยนตร์วิทยาศาสตร์เรื่อง Minority Report (2002) มาสู่โลกความเป็นจริง ที่ระบบคอมพิวเตอร์ทำหน้าที่ทำนายอาชญากรรมล่วงหน้าจากพฤติกรรมดิจิทัลของประชาชน.

²⁶ Article L. 851 - 3 du Code de la sécurité intérieure (Version en vigueur du 03 octobre 2015 au 31 juillet 2021) : « I. - [...] pour les seuls besoins de la prévention du terrorisme, il peut être imposé [...] la mise en œuvre [...] de traitements automatisés destinés [...] à détecter des connexions susceptibles de révéler une menace terroriste. Ces traitements [...] [s'effectuent] sans permettre l'identification des personnes [...]. IV. - Lorsque les traitements [...] détectent des données [...], le Premier ministre [...] peut autoriser, après avis de [...], l'identification de la ou des personnes concernées [...] ».

บทที่ 4 ดุลยภาพระหว่าง “ความมั่นคงแห่งชาติ” กับ “สิทธิเหนือข้อมูล” บทเรียนและนัยสำคัญต่อกฎหมายดิจิทัลของประเทศไทย

คำวินิจฉัยของสภาแห่งรัฐในคดี *French Data Network et autres* มิได้เป็นเพียงข้อยุติในข้อพิพาททางปกครองของประเทศฝรั่งเศสเท่านั้น หากแต่เป็นตำราความรู้ชั้นครูที่แสดงให้เห็นถึงศิลปะในการบริหารจัดการความขัดแย้งของบรรทัดฐานกฎหมายในยุคดิจิทัล สำหรับประเทศไทยซึ่งกำลังเผชิญกับความท้าทายในการบังคับใช้กฎหมายความมั่นคงไซเบอร์และกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ท่ามกลางกระแสการตื่นตัวเรื่องการคุ้มครองข้อมูลส่วนบุคคล (PDPA) บทเรียนจากคดีนี้จึงมีความสำคัญในฐานะบทเรียนสำคัญในการออกแบบโครงสร้างทางกฎหมายที่สมดุลและยั่งยืน ดังนี้

4.1 การเปลี่ยนผ่านจากการกวาดเก็บข้อมูลสู่การจำแนกความเข้มข้นของข้อมูล

ระบบกฎหมายไทยในปัจจุบันมักกำหนดหน้าที่ให้ผู้ให้บริการอินเทอร์เน็ตต้องจัดเก็บ “ข้อมูลจราจรคอมพิวเตอร์” (Log Files) ไว้เป็นระยะเวลาหนึ่ง เช่น 90 วัน โดยมีได้จำแนกประเภทของข้อมูลอย่างชัดเจน ซึ่งแตกต่างจากบรรทัดฐานใหม่ที่สภาแห่งรัฐฝรั่งเศสได้วางไว้ตามแนวทางของศาลยุติธรรมแห่งสหภาพยุโรป นัยสำคัญที่ประเทศไทยอาจนำมาปรับใช้คือ การจำแนกระดับความสำคัญของข้อมูล (*Hierarchisation des données*) ซึ่งจำแนกตามระดับผลกระทบต่อสิทธิความเป็นส่วนตัว ได้แก่

1) ข้อมูลระบุตัวตนทางแพ่ง (*Données d'identité civile*) เช่น ชื่อ - นามสกุล ที่อยู่ ข้อมูลการชำระเงิน เป็นข้อมูลที่มีความละเอียดอ่อนน้อยที่สุด รัฐอาจกำหนดให้จัดเก็บได้เป็นการทั่วไปเพื่อวัตถุประสงค์ในการป้องกันปราบปรามอาชญากรรมทั่วไป

2) ที่อยู่ไอพี (*Adresses IP*) แม้จะเป็นข้อมูลทางเทคนิค แต่มีความจำเป็นอย่างยิ่ง (*Strictelement nécessaire*) ในการระบุตัวผู้กระทำความผิดในโลกออนไลน์ สภาแห่งรัฐจึงยอมรับให้จัดเก็บได้ แต่ต้องจำกัดเฉพาะเพื่อการต่อสู้กับ “อาชญากรรมร้ายแรง” (*Criminalité grave*) หรือภัยคุกคามต่อความสงบเรียบร้อยเท่านั้น มิใช่สำหรับความผิดลหุโทษทุกประเภท

3) ข้อมูลจราจรและข้อมูลระบุตำแหน่ง (*Données relatives au trafic et de localisation*) ข้อมูลกลุ่มนี้มีความละเอียดอ่อนสูงกว่าสองระดับแรกอย่างมีนัยสำคัญ เนื่องจากสามารถนำมาประมวลผลเพื่อเปิดเผยวิถีชีวิต ความสัมพันธ์ส่วนตัว หรือแม้แต่ความเชื่อของบุคคลได้ กฎหมายไทยจึงควรพิจารณายกเลิกการบังคับเก็บข้อมูลส่วนนี้แบบเป็นการทั่วไปในสถานการณ์ปกติ โดยควรสงวนไว้ใช้เฉพาะในกรณีที่มีภัยคุกคามร้ายแรงต่อความมั่นคงแห่งชาติ หรือใช้ผ่านกลไกการเก็บรักษาแบบเร่งด่วนที่เจาะจงเฉพาะรายคดีตามคำสั่งของศาล

4) ข้อมูลที่อยู่ทรัพยากรบนอินเทอร์เน็ตฉบับเต็ม (*Adresses complètes de ressources utilisées sur internet หรือ URL*) ซึ่งถือเป็นข้อมูลที่มีความละเอียดอ่อนสูงสุดและ

เป็น “เขตหวงห้าม” ทางรัฐธรรมนูญ เนื่องจาก URL ในปัจจุบันมิได้ทำหน้าที่เพียงแค่บอกที่อยู่ของเว็บไซต์แต่ยังสะท้อนถึงเนื้อหา (Content) ที่ประชาชนกำลังสืบค้นหรืออ่านอยู่ ซึ่งเชื่อมโยงโดยตรงกับความรู้สึกนึกคิดภายในจิตใจและเสรีภาพในการรับรู้ข้อมูลข่าวสาร ดังที่คณะตุลาการรัฐธรรมนูญฝรั่งเศสได้วางบรรทัดฐานไว้ในปี ค.ศ. 2025 ว่าการให้อำนาจรัฐเข้าถึงข้อมูล URL ฉบับเต็มแบบเหมารวมนั้นเป็นการกระทบต่อสิทธิในความเป็นส่วนตัวอย่างรุนแรงจนไม่อาจยอมรับได้ ดังนั้น กฎหมายไทยจึงควรจำกัดการเข้าถึงข้อมูลระดับนี้ไว้ภายใต้มาตรฐานที่เข้มงวดสูงสุด หรืออาจกำหนดให้เป็นข้อมูลประเภทที่รัฐไม่อาจบังคับให้เก็บรักษาแบบทั่วไปได้เลย เพื่อป้องกันมิให้เทคโนโลยีถูกนำมาใช้ในลักษณะการทำนายความนึกคิดของพลเมืองจนเกินขอบเขตของนิติรัฐ

การจำแนกประเภทเช่นนี้ จะช่วยให้การจัดเก็บข้อมูลของไทยมีความได้สัดส่วน (Proportionnalité) และลดความเสี่ยงที่จะขัดต่อหลักการคุ้มครองข้อมูลส่วนบุคคลในระดับสากล เมื่อนำเกณฑ์การพิจารณาจากคำวินิจฉัยคดี *French Data Network* ของสภาแห่งรัฐฝรั่งเศสมาเป็นมาตรวัดกับระบบกฎหมายดิจิทัลของประเทศไทย จะพบช่องว่างทางกฎหมายที่มีนัยสำคัญอย่างยิ่ง โดยเฉพาะอย่างยิ่งเมื่อพิจารณาบทบัญญัติในมาตรา 26 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (และที่แก้ไขเพิ่มเติม) ซึ่งกำหนดหน้าที่ให้ผู้ให้บริการอินเทอร์เน็ตต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log Files) ไว้เป็นระยะเวลาไม่น้อยกว่าเก้าสิบวัน แต่อาจถูกขยายออกไปได้สูงสุดถึงสองปีตามคำสั่งของพนักงานเจ้าหน้าที่²⁷ กฎหมายไทยในส่วนนี้มีลักษณะเป็นการกวาดเก็บข้อมูลแบบเหมาเข่งที่ไม่ผ่านมาตรฐานในเชิงนิติวิธีตามมาตรฐานสากลในหลายประการ ประการแรกคือการขาดการจำแนกประเภทความเข้มข้นของข้อมูลโดยมาตรา 26 ของไทยมิได้แยกแยะความแตกต่างระหว่างข้อมูลทางเทคนิคที่จำเป็นเพียงอย่างเดียว เช่น IP Address กับข้อมูลที่มีความละเอียดอ่อนสูงที่สามารถสะท้อนวิถีชีวิตหรือพฤติกรรมการสื่อสารได้ เช่น ข้อมูลจราจรและข้อมูลระบุตำแหน่งซึ่งในบรรทัดฐานฝรั่งเศสนั้น การจัดเก็บข้อมูลที่มีความเข้มข้นสูงเช่นนี้จะกระทำได้เฉพาะกรณีมีภัยคุกคามร้ายแรงต่อความมั่นคงแห่งชาติที่เกิดขึ้นจริงและเป็นปัจจุบันเท่านั้น มิใช่มาตรการบังคับใช้เป็นการทั่วไปในสถานการณ์ปกติเช่นที่ปรากฏในกฎหมายไทย นอกจากนี้ กฎหมายไทยยังเผชิญกับปัญหาเรื่องความไม่ได้สัดส่วนอย่างรุนแรง เนื่องจากมาตรา 26 บังคับให้มีการเก็บข้อมูลจากพลเมืองทุกคนอย่างไม่เจาะจงโดยมีต้องมิเงื่อนไขด้านภัยคุกคามมารองรับ ซึ่งขัดแย้งโดยสิ้นเชิงกับหลักการที่ศาลยุติธรรมแห่งสหภาพยุโรปและสภาแห่งรัฐฝรั่งเศสยืนยันว่าสภาวะปกติรัฐจะกระทำการดังกล่าวไม่ได้

²⁷ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

มาตรา 26 ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ให้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การให้บริการสิ้นสุดลง...

ความเสี่ยงต่อการละเมิดสิทธิส่วนบุคคลเกินสมควรนี้ยิ่งทวีความรุนแรงขึ้นเมื่อพิจารณาความเชื่อมโยงกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ซึ่งแม้จะเป็นกฎหมายที่มุ่งยกระดับสิทธิเหนือข้อมูลสู่มาตรฐานสากล แต่กลับบัญญัติข้อยกเว้นไว้ในมาตรา 4 (2) มิให้นำกฎหมายคุ้มครองข้อมูลส่วนบุคคลมาใช้บังคับกับการรักษาความมั่นคงของรัฐและความมั่นคงปลอดภัยไซเบอร์ การยกเว้น PDPA ให้กับงานความมั่นคงแบบเหมาเข่ง (ครอบจักรวาล) เช่นนี้ ส่งผลให้รัฐสามารถอ้างอำนาจตามมาตรา 26 ของพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อประมวลผลข้อมูลได้โดยปราศจากหลักประกันสิทธิพื้นฐาน เช่น การแจ้งวัตถุประสงค์ที่ชัดเจน หรือสิทธิในการเข้าถึงและตรวจสอบข้อมูลของเจ้าของข้อมูล อันเป็นการสร้างสถานะที่รัฐมีอำนาจเหนือข้อมูลประชาชนอย่างไร้เงื่อนไข

4.2 ความจำเป็นขององค์กรตรวจสอบอิสระที่มีอำนาจผูกพัน

สภาแห่งรัฐได้ชี้ให้เห็นถึงจุดอ่อนทางนิติวิธีของระบบเดิมที่กำหนดให้ คณะกรรมการควบคุมเทคนิคการข่าวกรองแห่งชาติ (Commission nationale de contrôle des techniques de renseignement (CNCTR)) ที่เป็นองค์กรอิสระ (une entité administrative indépendante) มีอำนาจเพียงการให้ความเห็นในลักษณะคำแนะนำทางวิชาการ (Avis simple) ซึ่งไม่มีผลผูกพันทางกฎหมายให้ฝ่ายบริหารต้องปฏิบัติตาม สภาดังกล่าวนอกจากจะบั่นทอนประสิทธิภาพของระบบตรวจสอบถ่วงดุลแล้ว ยังขัดแย้งโดยสิ้นเชิงกับบรรทัดฐานของศาลยุติธรรมแห่งสหภาพยุโรปที่ยึดถือหลักการสำคัญว่า การตรวจสอบการใช้อำนาจรัฐเหนือข้อมูลประชาชนจะบรรลุผลตามเจตนารมณ์ของนิติรัฐได้ก็ต่อเมื่อความเห็นขององค์กรตรวจสอบนั้นมีผลบังคับอันเป็นเด็ดขาด (Effet contraignant) ต่อการตัดสินใจของฝ่ายบริหาร

อย่างไรก็ตาม เมื่อเชื่อมโยงกลับมายังกฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยจะเห็นถึงทัศนคติที่ให้น้ำหนักกับ “ประสิทธิภาพของรัฐ” มากกว่า “หลักประกันสิทธิ” โดยเฉพาะในระดับภัยคุกคามไซเบอร์ระดับวิกฤตที่เจ้าหน้าที่อาจใช้อำนาจเข้าถึงข้อมูลหรือสั่งการได้ทันทีเพื่อเยียวยาความเสียหายล่วงหน้าโดยไม่ต้องผ่านกระบวนการตรวจสอบโดยศาลล่วงหน้าตามมาตรา 67 และมาตรา 68 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562²⁸

²⁸ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

มาตรา 67 ในกรณีที่เกิดภัยคุกคามทางไซเบอร์ในระดับวิกฤต ให้เป็นหน้าที่และอำนาจของสภาความมั่นคงแห่งชาติ ในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามกฎหมายว่าด้วยสภาความมั่นคงแห่งชาติและกฎหมายอื่นที่เกี่ยวข้อง

มาตรา 68 ในกรณีที่เป็นเหตุจำเป็นเร่งด่วน และเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤต คณะกรรมการอาจมอบหมายให้เลขาธิการมีอำนาจดำเนินการได้ทันทีเท่าที่จำเป็น เพื่อป้องกันและเยียวยาความเสียหายก่อนล่วงหน้าได้โดยไม่ต้องยื่นคำร้องต่อศาล แต่หลังจากการดำเนินการดังกล่าว ให้แจ้งรายละเอียดการดำเนินการดังกล่าวต่อศาลที่มีเขตอำนาจทราบโดยเร็ว...

ซึ่งแตกต่างจากโมเดลของฝรั่งเศสที่แม้จะให้ความสำคัญกับความมั่นคงของรัฐ แต่ยังคงรักษาหลักประกันผ่านองค์การตรวจสอบอิสระที่มีผลผูกพันอย่างแท้จริง การเปรียบเทียบนี้ชี้ให้เห็นว่า นิติรัฐไทยในยุคดิจิทัลกำลังเผชิญกับสภาวะย้อนแย้งที่อันตราย ในขณะที่ภาคเอกชนและภาคพลเมือง ถูกบังคับให้ปฏิบัติตามมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แต่ในทางกลับกัน หน่วยงานความมั่นคงกลับได้รับยกเว้นการบังคับใช้กฎหมายดังกล่าวตาม มาตรา 4 (2) แห่งพระราชบัญญัติฉบับเดียวกัน²⁹ ส่งผลให้การปฏิบัติงานด้านความมั่นคงของรัฐคงตกอยู่ในเขตยกเว้นทางกฎหมายที่ขาดระบอบคู่ขนานในการคุ้มครองสิทธิที่เทียบเท่ากับมาตรฐานสากล การนำนิติวิธีและนวัตกรรมทางนโยบายจากคำวินิจฉัยคดี French Data Network มาปรับใช้เพื่อสร้าง “ระบอบคู่ขนานที่เป็นไท” ในกฎหมายไทย จึงมิใช่เพียงทางเลือกทางวิชาการ แต่เป็นความจำเป็นเร่งด่วนในการปกป้องศักดิ์ศรีความเป็นมนุษย์และอธิปไตยทางดิจิทัลของพลเมืองมิให้ถูกล่วงละเมิดภายใต้ข้ออ้างแห่งเหตุผลทางความมั่นคงที่ไม่มีขอบเขต

นัยสำคัญเชิงปฏิรูปสำหรับประเทศไทยจากการวิเคราะห์บรรทัดฐานดังกล่าว คือ ความจำเป็นในการทบทวนกระบวนการตรวจสอบการใช้อำนาจรัฐในการเข้าถึงข้อมูลส่วนบุคคล ซึ่งปัจจุบันมักจำกัดอยู่เพียงการพิจารณาทางธุรการภายในหรือการขอหมายศาลที่อาจกลายเป็นเพียงพิธีกรรมทางกฎหมายหากปราศจากการวิเคราะห์ข้อมูลทางเทคนิคที่ซับซ้อนอย่างถ่องแท้ กฎหมายดิจิทัลของไทยจึงควรได้รับการพัฒนาให้มีกลไกตรวจสอบที่เข้มข้นขึ้นใน 2 ระดับตามมาตรฐานสากล ในระดับแรก คือการสถาปนาระบบการตรวจสอบล่วงหน้า (Contrôle préalable) ที่มีประสิทธิภาพ กล่าวคือ ก่อนที่เจ้าหน้าที่รัฐจะใช้อำนาจเข้าถึงข้อมูลจราจรคอมพิวเตอร์หรือข้อมูลระบุตำแหน่งที่มีความละเอียดอ่อน กระบวนการดังกล่าวจะต้องไม่หยุดอยู่เพียงการขออนุญาตตามลำดับชั้นบังคับบัญชา แต่ต้องผ่านการกลั่นกรองและได้รับคำอนุมัติจากศาลหรือองค์กรตรวจสอบอิสระที่มีอำนาจตัดสินใจเด็ดขาดในการระงับยับยั้งการใช้อำนาจที่ไม่สมควรแก่เหตุ การเปลี่ยนผ่านจากระบบ “รับทราบ” ไปสู่ระบบ “อนุมัติโดยองค์กรที่เป็นกลาง” จะเป็นหลักประกันขั้นพื้นฐานในการคุ้มครองสิทธิความเป็นส่วนตัวมิให้ถูกละเมิดโดยดุลพินิจฝ่ายเดียวของหน่วยงานความมั่นคงระดับที่สองที่มีความสำคัญอย่างยิ่งในยุคเทคโนโลยีเปลี่ยนผ่าน คือ การตรวจสอบความชอบด้วยกฎหมายของนวัตกรรมเทคนิค โดยเฉพาะในมิติของการนำระบบประมวลผลข้อมูลอัตโนมัติหรืออัลกอริทึมมาใช้สืบค้นพฤติกรรมต้องสงสัย สภาแห่งรัฐฝรั่งเศสได้วางรากฐานที่ไม่อาจสั่นคลอนได้ว่า

²⁹ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

มาตรา 4 พระราชบัญญัตินี้ไม่ใช้บังคับแก่... (2) การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์.

การจะเปลี่ยนสถานะจากข้อมูลนิรนามไปสู่การระบุตัวตนบุคคลจากผลลัพธ์ของระบบอัลกอริทึมนั้น จะต้องผ่านกระบวนการตรวจสอบความถูกต้องแม่นยำจากองค์กรอิสระก่อนเสมอ มาตรการเชิงป้องกันนี้มีได้มีวัตถุประสงค์เพียงเพื่อขัดขวางการทำงานของรัฐบาล แต่เป็นการสร้าง “นิติวิธีดิจิทัล” เพื่อป้องกันความผิดพลาดทางเทคนิคที่อาจนำไปสู่การละเมิดสิทธิเสรีภาพของพลเมืองผู้บริสุทธิ์ ในวงกว้าง ท้ายที่สุด การสร้างดุลยภาพระหว่างประสิทธิภาพของรัฐและหลักประกันสิทธิในบริบทไทย จึงมีความจำเป็นต้องอาศัยการจัดตั้งหรือยกระดับองค์กรอิสระที่มีความเชี่ยวชาญเฉพาะด้าน ให้มีอำนาจหน้าที่มากกว่าเพียงพนักงานเจ้าหน้าที่ตามกฎหมายปกติ แต่ต้องเป็นผู้ถือดุลพินิจ ขั้นสุดท้ายที่มีอำนาจผูกพันฝ่ายบริหารอย่างแท้จริง อันจะทำให้ระบบกฎหมายไทยหลุดพ้นจากสถานะการใช้อำนาจอย่างเบ็ดเสร็จในเขตยกเว้นทางกฎหมาย และก้าวเข้าสู่มาตรฐานการเป็นนิติรัฐ ที่สมบูรณ์ภายใต้ความท้าทายของเทคโนโลยีอุบัติใหม่

4.3 อธิปไตยทางกฎหมายภายใต้หลักนิติรัฐ

การสร้างกฎเกณฑ์ที่ซับซ้อน (หรืออาจกล่าวได้ว่าหลุดพ้นไปจากความเป็นจริง (Sophistication inouïe qui les éloignent de la réalité))³⁰ ของศาลยุติธรรมแห่งสหภาพยุโรป ทำให้สภาแห่งรัฐต้องหาวิธีมาตอบโต้เพื่อธำรงไว้ซึ่งอธิปไตยแห่งชาติ (Souveraineté nationale) คำวินิจฉัยคดี *French Data Network et autres* (2021) ได้พิสูจน์ให้เห็นแล้วว่าการรักษาความสงบเรียบร้อยมิได้หมายความว่าความถึงการปฏิเสธพันธกรณีระหว่างประเทศหรือการละเมิดสิทธิมนุษยชนอย่างสิ้นเชิง หากแต่คือการแสวงหาจุดสมดุลผ่านการตีความกฎหมายอย่างชาญฉลาด และสร้างสรรค์ สภาแห่งรัฐได้แสดงบทบาทในฐานะผู้พิทักษ์รัฐธรรมนูญที่กล้าหาญในการยืนยันว่า หากกฎหมายระดับเหนือรัฐ (ในกรณีนี้คือกฎหมายของสหภาพยุโรป) ไม่สามารถให้หลักประกันความปลอดภัยแก่พลเมืองได้เทียบเท่ากับรัฐธรรมนูญภายใน ศาลก็มีความชอบธรรมที่จะเพิกเฉยกฎหมายนั้นเสีย แต่ในขณะเดียวกัน ศาลก็ได้ทำหน้าที่เป็นสถาบันที่ออกแบบระบบการจัดเก็บข้อมูลขึ้นมาใหม่เช่น การใช้ระบบการเก็บรักษาแบบเร่งด่วนมาทดแทน เพื่อให้รัฐยังคงมีเครื่องมือในการปราบปรามอาชญากรรมต่อไปได้ โดยไม่ขัดต่อหลักสิทธิมนุษยชน

สภาแห่งรัฐได้ใช้นิติวิธีตีความกฎหมายอย่างสร้างสรรค์เพื่อประสานรอยร้าวระหว่างความจำเป็นในการปราบปรามอาชญากรรมกับข้อห้ามของสหภาพยุโรป โดยการอนุญาตให้เจ้าหน้าที่ดึงข้อมูลจากฐานข้อมูลความมั่นคงมาใช้ในคดีอาญาได้ ซึ่งในทางปฏิบัติแล้วเท่ากับเป็นการทำให้ข้อจำกัดของศาลยุติธรรมแห่งสหภาพยุโรปที่สภาแห่งรัฐมองว่าไม่สามารถปกป้องคุ้มครองความมั่นคงของประเทศฝรั่งเศสได้ไร้ผลบังคับ (Neutralisé) ไปโดยปริยาย คำวินิจฉัยนี้สะท้อนให้เห็นจุดยืนของสภาแห่งรัฐที่ว่า กฎหมายมหาชนคือเครื่องมือในการรักษาผลประโยชน์สาธารณะ และรัฐธรรมนูญ

³⁰ Brunessen Bertrand, *op. cit.*

ยังคงอยู่สูงสุดในลำดับชั้นกฎหมายภายใน การที่สภาแห่งรัฐยืนยันอำนาจการจัดเก็บข้อมูล จึงไม่ใช่การโต้แย้ง แต่เป็นการทำหน้าที่ถ่วงดุลระหว่าง “สิทธิ” ในอุดมคติของยุโรป กับ “ความมั่นคง” ในโลกความเป็นจริง³¹

สำหรับประเทศไทย บทเรียนจากคดีนี้คือเครื่องเตือนใจว่า ในยุคที่ข้อมูลคือน้ำมันแห่งศตวรรษที่ 21 กฎหมายความมั่นคงไซเบอร์และกฎหมายอาญาของไทย จะต้องไม่ถูกออกแบบมาให้เป็นเพียงเครื่องมือของรัฐในการสอดแนมประชาชนแบบไร้ขอบเขต แต่ต้องถูกกำกับด้วยหลักการความจำเป็นอย่างเคร่งครัด (Strict nécessaire) และความได้สัดส่วนเฉกเช่นเดียวกับกฎหมายของสหภาพยุโรปและของประเทศฝรั่งเศสและรวมถึงแนวคำพิพากษาที่ศาลยุติธรรมแห่งสหภาพยุโรปและสภาแห่งรัฐฝรั่งเศสได้วางบรรทัดฐานไว้ เพื่อให้กฎหมายเป็นเครื่องมือที่สร้างความมั่นคงให้กับรัฐควบคู่ไปกับการสร้างความมั่นใจให้กับสิทธิเสรีภาพของประชาชนอย่างแท้จริง

4.4 ระบบวิธีคิดของสภาแห่งรัฐในการสร้างสมดุลเชิงโครงสร้างทางกฎหมาย

คดี French Data Network สะท้อนให้เห็นถึงระบบวิธีคิดของสภาแห่งรัฐฝรั่งเศสที่ใช้นิติวิธีที่ซับซ้อนเป็นเครื่องมือหลักในการสร้างสมดุลภายใต้ความขัดแย้งของระบบกฎหมาย สภาแห่งรัฐได้แสดงให้เห็นว่าความสมดุลที่แท้จริงไม่ได้เกิดจากผลลัพธ์ของคำวินิจฉัยเพียงอย่างเดียว แต่เกิดจากระบบวิธีคิดและการให้เหตุผลที่ประสานสอดคล้องความขัดแย้งในสองมิติหลัก ดังนี้

มิติแรกคือการบริหารจัดการลำดับศักดิ์ของกฎหมาย สภาแห่งรัฐเผชิญกับแรงกดดันระหว่างหลักความเป็นกฎหมายสูงสุดของกฎหมายสหภาพยุโรปและหลักความเป็นกฎหมายสูงสุดของรัฐธรรมนูญ แต่แทนที่จะใช้วิธีการทางกฎหมายแบบหักดิบด้วยการประกาศว่าศาลยุติธรรมแห่งสหภาพยุโรปกระทำการโดยนอกเหนืออำนาจตามกฎหมายซึ่งจะนำไปสู่สงครามระหว่างศาล สภาแห่งรัฐกลับเลือกใช้วิธีการตีความกฎหมายแบบประสานประโยชน์ โดยการดึงเอาข้อยกเว้นเรื่องภัยคุกคามความมั่นคงแห่งชาติตามมาตราฐานยุโรปมาขยายความและปรับใช้กับข้อเท็จจริงของฝรั่งเศส แนวทางเช่นนี้คือการบริหารจัดการลำดับชั้นของกฎหมายอย่างชาญฉลาด ที่สงวนไว้ซึ่งอธิปไตยทางรัฐธรรมนูญของชาติโดยไม่ทำลายเอกภาพของระบบกฎหมายเหนือรัฐ

มิติที่สองคือการรักษาสมดุลระหว่างความจำเป็นในการใช้อำนาจเพื่อรักษาความสงบเรียบร้อยและการคุ้มครองสิทธิเสรีภาพของประชาชน สภาแห่งรัฐตระหนักดีว่าการอ้างเหตุผลด้านความมั่นคงเพียงอย่างเดียวและโดยที่ไม่ได้สัดส่วนย่อมนำไปสู่การละเมิดสิทธิความเป็นส่วนตัวอย่างรุนแรง ระบบวิธีคิดของสภาแห่งรัฐจึงมุ่งสร้างกลไกทางกฎหมายเพื่อรักษาสิทธิเสรีภาพของ

³¹ F.-X. Millet, « Le glissement jurisprudentiel en matière de données de connexion : l'expansion des compétences de l'Union et sa réception dans les États membres », RFDA, 2023, p. 606, spéc. p. 613 - 614

ประชาชนไปพร้อมกันกับการรักษาความมั่นคงปลอดภัยของประเทศ โดยอนุญาตให้รัฐจำกัดสิทธิของประชาชนได้ก็ต่อเมื่อและตราบท่าที่ยังคงมีภัยคุกคามร้ายแรงอยู่จริงเท่านั้น รวมถึงการสร้างหลักเกณฑ์จำแนกความเข้มข้นของข้อมูล และการกำหนดให้องค์กรตรวจสอบอิสระมีอำนาจอย่างแท้จริงในการบังคับผูกพันให้ต้องปฏิบัติตามกฎหมาย

กรณีศึกษาในคดีนี้จึงสะท้อนให้เห็นว่าระบบวิธีคิดในการทำงานกฎหมายคือศิลปะชั้นสูงในการทำหน้าที่ของตุลาการไกล่เกลี่ยข้อพิพาทเชิงโครงสร้าง เพื่อประสานอุดมคติแห่งการคุ้มครองสิทธิมนุษยชนระดับสากลให้สามารถดำรงอยู่ร่วมกับความจำเป็นในการรักษาความมั่นคงปลอดภัยของรัฐในโลกแห่งความเป็นจริง และโดยเฉพาะอย่างยิ่งในโลกยุคดิจิทัล ได้อย่างยั่งยืน

บทสรุป

คำวินิจฉัยของสภาแห่งรัฐฝรั่งเศสเมื่อวันที่ 21 เมษายน 2021 ในคดี *French Data Network et autres* ถือเป็นหมุดหมายสำคัญทางประวัติศาสตร์กฎหมายมหาชน ที่มีได้เพียงคดีข้อพิพาทเรื่องการจำกัดข้อมูลจราจรทางคอมพิวเตอร์เท่านั้น หากแต่เป็นการวางรากฐานนิติวิธีใหม่ในการจัดการความขัดแย้งระหว่างระบอบกฎหมายในยุคดิจิทัล โดยสภาแห่งรัฐได้แสดงให้เห็นถึงความเป็นผู้พิทักษ์รัฐธรรมนูญที่เฉียบคมผ่านการใช้นิติวิธีแบบ “Solange” ในรูปแบบของฝรั่งเศสซึ่งเป็นการยืนยันหลักการสำคัญว่า โดยหลักแล้วแม้กฎหมายสหภาพยุโรปจะมีสถานะเหนือกว่ากฎหมายภายในตามหลักความสำคัญเหนือกว่าของกฎหมายสหภาพยุโรป แต่ความเหนือกว่านั้นมิได้มีลักษณะสมบูรณ์ไปเสียทั้งหมด หากการบังคับใช้กฎหมายหรือการตีความของศาลยุติธรรมแห่งสหภาพยุโรปส่งผลให้ข้อเรียกร้องทางรัฐธรรมนูญ (Exigences constitutionnelles) ที่สำคัญ เช่น ความมั่นคงแห่งชาติต้องสูญเสียหลักประกันที่มีประสิทธิภาพไป สภาแห่งรัฐในฐานะศาลปกครองสูงสุดย่อมมีอำนาจที่จะเพิกเฉยหรือปฏิเสธการบังคับใช้กฎหมายของสหภาพยุโรปในส่วนนั้นได้ เพื่อรักษาไว้ซึ่งโครงสร้างพื้นฐานและค่านิยมสูงสุดของรัฐธรรมนูญแห่งชาติ

ในมิติของการสร้างดุลยภาพใหม่แห่งความมั่นคงสภาแห่งรัฐมิได้เลือกหนทางที่นำไปสู่ความแตกหักโดยตรงกับศาลยุติธรรมแห่งสหภาพยุโรป แต่กลับเลือกใช้ศิลปะแห่งการตีความเพื่อสร้างระบบคู่ขนานที่มีความยืดหยุ่นสูง โดยวางหลักการว่าในภาวะปกติ รัฐมีหน้าที่ต้องเคารพสิทธิความเป็นส่วนตัวอย่างเคร่งครัดตามมาตรฐานยุโรปซึ่งห้ามการเก็บข้อมูลจราจรแบบทั่วไปและไม่เจาะจงแต่ในขณะเดียวกัน เมื่อรัฐต้องเผชิญกับภัยคุกคามร้ายแรงต่อความมั่นคงแห่งชาติ ซึ่งสภาแห่งรัฐวินิจฉัยอย่างมีนัยสำคัญว่าสถานการณ์การก่อการร้ายในปัจจุบันของฝรั่งเศสเข้าข่ายภัยคุกคามที่เกิดขึ้นจริงและเป็นปัจจุบัน (Réelle et actuelle) รัฐย่อมมีความชอบธรรมที่จะใช้อำนาจเต็มทีในการสั่งให้ผู้ให้บริการจัดเก็บข้อมูลแบบเป็นการทั่วไปและไม่เจาะจงต่อไปได้ ตราบเท่าที่ภัยคุกคามดังกล่าวยังคงดำรงอยู่และมีการทบทวนสถานการณ์เป็นระยะ

นอกจากนี้ คำวินิจฉัยดังกล่าวยังนำเสนอเอกลักษณ์ของนวัตกรรมทางกฎหมายเพื่อการปราบปรามอาชญากรรมโดยเฉพาะสำหรับคดีอาชญากรรมทั่วไปที่มีใช้เรื่องความมั่นคงแห่งชาติโดยตรง สภาแห่งรัฐได้วางแนวทางใหม่ด้วยการแยกประเภทข้อมูลที่น่าสนใจยิ่ง คือการอนุญาตให้รัฐสามารถจัดเก็บข้อมูล “IP Address” ได้เป็นการทั่วไปเพื่อประโยชน์ในการระบุตัวต้นผู้กระทำผิดทางออนไลน์ พร้อมทั้งนำกลไกการเก็บรักษาแบบเร่งด่วนมาใช้เพื่อทำการ “แซ่แซ่” ข้อมูลจราจรอื่น ๆ เฉพาะส่วนเมื่อมีเหตุอันควรสงสัย นิติวิธีนี้จึงถือเป็นการผสมผสานระหว่างประสิทธิภาพในการสืบสวนสอบสวนทางอาญากับการคุ้มครองสิทธิขั้นพื้นฐานของประชาชนได้อย่างลงตัวในทางปฏิบัติ

อย่างไรก็ตาม แม้คำวินิจฉัยนี้จะเปรียบเทียบสถานการณ์กอบกู้ระบบการทำงานของหน่วยข่าวกรองและความมั่นคงของฝรั่งเศสไว้ได้ในระยะสั้น แต่ในระยะยาวยังคงทิ้งโจทย์ปลายเปิดที่สำคัญและท้าทายสำหรับนักกฎหมายมหาชนในอนาคต โดยเฉพาะประเด็นเรื่องการนิยาม “ภัยคุกคามร้ายแรง” (menace grave) ซึ่งการที่สภาแห่งรัฐยอมรับสถานการณ์ภัยคุกคามจากการก่อการร้ายให้เป็นสถานะที่เกิดขึ้นต่อเนื่องเป็นเวลานาน อาจนำไปสู่สถานะที่ข้อยกเว้นกลายเป็นหลักการ และหากภัยคุกคามนั้นถูกทำให้กลายเป็นสิ่งถาวรในความรู้สึกของรัฐ สิทธิความเป็นส่วนตัวของประชาชนย่อมเสี่ยงที่จะถูกระงับไว้เป็นเวลายาวนานโดยไม่มีกำหนด ซึ่งถือเป็นเส้นแบ่งที่เปราะบางอย่างยิ่งระหว่างการรักษาความมั่นคงภายใต้หลักนิติธรรมกับการก้าวเข้าสู่ระบอบรัฐตำรวจ (État policier) ในคราบของกฎหมายความมั่นคงดิจิทัล

ความท้าทายที่รออยู่เบื้องหน้าจึงมิได้จำกัดอยู่แค่ตัวบทกฎหมาย แต่ยังรวมถึงบทบาทของเทคโนโลยี “อัลกอริทึม” โดยเฉพาะที่พัฒนาสู่ระบบปัญญาประดิษฐ์ (AI) ที่คำวินิจฉัยนี้ยอมรับให้ใช้ตรวจจับพฤติกรรมต้องสงสัย ทว่าในวันที่เทคโนโลยี AI พัฒนาไปจนถึงขั้นสามารถวิเคราะห์ความเชื่อมโยงที่ซับซ้อนเกินกว่าสติปัญญาของมนุษย์จะหยั่งถึง เส้นแบ่งระหว่างการ “ตรวจจับภัยคุกคาม” กับการ “ทำนายพฤติกรรม” (Police prédictive) จะยิ่งเลือนลางลง และโจทย์ใหญ่ที่กฎหมายมหาชนต้องขบคิดคือเราจะก้าวตามให้ทันเทคโนโลยีเพื่อคุ้มครองเสรีภาพและเจตจำนงของมนุษย์ (Libre arbitre) มิให้ถูกลดทอนลงเหลือเพียงแค่ข้อมูลตัวเลขภายใต้การบงการของชุดคำสั่งได้อย่างไรท้ายที่สุด คดีนี้สะท้อนให้เห็นว่าในศตวรรษที่ 21 “ข้อมูล” (Data) ได้แปรสภาพเป็นทรัพยากรแห่งอำนาจจิปาถะใหม่ การที่รัฐจะรักษาความมั่นคงของตนเองได้อย่างยั่งยืน จำเป็นต้องมีอำนาจควบคุมเหนือโครงสร้างพื้นฐานทางข้อมูลเหล่านี้ควบคู่ไปกับการรักษาศรัทธาของพลเมือง

สำหรับประเทศไทย การออกแบบกฎหมายดิจิทัลจึงมิใช่เพียงการลอกเลียนมาตรฐานสากลแบบไร้ราก แต่ต้องเป็นการสร้าง “ระบอบกฎหมายที่เป็นไท” (Autonomie juridique) ที่สามารถปกป้องผลประโยชน์ของชาติและสิทธิของพลเมืองไปพร้อมกันได้อย่างสง่างาม คำวินิจฉัยคดี French Data Network จึงเป็นดังประกายที่ส่องแสงนำทางท่ามกลางพายุแห่งความขัดแย้งในโลกดิจิทัล ย้ำเตือนให้เราตระหนักว่ากฎหมายที่ดีที่สุดมิใช่กฎหมายที่เคร่งครัดที่สุด หากแต่คือกฎหมายที่สามารถปรับตัวและรักษาคุณภาพแห่งคุณค่าที่ขัดแย้งกันได้อย่างชาญฉลาดและเที่ยงธรรมที่สุดนั่นเอง

บรรณานุกรม

1. กฎหมาย (Normes juridiques)

1.1 กฎหมายต่างประเทศและระหว่างประเทศ

Charte des droits fondamentaux de l'Union européenne.

Constitution du 4 octobre 1958 (France).

Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002
(Directive vie privée et communications électroniques).

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril
2016 (RGPD).

Code de la sécurité intérieure (France).

Code des postes et des communications électroniques (France).

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique
(LCEN, France).

Traité sur l'Union européenne (Traité de Lisbonne).

1.2 กฎหมายไทย

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562.

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562.

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (และที่แก้ไข
เพิ่มเติม).

2. คำวินิจฉัยของศาล (Jurisprudence)

2.1 ศาลยุติธรรมแห่งสหภาพยุโรป (Cour de justice de l'Union européenne)

CJUE, Gde ch., 6 octobre 2020, *La Quadrature du Net et autres*, aff. jointes
C-511/18, C-512/18 et C-520/18, ECLI:EU:C:2020:791.

2.2 ศาลฝรั่งเศส (Juridictions françaises)

Conseil d'État, Ass., 21 avril 2021, *French Data Network et autres*, n° 393099
(และดูบทวิเคราะห์ประกอบ *Analyse de la décision* และคำแถลงการณ์
ตุลาการผู้แถลงคดี *Conclusions de M. Alexandre Lallet* ทาง <https://www.conseil-etat.fr/arianeweb>).

Conseil d'État, Ass., 8 février 2007, *Société Arcelor Atlantique et Lorraine
et autres*, n° 287110.

Conseil constitutionnel, 12 juin 2025, décision n° 2025-885 DC, Loi visant à sortir la France du piège du narcotrafic.

2.3 ศาลเยอรมัน (Juridictions allemandes)

BVerfG, Urteil des Zweiten Senats vom 5. Mai 2020 - 2 BvR 859/15 - (Weiss / PSPP).

BVerfG, 29 mai 1974, *Internationale Handelsgesellschaft mbH* (BVerfGE 37, 271 - Solange I).

3. เอกสารวิชาการ (Doctrine)

AZOULAI, L. et RITLENG, D. « “L’État, c’est moi”. Le Conseil d’État, la sécurité et la conservation des données », *Revue trimestrielle de droit européen (RTD eur.)*, 2021.

BERTRAND, B. « L’arrêt French Data Network du Conseil d’Etat : un dialogue des juges en trompe l’œil », *Le Club des juristes*, 7 mai 2021, [en ligne].

DE MONTECLER, M.-C. « Conservation des données : la guerre des juges n’aura pas lieu », *Dalloz actualité*, 26 avril 2021, [en ligne].

DUPRÉ DE BOULOIS, X. (dir.), *Les grands arrêts du droit des libertés fondamentales*, 5e éd., Paris, Dalloz, 2025.

GRYNBAUM, L., *Droit des activités numériques*, 2e éd., Paris, Dalloz, 2023.

MILLET, F.-X. « Le glissement jurisprudentiel en matière de données de connexion : l’expansion des compétences de l’Union et sa réception dans les États membres », *RFDA*, 2023.

4. ทรัพยากรอื่น ๆ (Autres sources)

Vie-publique, « Qu’est-ce que la Charte des droits fondamentaux de l’Union européenne ? », 9 août 2024, [en ligne].

Minority Report (ภาพยนตร์), กำกับโดย Steven Spielberg, ค่าย 20th Century Fox / DreamWorks Pictures, 2002.